December 2004

Investigating the role of Profiling in the Detection and Prevention of Identity Fraud

Krish De  
*University of New South Wales*

Kenneth Stevens  
*University of New South Wales*

Follow this and additional works at: [http://aisel.aisnet.org/acis2004](http://aisel.aisnet.org/acis2004)

Recommended Citation

[http://aisel.aisnet.org/acis2004/69](http://aisel.aisnet.org/acis2004/69)
Investigating the role of Profiling in the Detection and Prevention of Identity Fraud

Krish De
Kenneth J Stevens

SEAR: Security, E-Business, Assurance Research Group
School of Information Systems Technology and Management
University of New South Wales
Sydney, NSW, 2052, Australia
Email: k.stevens@unsw.edu.au, http://www.sear.unsw.edu.au

Abstract
Identity (ID) Fraud is a global issue that affects all aspects of society. There are also very serious financial costs: if the problem continues unabated, the worldwide costs will reach $US 2 trillion by the end of 2005. Various profiling techniques are already being successfully used in industry and law enforcement and it is the aim of this research to investigate the utility of these techniques for the detection and prevention of ID Fraud.

Keywords
Identity Fraud, Profiling

INTRODUCTION
Identity fraud (ID fraud) is a complicated issue in the complex domain of fraud that has gained the attention of law enforcement, regulatory bodies, commercial interests, academia and the general public. ID fraud is a problem because it is difficult to detect and even more difficult to apprehend the perpetrators. It is a component of almost every major crime and its presence is felt throughout the world (Gordon & Willox, 2003). ID fraud is a significant Information Systems (IS) problem due to the key role of facilitation that IS has in the domain, as highlighted by a report on the changing nature of fraud in Australia (Office of Strategic Crime Assessments, 2000):

“Technology has weakened the integrity of many identifiers currently in use – birth certificates can be reproduced using desktop publishing software; counterfeit passports and counterfeit smartcards can be purchased over the Internet. Easier access to these false identifiers facilitates a range of fraudulent behaviour, including tax evasion, immigration malpractice, fraudulent claims against social security and health insurance companies. It also assists in hiding the proceeds of frauds.”

The detection and prevention of ID fraud is of vital significance as its impacts are society wide. Individuals face the risk of offenders assuming their identities in order to use their credit cards or obtain loans, goods and services in their victim’s name. These activities have left many ID fraud victims with destroyed credit ratings and large debts. (Gordon & Willox, 2003). Businesses face the liability of selling goods and services to fraudsters as well as the risk of fraudsters obtaining business loans in their names. Governments face the issues of illegal immigrants entering the country with counterfeit identities, the organised fraud of state benefits and the threat of terrorists entering the country (Cabinet Office, 2002). Apart from the considerable social cost, ID Fraud has very significant financial costs. The Aberdeen Group (2003) estimated a worldwide loss of $US73 billion in 2002 and a further estimated loss of $US221 billion for 2003. If the problem continues unabated, it will cause losses of $US2 trillion by end of 2005.

LITERATURE REVIEW

ID Fraud

Simply stated, ID fraud is defined as “the gaining of money, goods, services or other benefits through use of a false identity” (Etter, 2004). It is an underexposed problem, as highlighted by a lack of criminal and civil regulation in Australia. Only South Australia, through laws soon to come into effect, considers the theft or assumption of an identity to be a mainstream criminal offence (Etter, 2004).

Most research concerning ID fraud has concentrated on definitional aspects (Etter, 2004), the evaluation of extent of the problem (Graycar & Smith, 2002; OSCA, 2000 and Cuganesan & Lacy, 2003), studies of
practitioner responses (Gordan & Willox, 2003) or the need for governmental and legislative regimes (OSCA, 2000; US Federal Trade Commission, 2003 and Cabinet Office, 2000). Little, if any, academic research has focused specifically on how ID fraud is detected or prevented.

Within Australia, ID fraud is at the centre of a major research initiative being driven by the Securities Industry Research Centre of Asia-Pacific (SIRCA). SIRCA is a not-for-profit financial services research organisation involving twenty-six collaborating universities, various industry partners and government agencies across Australia and New Zealand (SIRCA, 2004). Their research has focussed on the impact of identity fraud and the extent and type of organisational responses. It also provides an estimate of the total cost of identity fraud to Australia and presents new and innovative ways to assist practitioners and researchers in better understanding the impact of this type of crime at a national level (Cuganesan & Lacey, 2003).

Most ID fraud research has taken a ‘bottom-up’ approach, with most studies adopting a single perspective of a key stakeholder group, such as a victim perspective (Graycar & Smith, 2002), a law enforcement perspective (Etter, 2004) or a government perspective (OSCA, 2000 and Cabinet Office, 2000). A ‘top-down’ approach has also been used. Malkedsuw & Stevens (2003) adopted a ‘process’ perspective and found the holistic view afforded by the approach to be valuable in understanding the organizational response to ID fraud.

The preliminary research model adopted in this research includes elements of both a top down and a bottom up approach. The model is an adaptation of Graycar & Smith’s (2002) model of crime, which views ID fraud as a crime.

![Figure 1: A “crime” model of ID Fraud (adapted from Graycar and Smith, 2002)](image_url)

The model is based on the principle that ID fraud, like all crimes, is the product of (a) Motivation – somebody willing to offend; (b) The presence of prospective targets or victims and; (c) The absence of a capable guardian, as depicted in Figure 1. This approach is advantageous because it allows for a systematic analysis of the possible applications of profiling, not only at a holistic level but also at a component level.

**Profiling**

Profiling, in the broadest sense, is defined as a family of multi-factor screening or file analysis techniques that are used to identify instances that match a predetermined characterisation (Clarke, 1993 and Marx & Reichman, 1984). The instances and predetermined characterisations are dependent on the application of profiling; for example, in offender profiling, the instances are suspects and the predetermined characterisation is the offender profile. Appendix 1 summarises the families of profiling identified from the literature.

Information Systems (IS) are used extensively in profiling in a variety of functions: database management systems are used to store the large amounts of data collected (Holmes & Holmes, 2002), specialised applications such as CGT (Rossmo, 2000) are integral to processing data for profiling and computer networks are essential in communicating the results of profiling (Holmes & Holmes, 2002).

Profiling techniques can be classified into two broad families: criminal and customer profiling. The criminal profiling family of techniques include offender, victim and geographic profiling. **Offender profiling** relies on the notion that behaviours and characteristics left at a crime scene allows for inferences to be made about the likely offender (Canter & Heritage, 1990, Marx & Reichman, 1984 and Geberth, 1981). Similarly, **victim profiling** involves studying the victim’s behaviours and characteristics to allow inferences to be made about the offender also (Holmes & Holmes, 2002). **Geographic profiling** uses the offender profile and the investigation of the crime site(s) to determine the most likely residence of the offender (Rossmo, 2000).
The Customer profiling family of techniques includes abstract and personal customer profiling, use of geo-demographics and use of psychographics. Abstract profiling describes a general class of person for comparison purposes against a larger dataset to identify potential customers (Clarke, 1993) whereas a personal profiling involves the accumulation of data concerning a particular individual for the purposes of personalised advertising (Wiedmann, Buxul & Walsh, 2002). Geo-demographics are used to segment and cluster individuals into groups by their geographic location through use of Geographic Information Systems (GIS) for the purposes of targeted advertising whereas psychographics profile consumers into abstract groups based on their lifestyle (activities, interests and opinions) and then cluster them into potential markets through use of GIS (Mowen & Minor, 1998).

**Theory Development**

Little evidence exists in literature regarding the use of profiling for the detection and prevention of ID fraud. It could be argued that the nature of profiling is such that organizations undertaking profiling are unwilling to allow the practices and techniques to become public. Dilution of the effectiveness of profiling (as perpetrators become aware of the variables and sensitivity of profiling algorithms), and the public’s perception of the unethical nature of profiling practices are both plausible concerns that may inhibit an organization’s participation in research. It is felt however that the desire to capitalise on the deterrent effect which would occur through the awareness of the use of these techniques would outweigh these concerns. The conclusion drawn from the lack of literature is that, within the commercial arena at least, the use of profiling to detect and prevent ID fraud is not widespread.

Based on an analysis of the profiling methods identified in the literature review as applied to the preliminary research model of ID fraud, it would seem that the use of profiling would be of high utility in detecting and preventing ID fraud. The most likely barriers to use of profiling include privacy issues and the technological feasibility of profiling systems.

Thus the primary goal of this research is to report on whether or not profiling is being used to address ID fraud and why this is the case.

**PROPOSED RESEARCH METHOD**

The use of profiling techniques may well hold the key to detecting and preventing ID fraud and thus reducing the problem. This research will take the form of a “mini” case study based on the content analysis of semi-structured interviews with the research organisation. The research organisation is a specialist in dealing with ID fraud and leads an industry initiative with its client organisations in combating ID fraud.

With assistance from the research organisation, it is hoped that each profiling technique identified in the literature review will be explored with regards to the possible applications of the technique to detecting and preventing ID fraud; the data, processing and resource requirements and the limitations or barriers to use of the technique.

It is also hoped that the results of this preliminary work may lead to candidate techniques which will be investigated further and be refined. From this, tools may be built and tested within a larger, ongoing ID fraud research effort, of which this research is part.

**SIGNIFICANCE AND CONTRIBUTION OF RESEARCH**

This research is significant as it adds to the limited body knowledge to the field by providing a systematic view of profiling and its applications. We hope to enhance our research model by filling in the links between the profiling techniques and each of the elements of ID fraud and perhaps investigate if a mix of different profiling techniques would beneficial to maximise detection and prevention of ID fraud. By involving industry partners in our research process we hope to aid our industry partners in refining their techniques. If successful, the research will also provide contributions to industry by assisting organisations in understanding the different applications of profiling and by raising the awareness of ID fraud.

**CONCLUSIONS AND LIMITATIONS**

This research aims to investigate profiling as a technique that seems to be promising in the detection and prevention of ID Fraud. By investigating profiling techniques from outside the realm of IS, we hope to provide some recommendation as to the utility of the adaptation of these techniques to detect and prevent ID fraud.
This research is faced with one major limitation in that the access to information is fairly limited. First and foremost is that profiling techniques are often proprietary knowledge, which means that organisations are rightly unwilling to divulge the techniques for fear of losing competitive advantage. Secondly, it is quite likely that governments will be reluctant to share any profiling techniques they use, for example in immigration or state welfare, as there may be a potential for reverse engineering to find means to avoid detection by these applications.

REFERENCES


Rossmo, K, (2000), Geographic Profiling, CRC Press LLC, USA.

## APPENDIX 1:
### Taxonomy of Researched Profiling Techniques (based on the literature review)

<table>
<thead>
<tr>
<th>Family</th>
<th>Name</th>
<th>Context</th>
<th>Type</th>
<th>Extent of Computerisation</th>
<th>Basis</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criminal Profiling</strong></td>
<td>Offender Profiling</td>
<td>Behaviours and characteristics left at crime scene allows for inferences to be made about the offender.</td>
<td>Behavioural, Demographical and Personality-based</td>
<td>Medium to Low</td>
<td>Psychology and Behavioural Science</td>
</tr>
<tr>
<td><strong>Criminal Profiling</strong></td>
<td>Victim Profiling</td>
<td>In a similar process to offender profiling, compiling a profile on the victim also allows inferences to be made on the offender.</td>
<td>Behavioural, Demographical and Personality-based</td>
<td>Medium to Low</td>
<td>Psychology and Behavioural Science</td>
</tr>
<tr>
<td><strong>Criminal Profiling</strong></td>
<td>Geographic Offender Profiling</td>
<td>The examination of the crime scene(s) in conjunction with the offender profile may indicate the potential residence of the offender</td>
<td>Behavioural, Demographical and Personality-based</td>
<td>High</td>
<td>Psychology, Behavioural Science and Statistics</td>
</tr>
<tr>
<td><strong>Customer Profiling</strong></td>
<td>Abstract Customer Profiling</td>
<td>An abstract profile describes a general class of person for comparison purposes against a larger dataset to identify potential customers</td>
<td>Personality-based</td>
<td>High</td>
<td>Marketing and Statistical</td>
</tr>
<tr>
<td><strong>Customer Profiling</strong></td>
<td>Personal Customer Profiling</td>
<td>A personal profile is an accumulation of data concerning a particular individual for the purposes of personalised advertising</td>
<td>Behavioural and Demographical</td>
<td>Very High</td>
<td>Marketing and Data Surveillance</td>
</tr>
<tr>
<td><strong>Customer Profiling</strong></td>
<td>Geo-demographics</td>
<td>Demographics are used to segment and cluster individuals into groups by their geographic location through use of Geographic Information Systems (GIS) for the purposes of targeted advertising</td>
<td>Demographical</td>
<td>High</td>
<td>Marketing and Statistics</td>
</tr>
<tr>
<td><strong>Customer Profiling</strong></td>
<td>Psycho-graphics</td>
<td>Consumers are profiled into abstract groups based on their lifestyle (activities, interests and opinions) and then clustered into potential markets through use of GIS</td>
<td>Demographics, Behavioural and Personality-based</td>
<td>High</td>
<td>Marketing, Psychology and Statistics</td>
</tr>
</tbody>
</table>

---

**COPYRIGHT**

De and Stevens © 2004. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.