This is the published version of:


Copyright:

Publisher version archived with the permission of the publisher Macquarie Graduate School of Management, Macquarie University, NSW, Australia. This archived copy is available for individual, non-commercial use. Permission to use this version for other uses must be obtained from the publisher.
IN THIS ISSUE

The Decision to Enter Voluntary Administration: Timeley Strategy or Last Resort
   J. Routledge

Organisations, Control Systems and Fraud
   S. Cuganesan & D. Lacey

Taxation of Infrastructure
   G. Mackenzie

Does Competition Drive Credit Risk and Performance in Financial Services Lending?
   An Australian Investigation
   J. Donato

Tyrone M. Carlin          Joint Editors          Guy Ford
The Journal of Law and Financial Management is a refereed Journal. Every manuscript submitted to the journal is subject to review by at least one independent, expert referee.
The Decision to Enter Voluntary Administration: Timeley Strategy or Last Resort

J Routledge

One of the options available to directors of financially distressed companies is to place their company into voluntary administration (VA). The decision to enter VA should enhance corporate governance because it allows for informed decision-making about a company’s future, and ensures that administration of a company’s affairs proceeds in an orderly manner. Once in VA, a company has a short ‘breathing space’ during which it can develop a strategy to address its insolvency. The strategic options available will be significantly affected by past performance and current financial position. If the company’s position has deteriorated significantly, the VA process will merely delay an inevitable liquidation. Therefore, a timely decision about entering VA is critical to the effectiveness of the procedure. This paper attempts to shed some light on the timeliness of the decision to enter VA. It presents an exploratory empirical examination of the change in financial characteristics for a sample of listed public companies over the critical time immediately prior to VA. The analysis focuses on how the changes that are observed affect prospects for reorganisation. The results suggest that the sample companies’ prospects for reorganisation were significantly diminished in the time prior to VA, and that directors should have taken more timely action.

Organisations, Control Systems and Fraud

S Cuganesan & D Lacey

This paper examines how organisations are responding to the threat of identity fraud and the challenges that they face in doing so. Quantitative data were collected from 29 Australian organisations. The majority of organisations sampled emphasised the ‘anticipation’ of identity fraud and, in particular, activities performed in relation to prevention, deterrence and detection. Furthermore, organisations with more sophisticated preventative controls reported lower losses. Counter-intuitively on first glance, organisations with higher detection capabilities reported higher losses (other things being equal). The contributions of this paper are two-fold. Firstly, a framework is presented that both operationalises the identity fraud construct and facilitates the measurement and understanding of organisational responses in terms of a ‘value-chain’ of activities. Secondly, exploratory evidence is presented on how organisations are responding to identity fraud and the efficacy of these responses.

Taxation of Infrastructure

G Mackenzie

Infrastructure in Australia is under strain from two influences. First, the existing limited infrastructure is unable to keep pace with economic growth and, secondly, the demand for health and welfare infrastructure because of an ageing population. There are no special rules for the taxation of infrastructure in Australian taxation law, except in very limited circumstances. The taxation of infrastructure assets is governed by the general taxation rules that apply to all other similar types of assets. However, what can be said about infrastructure taxation is the number of anti tax avoidance rules that it has attracted.

Does Competition Drive Credit Risk and Performance in Financial Services Lending? An Australian Investigation

J Donato

Increased competition in the Australian lending market over recent years has forced authorised deposit-taking institutions (ADIs) to attract and retain customers by means of relaxing lending standards. As larger amounts are granted, it appears credit is more easily available to borrowers in comparison to the past. The industry has further experienced significant growth in non-conventional products, such as low-documentation loans, which are generally offered at rates close to the standard rate for traditional loans. While these changes may not create problems during times of strong economic conditions, they are likely to exacerbate loan losses if economic conditions deteriorate, as it seems as if ADIs have taken on more risk in order to stay competitive. The aim of this paper is to examine how lending market competition affects banking institutions’ credit risk and performance within Australia. Thus, I hypothesise that increased competition leads to a rise in credit risk and that increased competition tends toward a reduction in performance, I test these hypotheses using linear regression.
At the time of writing, it appears that the global economic system is in the grips of a massive shock. Debt capital markets are not functioning as they have functioned over the past half decade, liquidity is tight and credit, where it can be obtained, is becoming increasingly costly. Though the global default and bankruptcy rate has been at record lows over the past three to four years, the re-emergence of inflation, capital market disruptions and an apparent move towards recession in the U.S economy seem to represent a suite of forces likely to drive bankruptcy and corporate insolvency rates higher.

This being so, James Routledge’s article on decisions relating to the entry into voluntary administration is particularly timely. James has a track record of providing insightful critiques into the operation of aspects of Australia’s corporate insolvency regime, and his latest work on the subject only goes to further establishing his credentials as a key thought leader in the area.

In a climate where financial institutions are facing considerable liquidity and funding pressure (not to mention political pressure in relation to rate setting), Josephine Donato’s analysis of the impact of competition on credit risk and performance in financial services lending is also timely and interesting.

Gordon Mackenzie has contributed a very interesting piece pertaining to the taxation of infrastructure, a vital and growing asset class, while Suresh Cuganesan and David Lacey provide a thought provoking discussion of issues pertaining to control systems and fraud, a perennial concern of any well governed organisation.

Tyrone M Carlin & Guy Ford, Sydney

December 2007.
Organisations, Control Systems and Fraud

By Suresh Cuganesan*
Macquarie Graduate School of Management, Macquarie University

and

David Lacey
Macquarie Graduate School of Management, Macquarie University

Abstract

This paper examines how organisations are responding to the threat of identity fraud and the challenges that they face in doing so. Quantitative data were collected from 29 Australian organisations. The majority of organisations sampled emphasised the ’anticipation’ of identity fraud and, in particular, activities performed in relation to prevention, deterrence and detection. Furthermore, organisations with more sophisticated preventative controls reported lower losses. Counter-intuitively on first glance, organisations with higher detection capabilities reported higher losses (other things being equal). The contributions of this paper are two-fold. Firstly, a framework is presented that both operationalises the identity fraud construct and facilitates the measurement and understanding of organisational responses in terms of a ’value-chain’ of activities. Secondly, exploratory evidence is presented on how organisations are responding to identity fraud and the efficacy of these responses.

Key Words: Identity fraud, Performance measurement, Performance management.

1. Introduction

Recent and prominent corporate collapses have made fraud response foremost upon the agenda of organisations, regulators and policy formulators. Subsequent research on fraud prevention and detection has focused primarily on financial statement fraud (for example, Braun, 2000; Knapp and Knapp, 2001; Rezaee, 2005). This paper contends that organisations face another pressing fraud problem; the prospect of identity fraud. Available evidence indicates that this form of criminality is significant and wide-ranging, with current assessments of its impacts against businesses exceeding billions of dollars each year (Cabinet Office, 2002; Cuganesan and Lacey, 2003; General Accounting Office, 1998; , 2002). In the United States (US), for example, identity theft is described as growing at a rate of 30% per annum, with its losses estimated at reaching US$8 billion by 2005 (Supreme Court of the State of Florida, 2002). In the United Kingdom (UK), identity fraud has been estimated as costing GBP 1.3 billion (Cabinet Office, 2002). While its impact is sizeable, the role of organisations in responding to identity fraud has been largely overlooked in the literature to date (for an exception, refer to Lacey and Cuganesan, 2004).

Despite the importance of identity fraud as a threat, prior research has been largely descriptive, enumerating identity theft cases often as a precursor to discussions about potential solutions (for example, Givens, 2000; Graycar and Smith, 2002; Moore, 2002; Willox and Regan, 2002). An alternative strand of research has considered the role of governments and, in particular, the relevance of existing legislative provisions and the efficacy of penalties towards identity fraud (Matejkovic and Lahey, 2001; May, 2002). While governments consider a variety of responses ranging from increased data matching to the issuance and use of national identity cards, overlooked has been the role of organisations in responding to identity fraud, with significant questions remaining about how commercial businesses and government agencies can better manage their performance in combating identity fraud.

This paper presents initial exploratory evidence from Australian organisations on their response to identity fraud. In so doing, a framework for analysing identity fraud response is developed in terms of a ’value-chain’ of activities performed. Results from data collection at 29 of Australia’s public and private-sector organisations are then presented. This involves information on the value-chain of activities performed by organisations in responding to identity fraud and the associated losses. The paper ends with a discussion of the challenges for organisations in controlling identity fraud, together with areas for further research.

2. Identity Fraud Response: A Framework For Analysis

2.1 The Identity Fraud Construct

Prior research on identity fraud has largely been driven by government and government-sponsored agencies. Overseas examples of government agencies and their work on identity fraud include the UK Cabinet Office (2002), and the US GAO reports (1998; 2002). Within Australia, a dearth of publicly available government research exists, with an exception being Main and Robson (2001), an abridged version of a non-public report on identity fraud risks to Commonwealth agencies. More ‘academic’ research has focused on legislative and regulatory ‘solutions’ (Matejkovic and Lahey, 2001; May, 2002). Due to its formative nature, prior research on identity fraud has yet to...
empirically investigate the role of organisations in responding to identity fraud. In addition, its nature can be characterised as fragmentary.

For example, previous identity fraud studies have utilised a multitude of different definitions. Identity fraud has been variously defined as an "individual falsely representing him or herself as either another person or a fictitious person to an organisation for some benefit" (Main and Robson, 2001), involving "the illegal use of personal identifying information…to commit financial fraud" (General Accounting Office, 1998), and arising "when someone takes over a totally fictitious name or adopts the name of another person with or without their consent" (Cabinet Office, 2002). Each defines identity fraud differently, the first focusing on the use of real or fictitious identities for benefit, the second for financial benefit, and the third different again, being the use of another person’s name only, but for any purpose. More recently, identity fraud has been conflated with identity theft (BITS Fraud Reduction Steering Committee, 2003). It is perhaps for this reason that estimations of identity fraud’s impacts have been so disparate2.

Hence, a limitation of extant understandings of identity fraud comprises the absence of conceptual clarity as to the identity fraud construct. In responding to this need for conceptual development, we develop three broad operationalisation principles of the identity fraud construct based on both a review of prior literature and the conduct of workshops and focus-groups comprising industry practitioners that had first-hand experiences of identity fraud (Cuganesan and Lacey, 2003). These principles comprise method, objectives and context, and are discussed in turn below.

2.1.1 Identity Fraud - Method

Identity fraud can involve the adoption or use of a fictitious or stolen or altered name. Stolen names can involve the unauthorised use of the identity of living or deceased persons, while altered names can involve either the use of legitimate but previously known names, or variations of the existing name that occur due to data entry error when interacting throughout the community. Furthermore, when considering transactions in the electronic world, identities begin to broaden beyond name to also involve other unique identifiers such as Personal Identification Numbers (PINs), passwords and other knowledge-based identifiers.

A further complication is the concept of identity. Arguably identity fraud can relate to most frauds, such as misrepresenting employment history or income level. However, much of the debate surrounding identity fraud focuses on something more fundamental than misrepresenting the circumstances of an identity. To distinguish identity fraud from broader fraud, the misrepresentation of an individual or entity’s attributable and biographical details by themselves alone, such as address and date of birth/registration, is outside the scope of the study’s identity fraud conceptualisation. It is, however, possible for identity fraud to occur should a culmination of attributable and/or biographical details infer that an identity is being impersonated.

2.1.2 Identity Fraud - Objectives

The objectives of the identity fraud perpetrator are many and varied. For example, identity fraud can result (if successful) in direct financial gain, appropriation of services, avoidance of payment or financial loss, and intangible benefits, such as access to citizenship, professional affiliation and medical services, to name but a few. Identity frauds can also feature and facilitate other criminal acts such as drug trafficking and people-smuggling. The objectives of a perpetrator’s actions can thus be categorised as including the financial gain and/or appropriation of services, the avoidance of financial loss, and/or a non-financial but subversive motive. Importantly, intent needs to exist at the time of the fraudulent event for it to be labelled as an identity fraud, be it the provision of a service or benefit or the issuing of an identity document. Mere receipt of an identity token, such as a driver’s licence that contains spelling mistakes with respect to name does not mean that the holder is an identity fraud perpetrator. Furthermore, cases where an alteration of an identity occurs for bona fide purposes, such as for aliases and witness protection schemes are also considered to be outside the bounds of identity fraud.

2.1.3 Identity Fraud - Context

Identity fraud can manifest in two distinct contexts in relation to organisational impacts. The first involves the creation of a new relationship between the identity fraud perpetrator and the organisation. Examples of this include applications for a new account, a new facility, or a new benefits stream through the use of fictitious, altered or stolen identities where the identity has not been presented to the organisation before. The second involves the appropriation of an existing relationship between a real identity and the organisation by the identity fraud perpetrator, an example of this includes the impersonation of an account holder to draw cash benefits. A requirement here is that of an explicit act of impersonation, such as stolen credit cards that require the signing of another person’s name (i.e. the original card holder’s signature). Excluded are acts of card skimming on blank cards where no act of impersonation exists. Otherwise, too broad an interpretation of identity fraud results. Thus, skimming of account details onto blank credit cards, the use of telephones in a break and enter, and the theft of utility services through meter tampering are considered outside the scope of the identity fraud construct.

2.2 Managing Fraud Response: The Value-Chain of Activities

In addition to operationalising the identity fraud construct, a means of characterising and evaluating organisational responses is also required. To this end an activity value-chain framework was developed (refer to Cuganesan and Lacey, 2003). We contend that the response of organisations to identity fraud can be distilled into two main categories3. Firstly, there are those activities undertaken in anticipation of identity fraud. Here there is an acknowledgment that identity fraud is a risk to the organisation and a proactive response is entered into. Secondly, there are activities that only occur in reaction to a specific instance of identity fraud being committed against the organisation4. Within each of these anticipatory and reactionary configurations are individual activities as presented in Figure 1. Figure 1 defines these activities and provides examples of where they may be applied by organisations in response to identity fraud. Of note is the positioning of risk assessment activities as outside of the anticipatory and reactionary classification scheme. This is because risk assessments can relate (and often do) to both activity categories. Hence, it is not classified exclusively as an anticipatory or reactionary activity in Figure 1.
Thus an organisation in responding to identity fraud can decide where to allocate resources and which activities to emphasise in managing performance. Broadly, a ‘proactive’ or ‘reactive’ stance (or a combination of both) can be taken. A pure reactive stance implies that the organisation is not attempting to improve its business processes in relation to identity fraud, and is potentially reliant on third parties to inform it of identity fraud events. Here, an organisation’s resource spend occurs in investigating events, recovering amounts lost and restoring any reputational losses, and is driven by the level and impact of the specific identity fraud events that have occurred. Conversely, a proactive approach would see the majority of investment being incurred independent of specific identity fraud events. Here, the emphasis is on strengthening business processes through risk assessments, prevention and deterrence whilst also engaging in ‘stress-testing’ these processes through detection activity. It is important to note that within both of these ‘proactive’ and ‘reactive’ configurations, different levels of emphasis can be placed on individual activities.

In terms of normative prescriptions on ‘appropriate’ configurations of the fraud response value-chain, more work within the fraud and identity fraud research disciplines is required. However, insights into the configuration of these fraud response value-chains may be generated through reference to the cost-of-quality literature (Juran, 1962; Roth and Morse, 1983; Schneiderman, 1986; Shank and Govindarajan, 1994). This literature categorises costs associated with product quality into four; namely, prevention (costs incurred to avert defects occurring), appraisal (costs incurred in identifying defects), internal failure (costs associated with correcting defects identified prior to customer delivery) and external failure costs (costs associated with correcting defects subsequent to customer delivery). While an argument in this literature has been that an optimal level of conformance exists which minimises total quality costs (Juran, 1962), this approach has been criticised because it underestimates the true impacts of external failure on customer satisfaction, market share and organisational reputation (Deming, 1986; Schneiderman, 1986). Instead, a ‘zero defects’ approach is prescribed where it is argued that investments in prevention activities are returned several-fold through lower failure costs (Shank and Govindarajan, 1994), with the next best alternative for enhanced performance being a focus on detection (Roth and Morse, 1983).

Applied to fraud and identity fraud, these arguments suggest that the greater the resource spend on anticipatory activities, the better will be the organisation’s performance in combating identity fraud. Specifically, prevention activities offer the most ‘value’ in terms of reducing the impact of fraud and failure costs. Here, failure costs as per the costs-of-quality literature is equated in the identity fraud context to the costs of investigation, recovery and restoration activities, together with the net identity fraud losses sustained by the organisation. Furthermore, detection activities should be emphasised next in terms of isolating suspicious or fraudulent events before

- **Risk Assessment**: Activities that relate to the prioritisation and identification of identity threats. This excludes the actual implementation of controls. Can have an anticipatory and/or reactionary focus.
  Examples: threat evaluations and risk estimates; periodic risk reviews.

- **Prevention and Deterrence**: Activities related to strategy, policy and procedural development and implementation to avoid an identity fraud being perpetrated. Also includes activities related to the promotion/communication of disincentives to commit identity fraud acts.
  Examples: research and development for enhancement of identity documents/tokens; training of staff; media campaigns, communications of penalties for committing identity fraud; and front-office validation of identity documents/tokens.

- **Detection**: Activities related to the discovery of anomalies/events that may warrant further investigation.
  Examples: database cleansing, data matching, and analysis of usage patterns.

- **Investigation**: Activities related to the inquiry/following-up of detected/suspicious identity fraud acts.
  Examples: evidence/data collection, liaison with law enforcement personnel, additional surveillance to confirm/reject suspicions

- **Recovery**: Activities related to the recouping of losses/benefits that are directed at the perpetrator and which may be undertaken internally within the organisation and/or externally such as through the judicial system or debt collecting organisation.
  Examples: preparation of evidence briefs, time spent negotiating with the perpetrator and/or in the judicial system, legal costs.

- **Restoration**: Activities related to attempting to re-establish the victim’s position prior to the identity fraud occurrence. These activities are conducted in addition to those related to recovery and are not directed at the perpetrator.
  Examples: media campaigns to reassure stakeholders in response to identity fraud attack, transaction costs associated with hiring new staff (where staff involved in identity fraud attack), time spent to re-establish circumstances of the identity.

**Figure 1: Identity Fraud Activity Value-Chain**
amounts lost become sizeable. However, the transferability of costs-of-quality prescriptions to identity-fraud may be problematic due to significant and irreducible differences in context.

The methods through which identity fraud can be perpetrated are arguably less standardised than an organisation’s production processes. In the latter, inventory and goods need to pass through a pre-defined sequence of steps and worked upon in a particular manner to be converted into the finished product. In contrast, the method by which the former occurs is only limited by the imagination of the perpetrator. As discussed, identity fraud could comprise the theft of a real person’s identity, either living or deceased, the fabrication of a fictitious identity or the opportunistic utilisation of documentation that supports an altered identity (that contains spelling errors for example). Similar, the identity fraud could occur through the organisation’s physical offices, call-centres or electronic channels and could comprise the opening of new facilities or the take-over of existing. There is thus a greater degree of variation in identity fraud methods and lack of visibility over these vis-à-vis organisational production processes. Thus it remains to be seen whether the prescriptions identified are transferable to the identity fraud context, and whether an optimal configuration of activities exists which leads to enhanced performance in responding to identity fraud.

3. Research method

3.1 Research Sample

The research presented herein derives from a sample of 29 Australian public and private-sector organisations to evaluate the nature, cost and impact of identity fraud, and the manner of organisational responses to identity fraud. The targeted participants were each organisation’s Head of Fraud Department (or equivalent). Interviews were held comprising 1-2 hours duration where a structured questionnaire was administered for the eliciting of information on identity fraud response⁶. In addition to this, information on the resources spent on identity fraud response as well as the associated losses for the period 2001-02 was collected from these organisations.

Given that identity fraud was not likely to impact all industries equally (Federal Trade Commission, 2003), it was important to identify those settings containing significant incentives of identity fraud perpetrators to attack and, consequently, where investigating organisational responses was most imperative. Existing evidence on the propensity of certain industries to be victims of identity fraud was utilised to effect this, such as prior studies conducted in seeking to rank industries in relation to total fraud exposures (refer to Federal Trade Commission, 2003). Thus the sample is non-random, reflecting those organisations that collect and disburse sizeable financial benefits and other goods and services, which rely upon identity registration and authentication in their processes, and thus are more likely to be victims of identity fraud. In all, 29 organisations provided information and data about identity fraud as presented in Table 1.

### 3.2 Assessing Fraud Response

Collecting information on the resource spend of organisations on identity fraud and the associated losses proved problematic because identity fraud as a phenomena or event was not attributed costs by the majority of participants. Furthermore, the resources of fraud and other departments were rarely dedicated to specific identity fraud responses. Rather, resources were often focused on all types of fraud. Given these challenges, activity-based costing (ABC) techniques were utilised to estimate the resource spend on identity fraud response.

Having extracted cost information on the relevant resources from their organisational accounting systems for the period 2001-02, participants were required to attribute resource costs to individual activities on the basis of some measure of consumption by each activity. For personnel resources, this attribution was largely done on the basis of the percentage of time spent on identity fraud and the nature of that time spent (prevention versus detection, for example). For technology resources, this was done using estimates of the proportion of time used for identity fraud versus other uses and/or the proportion of system outputs that were identity-fraud related versus other uses. The specific activity these costs were attributed to depended on the nature of the system. For example, the costs of technologies used to detect identity anomalies in an organisation’s database would have been attributed to the detection activity.

To obtain financial loss information, organisations were asked to provide losses that were written-off during the financial year 2001-02 due to identity fraud. Losses that were not written-off during 2001-02 (irrespective of whether an identity fraud event had occurred) were excluded as the organisation either considered that some degree of recoverability existed or, alternatively, insufficient information existed to write-off that debt. As such, financial losses were operationalised as amounts written off due to identity fraud.

Participants were also asked to respond to an identity fraud management and control questionnaire. The questionnaire, to

### Table 1: Sample Demographics by Industry

<table>
<thead>
<tr>
<th>Respondent Classification</th>
<th>Number of Respondents</th>
<th>% of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Services</td>
<td>13</td>
<td>45%</td>
</tr>
<tr>
<td>Communications and Infrastructure</td>
<td>9</td>
<td>31%</td>
</tr>
<tr>
<td>Retail</td>
<td>2</td>
<td>7%</td>
</tr>
<tr>
<td>Government Organisations</td>
<td>3</td>
<td>10%</td>
</tr>
<tr>
<td>Other Organisations</td>
<td>2</td>
<td>7%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>29</strong></td>
<td></td>
</tr>
</tbody>
</table>
be completed by an organisation’s Head of Fraud Department (or equivalent), asked each respondent to categorise and rank responses on a 5-point Likert scale (in most cases) in relation to the items depicted in Figure 2. The questionnaire ratings provided information on the extent and nature of the activities performed by the various organisations.

4. Results

4.1 Identity Fraud Response Value Chains and Performance

To assess the configuration of activities performed in responding to identity fraud, the organisational resources expended in their conduct were investigated through an analysis of the outputs of the ABC process. As indicated in Table 2, the majority of organisational resources were expended in the anticipatory activities of risk assessment, prevention and deterrence, and detection. Furthermore, most resource spend (42%) occurred in prevention and deterrence, with the second most (34%) occurring in detection. Prima facie, this finding is consistent with the normative prescriptions adapted from the costs-of-quality literature that prescribed a primary emphasis on prevention activities with a secondary focus on detection if the costs of ‘non-conformities’ were to be minimised. However, it is important to note that resource spend per se does not indicate the effectiveness of activities but the amounts consumed in the conduct of the activities only. It is thus difficult to infer performance consequences using resource spend data alone.

In attempting to draw out the performance implications of different value-chain configurations, we turned to the ratings of prevention and detection controls. Based on the ratings assigned, organisations were classified as having high, medium and low prevention and detection. In addition, we used identity fraud loss information (adjusted for organisational size using total assets as a proxy) as measures of ‘identity fraud response performance’. The rationale for doing so was its popularity as a means of measuring identity fraud performance across the majority of organisations interviewed. As such, we examined the average dollar loss per $1,000 of total assets across the various prevention and detection groups. The small sample numbers imposed limitations on the analysis of quantitative data. For example, rather than analysing loss data by prevention and detection simultaneously, this had to be done sequentially, with differences in levels of the other variable qualitatively commented upon. Furthermore, the reduced group numbers precluded any comments on statistical significance. Thus, the analyses presented in Table 3 and 4 are indicative only.

Consistent with costs-of-quality prescriptions, Table 3 indicates that high prevention organisations also reported the lowest average losses. However, the losses sustained by medium prevention organisations were marginally higher relative to low prevention organisations. Interestingly, organisations with medium prevention tended to also have high or medium detection. In contrast, organisations with low prevention had a predominance of low detection capabilities. A potential explanation involves the inter-dependence of the detection and loss variables. Losses reported by organisations were those they had detected. Thus, it is conceivable that low prevention organisations that also tended to possess low detection capabilities may have incurred identity fraud losses but not detected and reported these. Consequently, their average losses may have been understated. Indicative support is thus provided for the prescription that increased prevention does translate into reduced identity fraud losses, despite the changing and fluid nature of identity fraud manifestations.

The above explanation is further supported by the results presented in Table 4, which examines identity fraud losses across detection groups. High detection organisations reported higher losses vis-à-vis medium detection organisations. However, lower detection organisations reveal an anomalous result with significant higher losses being detected. Investigating further revealed that one organisation was in a business where the ‘values’ transacted were much higher than the remainder of the sample, whilst two others had recently implemented a detection capability, revealing a number of long-running identity frauds.

Figure 2: Questionnaire Items

<table>
<thead>
<tr>
<th>Activity</th>
<th>Cost $</th>
<th>Relative %</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Assessment</td>
<td>54,424,840</td>
<td>14%</td>
</tr>
<tr>
<td>Prevention &amp; Deterrence</td>
<td>167,762,691</td>
<td>42%</td>
</tr>
<tr>
<td>Detection</td>
<td>134,857,761</td>
<td>34%</td>
</tr>
<tr>
<td>Investigation</td>
<td>11,227,740</td>
<td>3%</td>
</tr>
<tr>
<td>Recovery</td>
<td>11,289,474</td>
<td>3%</td>
</tr>
<tr>
<td>Restoration</td>
<td>21,162,159</td>
<td>5%</td>
</tr>
<tr>
<td><strong>Total Resource Spend</strong></td>
<td><strong>400,724,664</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

Table 2: Activity Configuration
for the first time. These factors, together with the low group numbers, explain the higher average losses reported by the low detection group.

Taken together, the results indicate a need to consider both prevention and detection in managing and evaluating the value-chain of activities performed to combat fraud. The results indicate that higher levels of preventative controls reduce the levels of losses sustained. However, the moderating effects of detection also require consideration. Losses reported in organisational information systems and detection capabilities are interdependent. While a higher detection capability may reduce the extent of losses sustained through a more timely identification of fraud, it is also likely to be associated with higher losses being reported for identity fraud or traced to their identity fraud cause in the short-term. In interpreting the above results, it is also important to consider some of the other factors that impact on organisational performance in identity fraud loss reduction, as presented in the following section.

5. Conclusions

Identity fraud represents a significant challenge for organisations and their fraud departments to counter. Despite this, a lack of research exists on how performance should be managed and response configured. To this end, the contributions of this paper are two-fold. Firstly, a framework that both operationalises the identity fraud construct and facilitates the measurement and evaluation of organisational responses in terms of a ‘value-chain’ of activities is presented and applied. Secondly, exploratory evidence is provided on how fraud departments are responding to identity fraud and the efficacy of these responses. Given the fragmentary nature of extant understandings of identity fraud and organisational responses, the frameworks developed and evidence presented are proffered as a means of facilitating ‘cumulative’ work, through both the ongoing refinement of concepts and the testing of the indicative findings presented herein.

The evidence presented indicated that the majority of organisations sampled emphasised the ‘anticipation’ of identity fraud and, in particular, activities performed in relation to prevention, deterrence and detection. However, it is difficult to conclude on the efficacy of response utilising resource spend information alone. Examining the extent of prevention controls and detection capabilities enabled the identification of performance consequences. Organisations with more sophisticated preventative controls also reported lower losses. Counter-intuitively on first glance, organisations with higher detection capabilities reported higher losses (other things being equal). Although it is argued that greater detection capabilities will result in more timely discoveries of fraud and identity fraud and, thus, less losses, greater detection capabilities resulted in the identification of more losses as identity fraud. This dual-impact is important to consider when fraud department managers are choosing the extent to which different activities comprising the identity fraud response value chain are performed and performance measured on an ongoing basis. In the short-term, an investment in greater detection might result in the opposite effects to those expected; namely, an increase in identity fraud losses. However, the results indicate that these losses may reduce in the long-term if this ‘intelligence’ can be translated into preventative efforts.

Given the lack of prior research, the results presented are exploratory at best. A number of limitations suggest caution in interpretation. Firstly, the low number of organisations able to provide accurate information on their identity fraud losses impinged upon the data analysis and the results presented. Secondly, only losses detected by organisations were captured and analysed herein. No attempt was made to account for losses undetected or the non-financial losses sustained as a result of identity fraud, such as the impacts on the organisation’s reputation and image. Furthermore, the losses sustained were standardised for comparison purposes using total assets as a proxy of organisational size. Given the focus on identity fraud, a volume-based measure such as the number of customer transactions may have been a more suitable measure. Finally, the impact of moderating variables was not controlled for in the investigation of fraud response performance. These could include industry factors, incentives to perpetrate and time-lags between fraud response and effects on loss.

In conclusion, a number of avenues exist for further research. Further empirical evidence as to the performance consequences of different fraud response activity configurations is required. This can also be extended to consider other types of fraud and can result in the building of fraud performance theories that offer prescriptions for further testing by researchers as well as important insights for fraud practitioners. In addition, the data presented suggests that a number of challenges exist for organisations in measuring the performance of their fraud departments. The extent to which existing performance measures are suitable and effective for performance measurement in organisational support areas such as fraud departments represents another area that merits further consideration. Such research is considered timely given.
the available evidence on identity fraud’s sizeable impact on contemporary organisations and the scarcity of evidence on the efficacy of organisational responses to this significant risk.

* Corresponding Author
Address: Macquarie Graduate School of Management, Macquarie University, North Ryde NSW 2109
Email: suresh.cuganesan@mgsm.edu.au
Phone: + 61 2 9850 6096

Endnotes
1. Identity theft meaning the theft of a real person’s identity, it is also important to acknowledge that these trends may also be the result of improved awareness and reporting.
2. Within Australia alone, identity fraud has been referenced as costing anywhere between $1.1 billion and $4.5 billion per year. In the United States, the disparity in costs has been stated as anywhere between $1 billion and $50 billion per year.
3. While developed in relation to identity fraud, the value chain of activities is generic enough to be applied against other types of fraud.
4. This classification is consistent with that prescribed by the (Home Office, 2000), who utilise an anticipation-consequence classification.
5. Failure costs involve corrective actions taken by organisations and the losses sustained as a result of ‘non-compliance’, be this a poor quality product or the circumvention/breakdown of fraud control processes. As such, failure costs comprise the investigation, recovery and restoration work done by an organisation in response to an identity fraud event as well as the irrecoverable losses sustained as a result. Conceivably, internal and external failure impacts can be distinguished by reference to whether the identity fraud involves (a) a legitimate customer and (b) is detected and its impacts rectified before the customer whose identity is taken over becomes aware of this. This distinction is not drawn herein due to the practical difficulties in measuring internal versus external failure.
6. In addition, an unstructured discussion on the issues and challenges facing organisations in responding to this crime was held, the results of which are presented in a separate paper.
7. While these cases would have ordinarily been excluded from the analysis on the basis of being ‘outliers’, the low group numbers resulted in their inclusion with their anomalous effects commented upon.

6. References


Deming., W. E., (1986), Out of the Crisis. Massachusetts, MIT.


General Accounting Office, (1998), Identity Fraud: Information in Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, United States, GAO/GGD-98-100BR.


Main, G. and Robson, B., (2001), Scoping Identity Fraud, Canberra, Commonwealth Attorney-General’s Department.


