Investigating ID Fraud in Australia: A Research Program

Rodger Jamieson\textsuperscript{a}, Kenneth Stevens\textsuperscript{a}, Peter Luckett\textsuperscript{b}, Kim Langfield-Smith\textsuperscript{c}, Warwick Sarre\textsuperscript{d}, Henry Pontell\textsuperscript{f}, Suresh Cuganesan\textsuperscript{f}, David Lacey\textsuperscript{f} and Michael Briers\textsuperscript{f}

\textsuperscript{a} School of Information Systems Technology and Management, University of New South Wales
Sydney, New South Wales, Australia, 2052
r.jamieson@unsw.edu.au, k.stevens@unsw.edu.au

\textsuperscript{b} School of Accountancy, University of New South Wales
Sydney, New South Wales, Australia, 2052
p.luckett@unsw.edu.au

\textsuperscript{c} Department of Accounting and Finance, Monash University
PO Box 197, Caulfield East, Victoria, Australia, 3145
kim.langfield-smith@buseco.monash.edu.au

\textsuperscript{d} School of International Business, University of South Australia
City West Campus, North Terrace, South Australia, Australia, 5000
Rick.Sarre@unisa.edu.au

\textsuperscript{e} Department of Criminology, Law and Society, University of California, Irvine
School of Social Ecology, Irvine, California, USA, 92697
hnpontel@uci.edu

\textsuperscript{f} SIRCA - Security Industries Research Centre of Asia-Pacific
Level 2, 9 Castlereagh Street, Sydney, New South Wales, Australia, 2000
suresh@sirca.org.au, dlacey@sirca.org.au, m.briers@sirca.org.au

Abstract

Identity fraud is recognised as a serious and significant problem in Australia by Government and industry, with estimates of losses ranging up to $4 billion per annum. This paper presents details of a research project which aims to research identity fraud from an organisational, information systems, and social perspective by investigating control, management and policy alternatives. Outcomes will include conceptual, effects and costing models of identity fraud, successful strategies for organisational management control, new techniques to improve prevention and detection, and comparative evaluations of social, legal and privacy implications. The research program will provide the missing research partnership that will inform control, management and policy decisions of national significance.

Keywords

Identity fraud, proof of identity, prevention, detection, correction,
Aims and Background

The aim of the research is to investigate and inform the control and management of identity fraud, a problem of growing national significance for both the private and public sectors in Australia. Using a series of cross-sectional interviews and focus groups, industry-wide surveys and in-depth qualitative fieldwork, this project applies a multi-disciplinary approach to a multi-dimensional problem: identity fraud and its perpetration, detection, prevention and management. Utilising Australian and United States data in particular, the objectives of the research program are to:

1. Develop a conceptual model to define the scope of identity fraud and its multi-dimensional impacts;
2. Identify the patterns of identity fraud and develop an explanatory model for the efficacy of prevention and detection strategies and activities that are currently being undertaken to manage identity fraud;
3. Develop activity-based costing methodologies to determine the cost of identity fraud both throughout the Australian business landscape and within individual organisations;
4. Determine appropriate structures and control systems that may be used to improve the prevention and detection of identity fraud; and
5. Examine the social expectation, legal and privacy implications of the various solutions available to policy-makers and contrast these with the United States which, arguably, is amongst the leaders internationally in terms of identity-fraud related policy.

Identity fraud is a sizeable and growing problem. Identity fraud involves either the theft of an existing person’s identity or the creation of a fictitious identity and the subsequent use of that identity to engage in fraudulent transactions, such as accessing loan finance or avoiding tax obligations. It has been claimed that identity fraud is the world’s fastest growing type of fraud, compromising the finance industry, global e-commerce, the collection of revenues and payment of benefits by governments, immigration, anti-terrorism, and law enforcement initiatives, such as criminal drug investigations (see General Accounting Office(GAO), 2002). In Australia, identity fraud is said to cost in excess of $4 billion per year, while in the United States (US) and United Kingdom the exact figures are in access of $8 billion per year (Main and Robson, 2001; GAO, 2002; and UK Cabinet Office, 2002). Furthermore numerous surveys (for example, Graycar, 2002; Main and Robson, 2001; and Walker 1997) confirm that the costs of identity fraud are on the rise.

While identity fraud is a significant problem for both private and public sector, it is also extremely complex to control and manage. One reason for this is the lack of standardised definitions (Matejkovic and Lahey, 2001). In addition, the diversity of methods of perpetrating, preventing, and detecting identity fraud adds to the complexity of the problem, with impacts in technology, management, regulation and criminology. Furthermore, identity fraud is difficult to monitor and record because it intersects with many other categories of crime (Chapman & Smith, 2001). This is partly due to the fact that the explicit recognition of identity theft, as a distinct category of fraud, is relatively recent. For these reasons, current approaches to identifying and countering identity fraud are fragmented, with individual organisations developing their own definitions of the problem and, consequently, isolated
solutions that yield little benefits. The first objective remedies a lack of conceptual clarity in the identity fraud construct and will explicate its multi-dimensional nature, potentially translating into a more integrative and cohesive response from Australian organisations and government.

The project team has already held some preliminary discussions with both public and private sector organisations, particularly from law enforcement, policy and the financial sector, to gauge the extent and forms of identity fraud. This has revealed that identity fraud involves both an acquisition and a use component. Common methods for acquiring alternative identities range from “dumpster diving” (retrieval of discarded documents), mail interception, social engineering of passwords, technological breaking of passwords, and wholesale hacking. Methods to create fictitious identities include the alteration of existing proof of identity (PoI) documents, creation of false PoI documents and the use of false identification details to acquire a legitimate (properly issued) but false PoI document. The “use” component is reflected in perpetrators using these false or stolen identities to commit a range of crimes including credit card fraud, bypassing immigration checks, creating fictitious organisations to evade tax or to launder money, and acquiring loans (Australian Federal Police, 2002). The second research objective is geared towards integrating current knowledge about identity fraud patterns and the development of a theoretical model that explains the effectiveness of various organisational responses in terms of contextual variables such as industry, control type and identity fraud type.

**Upstream Activities**

<table>
<thead>
<tr>
<th>Stage 1</th>
<th>Stage 2</th>
<th>Stage 3</th>
<th>Stage 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial issue of identity document</td>
<td>Use PoI to issue other documents</td>
<td>Use PoI and other documents to provide resources</td>
<td>Downstream activities involved in identity fraud management</td>
</tr>
</tbody>
</table>

**Organisational Examples:**

| Births, Deaths and Marriages (both Australian and Overseas) plus organisations involved in issues relating to individuals who may have lost, have stolen, or never had an established identity | Organisations, which, as part of their role in delivering services, create new documents which may come to serve as identifiers in their own right. RTA is one example. Based on identity check, creates a photo licence which can then be used as form of identity in other transactions. Other organisations would include Medicare, Tax Office (issues TFNs), utilities (accounts used in 100 points PoI). | Organisations that require some proof of identity when making decisions to provide financial or other resources to people. Resources are then at risk if the identity is fabricated or stolen. Financial institutions are the obvious example, but would include organisations such as the Tax Office (false returns), Centrelink, e-commerce, other agencies providing credit (e.g. retailers). | Once a fraud has been committed, aided by a stolen or fabricated identity, a number of agency can become involved, including Police Services, AUSTRAC, security and fraud sections of various organisations, and particularly those involved in the previous link of the “value chain”. |

Figure 1 – Organisational Players in the Management of Identity Fraud
A useful way of conceptualising the complexity of managing identity fraud is to view the various relationships as forming part of a “value chain” (originally developed by Porter (1985) in the context of strategic analysis). Adapted to the Australian identity fraud context, this model (see Figure 1) depicts the various organisations involved in activities related to establishing and relying upon evidence of identities. While the chain appears simple and linear there are many interdependencies amongst the parties involved. The high level of interdependencies between all organisations in the value chain has resulted in an awareness of the need to collaborate to control identity fraud. Hindering collaborative approaches, however, is the fact that, depending on their role, organisational objectives, interests and incentives relating to creating proof of identity documentation, verifying identities and transacting on the basis of identity documentation are likely to differ. Indeed, anecdotal evidence indicates that the costs and benefits associated with creating documentation to support a valid identity are likely to be unequally distributed across the various organisations in the value chain. However, there is a lack of academically rigorous evidence that identifies key sites of identity fraud cost incurrence. The third objective is aimed at accurately costing identity fraud both throughout the various stages of the value chain and within organisations to the individual activities that relate to identity fraud prevention, detection and response. This will enable a prioritisation of key areas for both public and private sectors and facilitate further debate on the need for collaborative approaches to the identity fraud problem.

The increased use of the Internet and the spread of electronic business (e-business) have undoubtedly played a large role in the growth of identity fraud. Both scholarly (eg. Smith, 1999; Graycar, 2002) and popular (eg. Lawrence, 2002; Taylor, 2002; and Lowe, 2002) authors argue that the Internet has dramatically altered the potential occurrence and impact of identity fraud. The Internet has increased access to the global publication of identification details that were previously unavailable to the public (both through legal and illegal means). Furthermore, the attraction for perpetrators in using the Internet as their medium is the sense of anonymity and potential reduction in the risk of being caught as compared with more traditional face-to-face transactions. Attempts have been made, both domestically and internationally, to raise awareness and develop countermeasures to this threat. One recent international example that has already influenced domestic practices is the “Wolfsberg Principles”, developed by the world’s leading international private banks to counter global money laundering. Acknowledgment of the need for greater due diligence with respect to the verification of clients’ identity is one strategy reinforced throughout (see Wolfsberg, 2000). Increasingly, the major international private banks require their smaller global partners (Australian banks included) to adopt these principles (see Hinterseer, 2001) and attest to the existence of effective identity fraud controls if their business relationships are to continue. Research conducted under the auspices of the fourth objective will investigate the effectiveness of extant control systems and the development of more effective prevention and detection techniques.

Within Australia, a large number of organisations play a role in the processes and activities associated with the management of identity fraud. This is recognised by the wide range of organisations represented on the AUSTRAC Steering Committee on Proof of Identity, a key industry partner in this project. In Australia, there is no one organisation with the policy-
making responsibility for identity fraud, with the closest being AUSTRAC (Australian Transaction Reports and Analysis Centre). Established through the enactment of the Financial Transaction Reports Act 1988, AUSTRAC is Australia's anti-money laundering regulator and specialist financial intelligence unit. Preliminary evidence indicates a number of impediments to a harmonised framework for identification issuance and authentication, including privacy legislation, jurisdictional boundaries between the Commonwealth and State governments and social expectations relating to identification. The fifth and final objective is to conduct research into the legal, social and privacy issues relevant to identity fraud policy solutions in Australia. International comparisons with the United States in particular will be conducted. The United States is arguably amongst the leaders internationally in developing responses to identity fraud, with specific data repositories for identity fraud hotlines set-up such as the Social Security Office’s – Office of the Inspector-General and the Federal Trade Commission’s Identity Theft Data Clearinghouse (in addition to legislative solutions enacted such as the Identity Theft and Assumption Deterrence Act 1998).

The following points summarise the current problems relating to identity fraud and the related objectives of the research program:

- There is a lack of consensus in defining and managing identity fraud, which contributes to the difficulty of identifying and managing the phenomenon – (Objective 1);
- Identity fraud is complex to manage, involving multiple methods of perpetration, prevention and detection - (Objective 2);
- The exact level of identity fraud is unknown, but it is believed to be widespread and hidden, and involves many organisations with different objectives and interests in managing the problem – (Objective 3);
- Identity fraud is growing as perpetrators discover new means such as the Internet. Concurrently, Australian businesses are forced to attest to effective identity fraud controls to maintain their global position – (Objective 4); and,
- Policy development in relation to identity fraud is difficult, with privacy, jurisdictional and social expectation implications – (Objective 5).

**Significance and Innovation**

Identity fraud is a significant and growing problem both in Australia and internationally, with some estimates of the cost in Australia up to $4 billion per annum (see Graycar, 2002; Main and Robson, 2001; and Walker, 1997). With the growing sophistication of information technologies, the opportunities for stealing identities or creating false ones are increasing. As the basis for many commercial and social transactions is premised on the belief that identity of the customer or client is genuine, failure to manage identity fraud effectively exposes individuals, businesses, governments and society in general to a wide-ranging set of damaging consequences. For example, it has the potential to undermine both national and global e-business efforts (e.g. e-procurement and on-line banking), and the confidence and trust the public places on government agencies to protect public revenues and safeguard society. Attaining a clear understanding of the issues involved and developing effective management strategies offer clear benefits to all parties.
The research program is innovative as this is the first time that the Australian identity fraud problem has been investigated in depth from both a conceptual and an applied viewpoint. Importantly, access to major stakeholders in Australia has been guaranteed, namely members of the AUSTRAC Steering Committee (e.g. peak government bodies, major banks), which provides a unique opportunity to study the issues from the perspectives of a diverse range of organisations. As these organisations play different roles in the process of managing and controlling identity fraud, an ability to understand and integrate their views, incentives and objectives better enables the development of comprehensive and cost-effective solutions. Further strengths of the project are the multi-disciplinary profile of the research team. The academic collaboration with fraud experts at the University of California (Irvine) will also enable the collection and analysis of data from the United States and the location of Australia within a global context across all objectives and, in particular, the final one. Overall, the research team will utilise their differing skills and expertise to develop and use a combination of research techniques including interviews, case analysis, survey fieldwork, simulation and modelling, tool and methodology development, and artificial intelligence techniques (e.g. data mining). This will provide an opportunity to influence significantly future standards and guidelines in this area, putting Australia at the forefront of identity fraud research and solution creation.

**Research Methods and Approach**

**Research Design**

The research involves a multi-method approach including the use of industry-based focus groups, cross-sectional interviews and surveys, in-depth qualitative fieldwork, analysis of participant databases, and use of activity based costing. To achieve the overall aim to investigate issues relating to the extent, control and management of identity fraud, and the more specific objectives, as outlined previously, the research program will be performed in modules that draw on the experience and skills of the research team. Importantly, the research team will provide training for more junior academics colleagues at the Universities involved in this research program, as well as research students, through extensive participation within each module. The five modules correspond with the five specific objectives outlined previously:

**Module 1: An Identity Fraud Conceptual Model**

This module will address the question “What is identity fraud?”, and will provide a foundation for the later modules of the research. Interviews will be held with managers in public and private sector organisations to identify similarities and differences in their views, and to define the multi-dimensional nature of the identity fraud construct. The research methods used to achieve this module will primarily involve a review of existing literature, interviews with key organisations and the conduct of focus groups.
Module 2: Patterns of Identity Fraud and Strategies of Detection and Prevention

This module will address the question “What are the patterns of identity fraud and what strategies are used to prevent and detect identity fraud?” Data relating to identity fraud occurrences obtained from various public and private sector organisations will be examined and analysed to establish identity fraud patterns, to provide an understanding of the nature of those patterns and their effects. This modelling will be used in later modules to develop tools and techniques that can be used to detect fraudulent identities. This work will also involve developing methodologies and heuristics to assist organisations to improve their identity fraud control systems. Attention will be drawn towards risk management, fraud control policies, reporting mechanisms, and effective training of staff. Through the analysis of the information provided, the research team will be able to develop and apply maturity models and organisational dimensions within and between the industries of focus (including the banking, finance and telecommunications industries). Importantly, the development and application of maturity models will provide insight into how identity fraud influences organisations and how they treat it in terms of control sophistication, management strategies, and reporting. The outcome will be to provide a way of modelling existing systems, which will assist management in understanding the business processes and management control structure of the system, and in identifying key points of vulnerability.

Interviews will be held with fraud experts and managers in organisations to identify identity fraud and their features. This data will be analysed, to develop a database of anonymous identity fraud cases. This analysis will also provide a validation of the identity fraud conceptual model that will help to inform the development of future models. Individual patterns will be detected by the use of data mining and artificial intelligence techniques, which will also aid in the development of models, heuristics and procedures (see Coderre, 1999), and provide a system of classification and measurement to support the second research objective.

Module 3: The Cost of Identity Fraud

This module will focus on “What is the cost of identity fraud?”, and involve the analysis of the costs and activities undertaken by organisations to manage and control identity fraud. Accurate cost information is needed to assess the effectiveness of identity fraud control activities to assist management in strategically managing the process. But as many of the activities and processes are likely to be distributed across the various functions and departments of an organisation, conventional costing systems are unlikely to provide the type of information needed to manage identity fraud. It is unlikely that organisations are aware of the “real cost” of identity fraud to their organisation, as activities occur across various function of the organisation and costs may be hidden in payroll and overhead accounts. Activity-based costing (ABC) and activity-based management (ABM) are methodologies that have been developed measure and manage costs more effectively in organisations (Langfield-Smith et al., 2002). These techniques will be used to develop accurate costing models to measure the costs of managing identity fraud and demonstrating how this information can be used to improve the management process.

A series of case studies of individual organisations will be conducted to identify the activities involved in managing identity fraud and to cost the activities. This will lead to the development of a taxonomy of the types of costs involved (such as prevention costs, detection
costs and failure costs) and the development of a generalised model for assessing and managing the costs of identity fraud across a variety of different organisations.

Module 4: Systems to Improve Prevention and Detection of Identity Fraud

This module addresses the question “What are the appropriate structures and control systems that may be used to prevent and detect identity fraud?” Research will be undertaken within target organisations to develop generic, but adaptable, fraud prevention, detection and correction models. Knowledge of the different systems and controls structures will be gained through the work performed on existing models and costing, in Modules 2 and 3.

One method that can be applied to understanding the internal and external complexity of identity fraud is semiotic modelling, which is an extension of conventional entity relationship modelling (Chen, 1976). Semiotic models extend entity relationship models by also modelling the pragmatics of relations. Rather than simply associating (business) entities in an untyped non-specific fashion, they are related in a functional manner (see Whobrey, 2000). In the past these additional “constraints” between entities where modelled, if at all, in a subsequent relational modelling analysis stage, but again this was mostly in an untyped fashion. In contrast, semiotic modelling permits the constraints between business entities to be described directly (Fetzer, 2000). For identity fraud, this is considered to be advantageous since it allows business processes to be more easily analysed in terms of the dependencies and influences of the relationships between the business entities involved. Consequently, the model can be readily inspected for security vulnerabilities and subsequently secured, if feasible or possible, through the introduction of suitable procedures (Will, 2000).

The more formal semiotic description (i.e. model) of the identity fraud domain acts as a foundation from which deductive and inductive observations can be made toward establishing either new or improvements to strategies for the prevention, detection and correction of identity fraud. To investigate how productive such strategy discovery will be, the relevant parts of a selection of the business processes of key stakeholders will be modelled semiotically and a methodology for strategy discovery developed. All data pertaining to the relations and behaviour of interrelated organisational functions (both internal and external) will be informed through a detailed understanding of the financial and resource distribution impacts of identity fraud on organisations and the strategies employed to manage the identity fraud problem in their organisations (i.e. following on from modules 2 and 3).

A key aspect that will be investigated in this module is how strong and effective control systems can be implemented in the light of the competitive positioning of modern organisations. Specifically, “How can an organisation design strong control systems that provide the appropriate level of assurance against identity fraud, while ensuring that key aspects of customer service are preserved or enhanced?” As organisations introduce customer transactions that are more technologically sophisticated, that can be brought to completion much faster, and that rely less on face-to-face contact, it becomes important to ensure that control systems are sophisticated enough to counter an increased risk of identity fraud. At the same time, increasing levels of competitiveness between organisations leads to a greater awareness of the need to enhance levels of customer service. Tight and intrusive control systems can act against achieving high levels of customer satisfaction. A series of case studies will be conducted in individual organisations and a risk management framework will be used to address both of these research questions. Managers will be interviewed to
determine how they make trade-offs between implementing tight controls, and preserving high levels of customer service.

Module 5: Social and Legal Ramifications

This module will address the question “What are the social, legal and privacy implications of identity fraud detection and prevention strategies?” While there is no tort of privacy recognised in Australia, Australians, like citizens of all democracies, have come to expect that their lives will be free from unwarranted intrusions and inappropriate surveillance.

This stage of the project will address the issue of appropriate legal protections of privacy, and explore the dilemmas associated with finding the optimal balance between freedom from identity fraud and freedom from breaches of privacy based upon the results and models developed from the preceding modules. Through determining the organisational and societal implications of identity fraud occurrences, the refinement, application and testing of various alternative models relevant to policy makers will be explored and considered in terms of these ‘balances’.

Engaging with key State and Commonwealth policy developers and stakeholders will be undertaken through interviews and on-site data collection activities in order to conduct a series of policy reviews and comparative work to evaluate the impact of potential prevention, detection and countering solutions on the Australian legal framework and the relevant social implications from a privacy perspective. The methodology to be applied will be informed by both national and international collaborators. Through the participation of the North American identity fraud experts, the extension of the analyses undertaken to incorporate overseas policy developments has the potential to give Australian policy-makers the opportunity to take a leading global role in relation to identity fraud. The research undertaken to provide a taxonomy of different methods, controls and management policies implemented as a result of identity fraud will be compared and contrasted to findings within key sectors of the United States. This will inform the research and analysis of key policy alternatives applicable to Australia.

Research Subjects

The AUSTRAC Steering Committee on Proof of Identity Fraud (AUSTRAC 2001) has been a key player in government initiatives on identity fraud, and was established to examine proof of identity processes in Australia’s public and private sectors. The AUSTRAC Steering Committee and its member organizations where appropriate and where the law permits will provide access to their personnel, databases and other information resources. The research team will draw on considerable expertise in the provision of research and thought leadership with respect to identity fraud from organisations represented on the Committee. This will include access to their information systems and data mining technologies, control mechanisms, and reporting infrastructure, which will be utilised for survey/benchmarking purposes, survey methodology and conceptual frameworks for adaptation and integration for the purposes of this project. The association with member organisations, which will be built up through this project, is expected to lead to further future collaborations, particularly as Australia emerges as a lead nation in preventing and countering identity fraud.
National Benefit of the Research Program

During 2001 Australia issued around 145,000 passports, 249,600 birth certificates, and lodged more than 3.5 million new Centrelink claims (Australian Bureau of Statistics, 2001; Centrelink, 2002; and Department of Foreign Affairs and Trade, 2002). Each of these three types of events requires more than one pre-existing form of identification or another. These are just three examples from a diverse and complex identification systems within Australia that are exposed to the threat of identity fraud. Prior studies have estimated that the total cost of identity fraud to Australia per year may be up to $4 billion per annum. The research program described provides Australia with a multi-disciplinary team of experts (both from within Australia and overseas) who have a unique insight into many areas of direct relevance to combating this phenomenon. The commitment made by the members, and the organisations they represent on the AUSTRAC Steering Committee, is evidence of the potential benefits Australia can gain from this research program. In addition to investing the extent, control and management of identity fraud, the direct benefit to Australia is the provision of an identity fraud effects model that is able to determine the impact of proposed alterations to the control and management techniques designed to prevent and counter identity fraud occurrences. The uniqueness of this model will result in a world’s first that is hoped to be applied throughout both public and private sector organisations within Australia and around the world. This will allow organisations to better understand the impact of their resource allocation choices and allow for the cost-effective testing of alternative decisions.

Progress to Date

A large ARC research linkage grant has been awarded to the researchers to investigate the five objectives of this research program. An initial investigation of the costs of ID fraud is currently underway with the AUSTRAC POI Steering Committee with the results due at the end of July 2003. Initial interviews have been held with representatives from key members of the AUSTRAC POI Steering Committee to provide an insight into the extent of the problem. These have provided further direction for the research team. Investigations are underway into potential solutions to the problem including biometrics, and work has commenced on investigating and building systems to provide a semiotic representation of business systems to determine weaknesses. Detection systems are being investigated including data mining and computational immunology. This research program will run for four years and at the end should provide organisations with a good understanding of the problem and methods of helping to prevent, detect and correct/recover from ID fraud attacks.

References


Australian Transactions and Analysis Centre (2001), Cost of Identity Fraud, AUSTRAC Steering Committee on Proof of Identity.


