2007

An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts

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*

Follow this and additional works at: [http://aisel.aisnet.org/pacis2007](http://aisel.aisnet.org/pacis2007)

Recommended Citation  
[http://aisel.aisnet.org/pacis2007/75](http://aisel.aisnet.org/pacis2007/75)
85. An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts

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

Abstract

This paper addresses many important questions. Firstly, what are the main identity fraud perpetrator categories? Secondly, what are the current Information Systems (IS) facilitated attack channels and methods used by identity fraud perpetrators? Thirdly, what are the effects sustained by targeted victim organisations? The major contribution of this paper is the development of an identity fraud perpetrator framework and an understanding of the model’s elements and relationships. This framework will be useful to law enforcement, business and government organisations when fighting identity crime. This research has spawned a larger research agenda into identity fraud.

Keywords: Information Systems, Proof of Identity (POI) and Personal Identifying Information (PII), Identity Fraud, Identity Fraud Perpetrators, Organisational Impact of Crime

* 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.

Introduction

To date research is sparse on what the main elements are in the identity fraud landscape, including the different specific methods that perpetrators use in their modes of attack, and the subsequent impact on the organisation as a victim (Malakedsuwan and Stevens 2003). This paper addresses these issues and investigates who are the main perpetrator groups, how identity fraud attacks occur against organisations, and what is their impact on organisations. Results are derived from analysis of interviews undertaken in an Australian context. Identity type crimes are pervasive in attacking organisations’ or individuals’ (customers’) information systems (IS) in order to gather private information to be used against organisations to extract some benefit for the perpetrator through the anonymity of identity theft or identity deception acts. A definition of an IS relevant to this study is “a system, whether automated or manual, that comprises people, machines, and/or methods organised to collect, process, transmit, and disseminate data that represent user information” (ATIS Committee T1A1 2007, p.1).
Identity theft and identity deception are identity crime categories spanning the continuum of initiating enablers and key drivers of identity fraud. Where “identity theft is from an actual person (living or dead, natural or corporate) by using stolen personal information, or fraudulently obtained, forged, or stolen identity documents” (Australasian Centre for Policing Research 2005, p.1). Identity deception (refer Wang et al. 2004) is extended to include all identity crimes type acts not covered by the identity theft definition e.g., includes documents lent to seek health benefits. Categorising the identity deception definition in this manner will cover any gaps not originally anticipated by Wang et al (2004) as the given example illustrates. The target organisations’ are predominantly financial institutions, utilities, retailers, government welfare agencies, issuers and users of proof of identity (POI) documentation. However, organisations across all sectors within industry, non-profit organisations, and other government agencies are also targets e.g., Real Estate, Health Care, Pharmacies, and Immigration. Identity fraud, by its very nature, is difficult to detect and is a major cause of the increasing trend over the last decade in the financial cost and social burden to the organisations targeted. Perpetrators target POI documents often referred to as a country’s ‘base documents’ (e.g., Birth Certificate, Passport, Driver’s License) and secondary level documents (e.g., education certificates, utility accounts, and bank statements). The legitimate purpose of secondary level documents is specific information exchange between issuer and user. Yet the secondary documents are also used to corroborate (along with base documentation) ‘who you are’ and that you have a ‘footprint’ (such documentation may show your current or past residential address) or that you are ‘known by that name’ in society. Perpetrators target both document categories to secure personal identifying information (PII). Often they obtain a ‘set’ of POI documents in order to present themselves as ‘legitimate customers’ to deceive the target organisations authentication and verification processes to commit identity fraud (Kochems and Keith 2006). Increasingly, the mode of attack for the fraud, especially the identity fraud perpetrator is tending to rely on electronic commerce or mechanical/digital devices to initialise the identity theft or identity deception act. This is to some extent enabled by internet adoption e.g., 77% of United States (US) adults were online at May 2006, up from 74% in 2005, 66% in 2002, 64% in 2001 and 57% in 2000 according to Harris Interactive (eMarketer 2006). Also, because in the e-commerce environment the perpetrator does not have face-to-face contact with customer service, they do not therefore give away any other tell tale signs of lying, cheating or deception. The perpetrators’ intent and purpose is to get to the targets’ money, goods and services (assets), or avoid costs and expenses (liabilities), and evade detection or blame through the use of another’s legitimate identification account channel with the target. According to identity theft complaints received by the US Federal Trade Commission (FTC) from November 1999 to September 2001, over 60% (58,078) of methods used by identity fraud perpetrators were unknown, and in only 20.5% (19,241) of complaints were the methods known (FTC 2006).

Methodology
In order to measure, manage, assign risks, and secure systems from identity fraud perpetrators we need to better understand the perpetrators methods of operation including mapping and categorising the vast majority that are unknown (according to the earlier complaints survey). This research addresses the following questions:

1. What are the main identity fraud perpetrator categories?
2. What are the current IS facilitated attack channels and methods used by identity fraud perpetrators?
3. What are the effects sustained by targeted victim organisations attacked by these perpetrators of identity fraud and related crimes?

<table>
<thead>
<tr>
<th>Participant Code</th>
<th>Participant Category</th>
<th>Participant Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bank 1</td>
<td>1. Head of Fraud – Policy &amp; Strategy</td>
</tr>
<tr>
<td>2</td>
<td>Bank 2</td>
<td>1. Chief Manager Operational Control 2. Fraud Management</td>
</tr>
<tr>
<td>5</td>
<td>Licensing Authority 2</td>
<td>1. Manager</td>
</tr>
<tr>
<td>6</td>
<td>Telecommunications</td>
<td>1. Fraud Risk</td>
</tr>
<tr>
<td>7</td>
<td>Government Agency 1</td>
<td>1. Compliance, Integrity &amp; Documentation Examination</td>
</tr>
<tr>
<td>10</td>
<td>Government Agency 4</td>
<td>1. Deputy CEO – Corp Services and Regulatory Issues</td>
</tr>
<tr>
<td>11</td>
<td>Government Agency 5</td>
<td>1. Client Account Management</td>
</tr>
<tr>
<td>12</td>
<td>U.S. Criminologist</td>
<td>1. Academic – Professor</td>
</tr>
</tbody>
</table>

The existing literature on identity crime methods that target information systems was reviewed to ascertain the following:

- identity theft and identity deception perpetrator methods;
- subsequent security breaches; and
- The impact on organisations targeted by identity fraud perpetrators.

Based on the findings from this review a series of structured interviews were conducted to capture data from Australian industry and government experts with respect to questions on identity fraud and related crimes – refer Table 1 above for a list of participants.

The interviews used an open-ended semi-structured set of questions in order to collect the research data. A pilot interview was conducted on the initial set of questions to evaluate their comprehension, relevance and to determine the interview duration. The research was conducted through a series of face-to-face interviews and teleconferences for interstate organisations. The interviews were recorded and transcribed. Analysis of interviewee transcripts was aided by the use of (QSR NVivo 7 2006) software. A model was developed that helps to categorise perpetrators, channels, attack methods, and victims. Results from the interviews also aided in understanding the impacts of identity fraud on organisations.

**Literature Review**

Existing models of identity fraud and interrelated crimes have usually focused on methodologies from the organisation’s perspective (see Cuganesan and Lacey 2003; Wilhelm 2004), with only a few interpreting the perpetrators and their attack methods or innovations (exceptions include Le Lievre and Jamieson 2005; Malakedsuwan and Stevens 2003; and Wang et al., 2006). Conceptual components of our model have both theoretical and empirical underpinnings - for example, from a criminological background of perpetrators organised crime is included (Calavita 1993), similarly,
criminal profiling for individual perpetrators (Kocsis 2006; Petherick 2006) is included, and, from management and IS insiders or employees (see Dhillon 2001; Dhillon and Moore 2001) are added. From the perspective of crime opportunities related to this study within IT/IS devices, e-commerce or systems, researchers have undertaken investigations of computer crime (Marx and Reichman 1984; Parker 1976), e-Crime (Malakedsuwan and Stevens 2003), and e-Fraud (Vasiu 2004) to name a few. More recently there has been an emergence of publications on the individual e-commerce methods perpetrators use to perpetrate identity theft and identity fraud events, such as Phishing (see Lininger and Vines 2005). The impact on organisations with respect to the role e-commerce or identity crime facilitates this is also receiving attention from IT/IS (Stephenson 2000), and identity fraud disciplines (Lacey and Cuganesan 2004) among others. Additional background discussion of the model’s subcomponents is briefly outlined in the following sections.

Model of Identity Fraud Perpetrators, their IS Attack Channels and Methods
Figure 1, overviews the contextual relationship from the identity fraud perpetrators attacking the targeted organisations through to the monetary losses suffered by firms and customers. Documented figures from targeted countries show that identity fraud costs American consumers US$5 billion and businesses US$48 billion in 2005. In February 2006 the United Kingdom (UK) reported that the annual cost of identity fraud had reached £1.72 billion up from £1.3 billion in 2002. In Canada, it was estimated that the identity theft and identity fraud annual cost was C$2.5 billion to Canadian consumers and businesses, and the total annual cost to the Canadian economy was estimated at C$5 billion. The cost of identity fraud in Australia was estimated to be AU$1.1 billion a year (refer Jamieson et al., 2007).

Figure 2 below, highlights the four perpetrator categories, three dominant channels of attack, and the organisations most often targeted by identity fraud perpetrators.
The actual methods used by identity theft and identity deception perpetrators are also shown. The interrelationships between these groups and related crimes include money laundering, illegal trafficking of people, drugs and weapons, and terrorism. Perpetrator categories, channels and methods of attack are discussed below.

**Four Perpetrator Categories**

The identity fraud perpetrator can be an external or internal party. Perpetrators can commit identity fraud using information of a prospective or existing customer or a prospective, existing, or terminated agent of the organisation. “The external fraudster has three basic profiles, the average offender, criminal offender, and organised crime offender. Average offenders display random and occasional dishonest behaviour when there is opportunity, sudden temptation, or when suffering from financial hardship” (Phua et al. 2005, p.2).

We classify identity fraud perpetrators into four distinct categories, three external to the target organisation and one internal (see Figure 2, above). The external categories are, organised crime groups (>2 perpetrators, usually sophisticated and well resourced), sophisticated perpetrators (mostly individuals, but possibly working in pairs) and opportunistic perpetrators (not necessarily unsophisticated individuals/pairs or of an unplanned mindset). The fourth category, internal to the target, is an agent of the organisation (includes employees, contractors, consultants etc). “Employees have also been used by organised gangs to infiltrate an organisation. This makes it easier for the external attack to go unnoticed by supplying information about an organisation’s system weaknesses, and peak usage times” (Participant 5). These identity theft and identity deception perpetrators attack victim entities across three dominant channels, ‘traditional’ methods, devices (mechanical/digital), and e-commerce. Within our designated three channels, perpetrators often specialise in a particular mode of attack that best suits their skill-set to attack through an organisation’s weakest verification or authentication points. The fact that some organisations still require POI documentation to be
presented in person potentially creates an interaction between the three dominant channels. For example, a sophisticated perpetrator could use the traditional method of mail interception to obtain a bank customer’s PII or POI documentation, and then use some mechanical or digital device to imprint their photo onto documentation. This documentation will be presented at a bank, then used via telebanking to transfer cash to other accounts or the perpetrator will use the PII or POI to drain bank accounts online.

The highest risk category is where external fraudsters are individual criminal offenders and organised crime offenders because this group repeatedly disguise their true identities. They can also evolve their mode of attack over time to approximate legal forms by obtaining legitimately issued, but fraudulent, POI documentation to counter organisation’s detection systems. Therefore, it is important to account for the strategic interaction, or moves and countermoves, between a fraud detection system’s learning capabilities and the professional perpetrators innovative modes of attack. It is probable that internal and insurance fraud is more likely to be committed by average offenders, whereas credit and telecommunications fraud is more vulnerable to professional (sophisticated) identity crime perpetrators (Phua et al. 2005).

Perpetrator agents can also be ‘insiders’ and as such include current disgruntled employees, ex-employees, contractors, outsourcers, partners, third party dealers and ‘employee plants’. Internal attacks by employees by way of identity fraud/crimes are increasing and occur for a variety of reasons. From an organisation’s perspective, this channel of perpetration is the most frightening because the perpetrator has broken their trust and passed through their outer perimeter controls and checking procedures, or breached their prescribed levels of security access, privileges, and authority. All of which can be used against an organisation to by-pass, conceal, and use systems access, ‘know-how’, and weaknesses to perpetrate identity fraud.

For example, “dishonest employees who have access to computer terminals connected to one of the credit reporting agencies. They might look for names similar to theirs or just someone with good credit [rating]. Obviously what goes hand in hand with this type of access is the negligence of the company, which is permitting such uses in an unmonitored environment” (Givens 2000, p.3). Most organisations implement a set of written rules, policies or procedures that employees must abide by for their level of authority, position or status. For example, one interviewee states “We actually have very stringent policies and procedures that we apply to the internal staff, like our code of conduct and ethics is very extensive. It actually covers a whole ambit of different issues in relation to use of information, accessing information. We’ve also got procedures that basically make every staff [member] aware of the implications of their actions. And what we also have is a fairly well controlled mechanism of detecting any misuse - so we have monitoring mechanisms. We basically have supervision - fairly active supervision. We have a database that gives us a good record of all access logs, so we are able to track anything that is done within the database by the staff. And, even for example, our call centres are well monitored, so if someone’s actually accessing a customer record, we become aware of it, and we have mechanisms to actually track back. So it is a very good system that way. There is always going to be the opportunity I suppose, but we have ... I confidently say that we have a very good system of basically prevention and detection” (Participant 4(2)). Yet real world examples of an internal agent perpetrating identity fraud are numerous. Participant 12 explains the risk as, “that anyone would need to steal my identity and it could have been done by just having just one insider ... minimum wage employee in this store and one crook or one guy that they would get to and it would be all over... so people just have to be concerned about this, businesses have to be concerned about it to ... more public education really is the thing it has to be made an issue with the
The government is not going to be able to do it alone, we aren’t going to be able to do it alone, systems people aren’t going to be able to do it alone, you can’t do it, you know, regardless of best technology and everything else, people have to be brought into it in a big way and it hasn’t happened in the U.S. and I assume it hasn’t happened here.”

The cost of employee related identity fraud in the UK could soon top £13 billion as criminal gangs infiltrate banks and other businesses with bogus employees planted to help commit fraud. However, the Financial Services Authority has warned that improvements in anti-fraud measures mean that organised crime syndicates are now seeking increasingly sophisticated ways to infiltrate organisations and instances of employee ‘plants’ have increased dramatically in the past 18 months (PR Newswire 2005). “It used to be unusual to make a connection between employee fraud and organised crime, but increasingly, the links are becoming evident. Some of the money from employee fraud, particularly from the deliberate infiltration of dishonest staff into major financial services companies, is believed to be finding its way to fund terrorism, drugs, vice and other organised crime” (CIFAS 2006, p.3).

“As much as 70 % of all identity theft starts with theft of personal data from a company by an employee” (Sullivan 2004, p.1).

Channels of Perpetrator Attacks and Examples of Specific Methods within Channels

A recent US survey (Javelin Strategy & Research 2006, pp.1-5) found that “computer crime accounted for 11.6% of identity theft cases in 2004, compared with 68% from paper sources”. Most identity fraud happens the ‘traditional’ way, via lost or stolen credit cards, wallets and cheques, with well over half the perpetrators known to victims. “The percentage of identity fraud occurring via the Internet is just nine percent, with much of that via online banking where the nation's major financial institutions fall short in prevention”, the Javelin study determined. "Ninety percent of the data accessed is done in a traditional way, through off-line channels like lost or stolen credit cards, wallets or check (i.e., cheque)". "Forty-seven percent of fraud victims could identify the source of data compromise and 36 percent could identify the actual person." Also, “when the person was known, nearly half the time that person was a relative, friend, neighbour, or in-home employee” (Javelin Strategy & Research 2006, pp.1-5). Traditional methods also include dumpster diving, scams to extract bank account details, mail interception or mail redirection, theft of laptops, hard drives and other information repository devices. Although identity theft has become more high-tech in recent years, pickpockets are still around, searching for loosely guarded personal items to steal. “Mail non-receipt frauds involve cards being stolen before they are delivered to the cardholder. This fraud type was up by 62 per cent from 2003, totaling at £72.9m (Nicholas et al. 2005, p.62).

Devices, including mechanical/digital devices are those that provide any method of replicating proof of identity documents (licenses, passports, security passes), are used to capture PII (e.g., PINs, passwords, signatures) that are then used to facilitate an identity fraud act. Often a perpetrator will commit an identity theft event and then clone the stolen POI or PII, or, using the format of the stolen information, commit identity deception by falsifying, or fabricating, new details of real people (living or deceased) or non-existent people profiles (fictitious). A list of such devices includes: skimming using embossing and encoding machines to produce skimmed bank credit or debit cards; computer hardware (e.g., printers); copying devices; camera equipment; wireless intercept devices; and other devices used to gather personal data from Web sites.
E-commerce modes include crimes by perpetrators who compromise computer databases by hacking into the information repositories via the Internet using software, such as email viruses (Trojans), scams, key loggers, phishing, pharming, malware, adware, spyware, vishing etc. The objective of these e-commerce modes is to extract POI or PII information to access bank accounts etc. Participant 3(1) adds, “We’ve seen, products, such as, keystroke capturing devices being used. But what we are seeing is increasingly, although the volumes of fraud or the value of the fraud and the volumes are not high, it is increasing where ... completely unknown, the software is left at shared PC environments, like Internet cafes or public libraries, and that’s a growing problem. So that’s sort of really current right now.”

Customer or Organisations Attacked for POI and PII (Identity Theft & Deception)
Targeted organisations include utility companies (e.g., telecommunication services), retailers that offer instant credit, large banks, and government agencies (e.g., welfare). Research found that perpetrators “tended to use a number of pieces of documentation including credit or bank cards, driving licenses, bank statements, utility bills and passports. It was rare for just one piece of documentation to be used; however, when this was the case it tended to be a driving licence” (Pascoe et al. 2005, p.7). Interviewees in an Australian context concur with this, adding, “a lot of these people (perpetrators) can walk in with genuine documents because they have already hit the license sergeant to run your genuine documents in the file before they start” (Participant 1). Another approach of perpetrators to access identity documents or authentication passes is finding ways to gain the victims confidence because identity theft is more easily carried out with unsuspecting people close to the perpetrator. Yet results from a victims study in the UK found that, “In 84 percent of the cases victims did not know the offender. Those that did (11 percent) pointed to friends and family members especially partners and ex-partners” (Pascoe et al. 2005, p.7). Alternatively, with identity deception, perpetrators endeavour to take over another person’s account, first by gathering information about the intended victim. The perpetrator then contacts the card issuer, pretending to be the genuine cardholder, to ask that mail be redirected to the perpetrator’s address. The perpetrator then reports the card lost and asks for a replacement to be sent. Perpetrators have also targeted organisations directly seeking to change their mailing address in a similar way as for individuals by informing a central agency that registers companies. All these identity fraud instances are omnipresent, yet they tend to be focused more towards developed countries to date.

Implementation of robust deterrence, prevention and detection systems by organisations tends to drive perpetrators to weaker organisations or weaker product channels within organisations.

Impact on Target Organisations of Identity Fraud
A recent victimisation survey report (FTC 2006) stated that 90 percent of total identity theft losses are borne by businesses and financial institutions. Targeted organisations and entities are the main focus of this research and identity fraud impacts them in the following ways:

- **Brand damage.** This is particularly evident in phishing attacks when identity thieves impersonate trusted organisations, creating false emails and Web sites to steal personal information. Credibility and reputation also suffers whenever a breach is made public.

- **Costly customer account repair.** Corporations that issue credit to people they believe are good credit risks, but are actually criminals, typically bear the cost of credit extended.
• **Systems failure.** In cases where a computer system is breached, organisations have to bear significant costs in strengthening the security features of those systems so that they are not breached again.

• **Legal costs.** Companies and consumers who are damaged by breaches are increasingly turning to private legal civil/criminal action to try to gain compensation for those losses” (Liberty Alliance 2005, p.5).

• **Loss of reputation.** Prior research has shown that an organisation’s reputation is positively correlated with that organisation’s financial well-being and organisations with a good reputation are more likely to maintain superior performance measured by profits over time (Roberts and Dowling 2002).

• **Cost, time and effort involved in restoration to situation prior to identity crime acts.** For example, there have been many recent instances where perpetrators have hacked into databases and stolen customer’s bank account details resulting in the bank having to reissue new credit cards to customers.

• **Poor credit standing with potential economic and financial hardship.** A poor credit rating by credit scoring firms (e.g., Experian, S&P, Moody’s, Dun and Bradstreet etc) lowers an organisations reputation leading to poor financial performance.

• **Final demands or other threats for products or services not purchased or received.**

• **Unwelcome receipt of summons, court actions, judgments, and publicity.**

• **Difficulty in opening new credit lines or accounts** (see BT Plc, 2006).

• **There have also been accounts of criminal/felony convictions against the victim** (we thank an anonymous referee for this point).

The mostly non-monetary losses made by the points above show identity theft and identity deception enable identity frauds to take a severe toll on targeted organisations in addition to the monetary losses alluded to in Figure 1, above.

**Implications and Limitations**
This Australian based study develops theory by framing a model for categorising identity fraud perpetrators. The model is further strengthened by categorising perpetrators’ channels of attack and listing methods within identified channels that facilitate the obtaining of POI or PII by identity theft and/or identity deception techniques. The results presented in this study will be investigated further for better understanding of identity fraud in a digital environment in the context of e-commerce. The model will also be empirically validated using the Australian Crime Commission’s fraud database of identity crimes.

**Discussion of Model**
We group identity fraud and related crime perpetrators’ modes of attack into three distinct categories – traditional methods, devices, and e-commerce, according to the generic method they use to secure POI documentation (by identity theft and identity deception) for PII or authentication information (PIN, token keys, passwords, biometrics etc). The POI
documentation or information is the enabler to help perpetrators to further commit identity fraud and related crimes against organisations. The first channel is categorised as the ‘traditional’ method and includes dumpster raiding, wallet theft, and mail interception. According to recent surveys (FTC 2006; Javelin Strategy & Research 2006) these identity theft penetration methods were the dominant modus operandi of the perpetrator to secure POI.

The second channel is categorised as ‘devices’ (mechanical/digital) where embossing and encoding machines produce skimmed cards, or where devices are used for skimming cards at automated teller machines. Other devices are also used, including printers, photocopieters and camera equipment as well as other computer hardware/software devices such as keyloggers. This method is predominantly used for identity theft, however, printing, photocopying, and camera equipment facilitate identity deception techniques as well (refer Wang et al. 2004). The third category is the ‘e-commerce’ channel, where the method of attack is mostly via the Internet. Here software such as viruses or methods labelled as, phishing, pharming, Trojans, worms and keyloggers are now evolving from PC’s to other platforms such as personal data assistants and mobile telephone devices (e.g., vishing etc) in order to harvest POI or PII (see for example, Turner 2006). The e-commerce platform is well-suited to identity theft and identity deception acts as mentioned by interviewees, as they permit perpetrator anonymity. As perpetrators don’t have to present their POI documentation in person, they avoid customer service interaction where the organisation can enforce additional security measures and customer requirements to supply more information (often referred to as ‘non-wallet questions’).

One practical benefit from documenting the actual methods used by identity theft and identity deception perpetrators will be that target organisations can then seek out security solutions and systems to better deter, detect, and prevent perpetrator attacks. Lobbying industry bodies and government for appropriate legislative change can also make a difference. The documentation of perpetrator methodologies and the interrelationships between identity theft, identity deception, identity fraud, gives deeper insights into their importance related to identity fraud crimes, such as, money laundering, illegal trafficking (people, drugs, weapons), and terrorism. Identity crimes are often associated with non violent ‘soft crimes’ and this may have been the cause of the time delay in appropriate specific identity fraud legislation being enacted in countries outside of the U.S. However, identity fraud’s relationship with money laundering, illegal trafficking (people, drugs, weapons) and terrorism, along with the identified organised crime perpetrator links, proves it is a pre-violent crime and legislative remedies need to be taken now. Since 11 September 2001, a significant number of countries have introduced specific legislation for anti-money laundering, illegal trafficking, and terrorism security. Specific identity fraud legislation in Australia at the federal level could also close off any loopholes and strengthen current related identity fraud legislation, such as anti-money laundering, and terrorism.

**Conclusion and Research Agenda**

The follow on effects of identity fraud attacks on IS, are that organisations in the short term decrease their internet commerce operations, reduce their online presence, or have resource constraints which place demands on expenses for security solutions (deterrence, prevention and detection). These systems include validation and identification devices to try and mitigate the identity fraud and related crime perpetrators attacks. The overall impact on target organisations includes a significant financial impact, likely reputational damage, increased burden passed onto customers and the potential flow-on effects including loss of business confidence and customer trust. All this is occurring when organizations, to the best of their
ability, are implementing current deterrence, prevention, and detection security measures (for a recent survey of measures see CyberSource 2007).

Research in-progress and future research initiatives include developing a comprehensive understanding of current digital identity fraud in e-commerce and internet solutions, validating proposed models and conceptual frameworks empirically, developing security solutions for identity fraud profiling and controls, initially with computational immunology techniques adapted from biology.

References


Dhillon, G., and Moore, S., “Computer Crime: theorizing about the enemy within,”


Vasiu, L., “A Conceptual Framework of E-Fraud Control in an Integrated Supply Chain,”
