New Challenges for Performance Management: Exploratory Evidence on Organisational Responses to Identity Fraud

Suresh Cuganesan
and
David Lacy

Available evidence indicates that identity fraud is a significant risk to organisations. Despite this, a lack of research exists on the role of performance measurement and costing systems in supporting organisational responses to this problem. This paper presents exploratory evidence on the challenges for performance measurement and costing systems if organisational responses to the identity fraud problem are to prove effective.

1. Introduction

Available evidence indicates that identity fraud is significant and wide-ranging, with current assessments of its impacts against businesses exceeding billions of dollars each year[1,2,3,4]. With identity fraud also being implicated in other forms of white-collar crime such as money-laundering and tax evasion, offences which are increasingly attracting sizeable corporate penalties[5], identity fraud poses a significant problem for contemporary organisations. Of focus here is the role of performance measurement and costing systems in supporting organisational initiatives to respond to this concern.

Concurrently, the discipline of management accounting and performance measurement has witnessed a number of so-called innovations in recent times. Within management accounting, the development of activity-based costing (ABC) has been held out as a significant evolution in costing systems[6,7]. In the field of performance measurement specifically, developments include the trend towards the utilisation and management of non-financial performance dimensions[8,9], balanced scorecard frameworks[10,11] and triple bottom-line approaches[12]. These advances were focused initially on the management of an organisation's 'core' business processes and departments, and are only now beginning to expand into the domain of what might be labelled 'support' functions such as information technology[13] and sales and marketing[14]. Managing the performance of organisational fraud departments is yet to receive such attention.

This paper presents initial evidence from Australian organisations on their response to identity fraud. Exploratory results from 70 interviews across firms within the public and private-sectors are presented, comprising qualitative insights into the difficulties that organisations face in managing the performance of their identity fraud response. The paper ends with a discussion of the challenges for organisations in combating identity fraud, the role of performance measurement and costing systems in this regard, and an agenda for future research.

2. The Identity Fraud Problem

The manner in which identity fraud is committed is both heterogeneous and fluid. Indeed, the means by which identity fraud 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). Similarly, 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 ones. There is thus a great degree of variation in identity fraud methods and a lack of visibility over these. Furthermore, it is conceivable that the manner in which identity fraud (and all fraud for that matter) is perpetrated will vary in reaction to organisational responses, as perpetrators learn about organisations' safety limits and risk thresholds. By its nature, identity fraud presents a complex and challenging problem for organisations to control.

In addition, the impacts of identity fraud on contemporary organisations are significant. While the fraudulent representation of identity has existed for an extended period, a number of factors have generated heightened concerns about its current impacts. Firstly, it is suggested that identity fraud is becoming easier to perpetrate with globalisation and its rapid information flows, technological improvements that result in a greater ease of forgery, and the increased use of the internet to transact at a distance, moving away from traditional face-to-face interactions. Secondly, identity fraud has been linked to organised crime[15], with the implication that professional criminals are dedicating time and resources to exploit weaknesses in organisational control systems. Thirdly, available evidence suggests that identity fraud is significant and growing. 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[16,17]. In Australia, the impact of identity fraud on businesses has been estimated at A$1.1 billion[18]. As a consequence, identity fraud and the formulation of an appropriate response have been dominating the agenda of government and public policy organisations[19].

In stark contrast to the important and complex nature of the identity fraud problem, the extant literature on the issue has been largely descriptive, often enumerating identity theft cases as a precursor to discussions about potential solutions (see, for example[20,21,22,23]). A number of government-initiated studies also exist, which are aimed primarily at estimating the impacts of identity fraud at a national level and identifying broad policy implications[24,25,26]. In similar fashion, the limited 'academic' research that has been completed to date has focused upon the role of governments and, in particular, the relevance of existing legislative provisions and the efficacy of penalties towards identity fraud[27,28]. Overlooked has been the role of organisations, with significant questions remaining about how commercial businesses and government agencies can better manage their performance in combating identity fraud. The research method used to explore how organisations are attempting to respond to identity fraud and the role of accounting and performance measurement systems is presented next.

3. Research Method

Given that identity fraud was not likely to impact all industries equally[29], 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 internationally that ranked industries in terms of reported identity fraud occurrences (for example, refer to[30]).

However, within most industries selected, there was heterogeneity in scale and scope (for example, national versus regional operations and diverse product ranges versus narrow offerings). Consequently, organisations that represented the diversity within each of the selected industries were targeted. 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, 70 Australian organisations across both public- and private-sectors provided information about their identity fraud response and challenges faced as presented in Table 1. While a diversity of organisations were interviewed, the sample did include the majority of the telecommunications and retail banking sector, as well as two large government agencies responsible for the provisioning of health and social security services.

Table 1: Sample Demographics by Industry

Respondent Classification	Number of Respondents	% of Respondents
Financial Services	30	43%
Communications and Infrastructure	14	20%
General and Health Insurance	11	16%
Retail	2	3%
Government Organisations	10	14%
Other Organisations	3	4%
Total	**70**	

The research conducted comprised a series of interviews conducted with the selected organisations. The interviews were held with organisations' Head of Fraud Department (or equivalent), their Fraud Managers and Analysts. Often, each interview had two to three organisational participants in addition to the researchers. The interviews comprised two elements; a structured questionnaire for the eliciting of information on identity fraud response and resource spend, and an unstructured discussion on the issues and challenges facing organisations in responding to this crime.

Given the lack of prior research on organisational responses to identity fraud and the role of accounting and performance measurement, an unstructured approach was considered best for the eliciting of 'novel' information and allowing interviewees the flexibility to identify and discuss issues germane to the control of identity fraud. However, focusing themes for the interviews included:

- the challenges faced in responding to the identity fraud problem;
- the ability of internal systems to provide cost information on an organisation's identity fraud response and associated net losses;
- the manner in which performance of the identity fraud response was assessed; and,
- the broader incentives that existed within the organisation to respond to the identity fraud problem.

4. Results and Discussion

The interviews yielded qualitative insights into the performance management challenges that organisations face. These can be broadly categorised into two separate issues; namely, the efficacy of performance measurement regimes and the ability to effect performance improvements.

4.1 The Efficacy of Accounting and Performance Measurement Systems

Across the majority of interviewed organisations, cost information about the resources expended on identity fraud response was lacking. As might be expected, information in costing systems was organised along departmental, product and customer lines, and identity fraud as a phenomena or event was not attributed costs by the majority of organisations interviewed. Furthermore, the resources of fraud and other departments were rarely dedicated to specific identity fraud responses, being focused instead on all types of fraud. As such, these organisations found it difficult to isolate their investment in identity fraud response, and were limited in their ability to conduct cost-benefit evaluations.

More surprising, however, was the lack of information on identity fraud losses. A number of participants had only recently focused on identity fraud as a risk to be managed, despite operating in industries that prior research had identified as having high exposures to this problem. As such, these organisations faced difficulties in quantifying the impacts of identity fraud upon their organisation as a means of risk evaluation. The following comments across the sample were reflective:

> *"We haven't got any sort of conclusive figures as to the exact amount of fraud or, you know, identity fraud that has been happening out there. But we recognise the need to have a more coordinated approach to reporting"*

And:

> *"We're now at a stage where we're starting to look at what the issues are, and as a result obviously what the consequences are for us of not addressing identity fraud, and also the consequences, or I suppose the areas of identity fraud that we've been exposed to date and what the costs might be of that. We're not at a stage yet where we've got any hard data on that, though."*

Adding to the difficulties in collecting cost information on identity fraud losses was their treatment within accounting systems. Within private-sector organisations in particular, identity fraud losses often manifested as amounts unpaid by customers, be these fictitious customers or real customers that had been the victims of identity theft. However, these amounts were routinely written off as part of an organisation's bad debt policy. Once this occurred, these amounts were removed from the internal accounting systems and, consequently, it was considered difficult to isolate and monitor these from the remainder of bad debts expenses. Important information on the impacts of identity fraud was lost. A Fraud Analyst explained:

> *"So we might identify it as an identity fraud and classify it as a identity fraud, but when it actually came to the write-off stage, it would just go into the bad debt bucket. So to actually quantify what fraud was costing the company, it was next to impossible."*

Within public-sector organisations, measuring the impact of identity fraud was more difficult. The nature of these organisations meant that monies or services were provided to 'customers' on some basis of eligibility, with no repayment of this required. Thus, there were less 'natural flags' to initiate investigative action (such as the payment of a credit-card bill or mobile phone account in the private-sector). Consequently, measuring total identity fraud exposures was problematic for the public-sector participants.

Exacerbating the deficiencies in cost information were the performance measurement systems in place. In the minority

of organisations that did collect identity fraud information, the performance of the identity fraud response was typically evaluated in financial terms using metrics such as identity fraud losses and percentage of bad debts that were identity fraud related. Non-financial measures were typically limited to the number of identity fraud events and, to a lesser extent, time to detect identity frauds. This is despite the discipline of performance measurement long since evolving to embrace both financial and non-financial measures of performance. While financial performance measures are important in terms of quantifying the consequences of performance levels for the organisation in monetary terms, by themselves they lack timeliness and are not reflective of the drivers of enhanced performance[32,33,34]. As such, the performance measurement systems observed across the organisations studied also suffered from the deficiencies ascribed to systems configured exclusively in financial measurement terms only.

For example, the performance measurement regimes that had been developed were overly focused on the symptoms of problems in identity fraud response rather than the problems themselves. Measures of the number of fraudulent events, associated financial losses, or fraud as a percentage of bad debts, only captured information about the event itself rather than the context in which it occurred and the factors that contributed to its occurrence. Indeed, measuring the number and value of external fraud occurrences was seen as information that was 'after-the-fact'. As such, they failed to consider the processes throughout the organisation that might be better utilised to prevent and detect identity fraud. One Fraud Manager observed in relation to their organisation:

> *"It is [performance measurement data] not around understanding the modus operandi. That comes as a consequence, and it's more by sharing of tacit information than it is from strict data analysis that says there is a vulnerability here."*

Indeed, the lack of visibility over identity fraud made it difficult to track and measure identity fraud and the performance of an organisation's response. Another Fraud Head expanded on the general difficulties in collecting data on identity fraud:

> *"We may not be able to track this person, we may not be able to 100% confirm if it's a false identity or not, it could be a true person, it could be a false identity, so we may never know. How far are we going to go in terms of investing resources to find out if the person exists or not? We don't have 100% access to all records…"*

Thus, not only were a significant proportion of organisations examined limited in their ability to quantify and measure identity fraud losses, the performance measurement regimes in place at those organisations able to collect identity fraud information were deficient in the measurement of processes and areas where vulnerabilities were situated.

An additional limitation of current fraud response performance measures comprised their actionability for performance management objectives. For example, a high level of detected fraud was seen by participants as capable of multiple interpretations. One possible interpretation was that the detection capabilities were strong within an organisation and its fraud response was proving effective. An alternative interpretation viewed this as indicative of poor fraud prevention capabilities. As such, the actionability of the measures used was seen as deficient. One participant commented on the flawed nature of financial performance measures for evaluating fraud response:

> *"The whole concept is a strange one because when you're doing a good job with this sort of work the figures are very small because you're finding them so fast. So in a way it's the opposite to what you'd expect. If you found a fraud worth $50,000, you'd think that's great, but it went on for so long to get to $50,000. So the concept is a weird one if you equate dollar value with efficiency and success, the smaller the amount in a way is an indicator of a better system."*

Overall, detected fraud measurements appeared to be difficult to interpret from an efficiency and effectiveness perspective, becoming limited as a result in their usefulness for managing towards improved performance.

Furthermore, a number of participants commented on how identity fraud response was not the sole domain of the fraud department. For example, an increasingly common form of identity fraud prevention involved the use of on-line verification technologies within customer service centres. Similarly, the role of the debt collections and recoveries units within organisations was seen as contributing to the fraud response effort through the discovery of amounts owed that related to accounts established in a false identity[35,36]. Despite this, identity fraud response rarely featured in terms of the multiple perspectives and accountabilities enshrined in the performance management frameworks that had been implemented in these organisational departments. For example, the performance measurement frameworks for customer-facing areas typically emphasised sales growth and customer service. While not arguing for wholesale changes, one Fraud Manager commented upon the role of other organisational units in implementing identity fraud controls and the impact of measures and incentives that rewarded:

> *"You're relying upon your own agents, either as employees or third parties, to have done something more than a cursory check of the [identity] document that's in front of them to the body that's sitting there presenting it, assuming that it's in a physical sense. Now, sadly, we've had cases where that hasn't been picked up. It adds to the risk because they're driven by a different incentive. They're rewarded on a commission basis for getting sales or whatever, so their application of your own protocols for verifying [identities] may be different."*

These sentiments were shared by other participants:

> *"You look at people writing bad business. I think there would be numerous cases right across of people writing bad business knowingly, but aiming to achieve a particular sales target. I guess they are driven by commission. So there's that opportunity to fudge figures or whatever. The emphasis has been, to get the business through without standing back and saying 'what is the purpose of writing this business'. 'What does this person really want it for?' Do you feel it is genuine? Do you feel the person is genuine?"*

And,

> *"Well Sales seem to, you know, run the company basically. You know, their needs must be met first, and we are sort of struggling to put these measures in place to protect the company. They are the main impediment to anything that we do. So it is just that balance. At the moment it is definitely leaning more toward sales than protection."*

Thus organisational departments that often contributed in some fashion to the perpetration of identity frauds through poor prevention and detection not only lacked measurement on this important aspect of their performance, but were often incentivised to do exactly this. Consistent with current prescriptions that performance measurement devices such as the balanced scorecard be configured to reflect the different performance drivers that various organisational units were responsible for[37], a few fraud departments were considering whether and how to incorporate fraud response measures within wider organisational performance measurement frameworks in areas such as sales and customer service. However, the implementation of these initiatives was not considered to be practicable in the foreseeable future.

4.2 Effecting Performance Improvements

In making decisions on whether to invest in new prevention and detection capabilities, fraud departments were often required to put together business cases to the wider business and executive management. Paramount was the ability to provide 'hard data' and the difficulties in doing. One participant commented:

"If we are able to give figures and justify why this is needed with hard data, we usually can make changes after a lot of resistance, but unfortunately we don't actually record things. Even if we had anecdotal evidence, we wouldn't have hard data."

In the provision of 'hard data' and the prioritisation of process improvements, however, fraud personnel faced difficulties in estimating the 'full' costs and benefits of new identity fraud response 'investments'. While the costs of extra personnel or technology solutions in responding to identity fraud were typically tangible and 'known', the benefits of these responses could rarely be quantified fully. For example, although the amounts lost could be determined, the amounts that would have been lost in the absence of particular prevention or detection capabilities were not measured. A Fraud Head explained the difficulty in measuring 'potential' losses:

> *"We know how many [identity documents] we've actually validated and confirmed as being fraud, but we don't know what losses could have arisen out of those, had we allowed them to proceed. And the same thing goes for everything else that we've stopped... Could that have led to something else? Well, we just don't know, and no one will ever be able to quantify that."*

For another Fraud Head, the problem in accurately estimating the benefits of identity fraud prevention was 'knowing the unknown'; specifically, quantifying the extent of 'undetected' identity fraud:

> *"What you identify, this is what you say you prevent. How can you quantify what you actually prevent? You know, at the moment we could say our exposure is what's detected. There's been no real attempt to quantify what things haven't been detected, the potential exposure [to identity fraud]."*

As a result, the savings ascribed to both existing and new investments in fraud response was perceived as being understated, reflecting the amounts lost due to detected identity fraud rather than the potential losses that were averted and not incorporating undetected identity fraud events that might become detected. Adding to this were difficulties in measuring other types of 'invisible' costs when making performance management decisions such as the tightening of controls:

> *"The reputational aspects to identity fraud, how do we quantify that? We don't know. In terms of the costs, the cost to run the unit, the loss - the fraud that goes to loss that are known. Things that are unknown are things such as foregone revenue from turning customers away. What else is there? Reputational costs and all that."*

Thus, the performance of cost-benefit assessments of both existing and new investments in identity fraud prevention and detection capabilities was considered difficult, with these being 'biased' towards those items that were tangible and easily quantified, and which were typically costs rather than benefits.

An additional complexity for organisations attempting to effect performance improvements in their identity fraud response comprised the issue of controllability. Prior to transacting with customers, organisations often require some form of evidence of identity and typically seek to verify that the documents presented are genuine. This involves a reliance on the provider of the documents presented. As such, each organisation's exposure to identity fraud was not only impacted by its own controls and processes but those of other organisations as well, with the latter not being directly controllable. This lack of controllability made it difficult to manage the identity fraud problem according to a number of participants:

> *"The lack of and/or the in-effective controls and verification at other organisations makes it easy to obtain source identity documents in a false or assumed name and therefore makes it difficult for us to protect themselves against identity fraud as the fraud can occur against identity documents which are valid and have been issued from a legitimate source."*

And,

> *"Accepting the integrity of the documents that are presented to you. While we are providing training to staff, it is very difficult then to sort of know what different identity documents look like etc etc. So it is really that initial evidence of identity processes where our major risks are happening."*

Indeed, achieving performance improvements required these other organisations to also improve their identity fraud response. Another participant expanded on the inter-dependencies amongst organisations in effecting performance improvements

> *"So before we even do business with a person we basically put them through the stringent checks to make sure we can positively identify the person. But in doing that we then rely on documents that may be issued by other organisations in proving themselves. Now the concern we have is that the other organisations may not have as stringent controls in the issue of their documentation… So it is important for us to make sure that other organisations look towards basically their loopholes and address them, so that that's going to really allow us to really fight towards you know reducing identity fraud."*

In sum, common themes in the qualitative data obtained from interviewed organisations indicate issues to be overcome both in aligning performance measurement regimes with performance management objectives and in the effecting of performance improvements specifically. Managing these performance management challenges is imperative if organisations are to respond to identity fraud in an effective and efficient manner.

5. Conclusions

The relationships between accountants and white-collar crime have been neglected by researchers. This is despite risk management and the mitigation of both financial loss and reputational damage deriving from fraud, illegal acts and non-compliance being an arena for the expanded activities of accounting at the culmination of the 20th century[39]. This study addresses this gap by examining the significant and growing problem of identity fraud and the role of performance measurement and costing systems in organisational responses to this problem.

Identity fraud represents a significant challenge for organisations and their fraud departments to counter. Despite this, a lack of research exists on how organisations are responding and the role of performance measurement and costing systems in supporting this process. Furthermore, the limited prior research that exists utilises different notions of identity fraud. In light of this, the contributions of this paper are two-fold. Firstly, a framework that operationalises the identity fraud construct is presented. Given the fragmentary nature of extant understandings of identity fraud, this framework is proffered as a means of facilitating 'cumulative' work through consistency and clarity in the conceptual underpinnings of identity fraud research. Secondly, exploratory evidence is provided on the issues faced by fraud departments in responding to the identity fraud problem. As an area which is yet to participate in the benefits of innovations in accounting, challenges are identified for the role of performance measurement and costing systems that could support these initiatives.

The results presented herein have a number of practical implications. In achieving performance improvements in identity fraud response, organisations face a number of challenges. The first is to adapt their costing systems to provide an indication of their exposure to identity fraud. Understanding the amounts lost to identity fraud (conversely, the amounts that could be saved from a more effective identity fraud response) is arguably the first step in risk assessment and the formulation of the appropriate control strategy. Doing so is necessary for cost-benefit assessments and awareness-raising throughout the organisation in relation to identity fraud. While a wholesale cost system redesign is not prescribed here, smaller scale adaptations are advocated and, indeed, are already being suggested in the areas of information technology and marketing for these purposes[40,41]. Secondly, organisations need to align their performance measurement regimes with the objective of reducing fraud losses. This may be achieved by expanding the scope of both financial and non-financial measures, measuring the causes of performance rather than the outcomes and expanding this across those parts of the organisation that contribute directly or indirectly to identity fraud response. The third challenge comprises the acknowledgement and potential measurement of the 'invisible' benefits of fraud response such as reputational impacts and reductions in undetected identity fraud losses. Concurrently, inter-organisational approaches to performance management may be required given the interdependent nature of identity fraud risk.

Given the lack of prior research, the results presented are exploratory, and its limitations suggest caution in interpretation. Firstly, the qualitative insights presented reflect the perspective and 'bias' of Fraud Departments only, rather than a wider organisational view. Secondly, the organisations sampled were focusing increasingly on identity fraud and, as such, changes may have occurred subsequent to the research. Despite these limitations, a number of clear avenues exist for future research. Empirical evidence as to the performance consequences of different identity fraud responses 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 evidence 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. **JARAF**

Dr. Suresh Cuganesan is Associate Professor in Management at Macquarie Graduate School of Management, Macquarie university and CPA qualified accountant. David Lacey is a lecturer at the Australian National University College of Business.

References

1. Cabinet Office, Identity Fraud: A Study, (London: Economic and Domestic Secretariat, Cabinet Office, 2002).

2. Suresh Cuganesan, and David Lacey, Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent (Sydney, Standards Australia, 2003).

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

4. General Accounting Office, Identity Theft: Prevalence and Cost Appear to be Growing, (Report to Congressional Requesters, United States, GAO-02-363, 2002)

5. E Fry, "Drug Money." (2004) CFO April http://www.cfoweb.com.au/stories/20040401/20022022p.asp

6. Malmi, T. (1997). "Towards explaining activity-based costing failure: accounting and control in a decentralized organization." Management Accounting Research 8: 459-480.

7. A Rafiq and A Garg, "Activity-Based Costing and Financial Institutions: Old wine in new bottles or corporate panacea?" (2002) Journal of Cost Management 15(2)

8. RD Banker, G Potter and D Srinivasan, "An empirical investigation of an incentive plan that includes nonfinancial performance measures" (2000) The Accounting Review 75(1) 65-92

9. S Perera, G Harrison, and M Poole, "Customer-Focused Manufacturing Strategy and the Use of Operations-based non-financial Performance Measures: A Research Note." (1997) Accounting, Organizations and Society 22(6) 557-572

10. CD Ittner, and DF Larcker, "Innovations in Performance Measurement: Trends and Research Implications." (1998) Journal of Management Accounting Research 10 205-238

11. RS Kaplan, and DP Norton, The Balanced Scorecard-Translating Strategy into Action (Boston, Harvard Business School Press,1996)

12. Elkington, Cannibals with forks: the triple bottom line of 21st century business (Oxford, Capstone, 1999)

13. E Peacock, and M Tanniru, "Activity-based justification of IT investments" (2005) Information & Management 42(3) 415-424

14. V Dickinson, and JC Lere, "Problems evaluating sales representative performance?: Try activity-based costing." (2003) Industrial Marketing Management 32(4) 301-307

15. National Criminal Intelligence Service, "Role of Identity Fraud in Underpinning Serious and Organised Crime." (2003) 27 February: http://www.ncis.co.uk/briefing/270203

16. Supreme Court of the State of Florida, "Statewide Grand Jury Report: Identity Theft in Florida" (First Interim Report of the 16th Statewide Grand Jury, Case No: SC 01-1095 2002)

17. Ibid. 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.

18. Op cit. see Suresh Cuganesan, and David Lacey, 2003

19. House of Representatives Standing Committee on Legal and Constitutional Affairs Crime in the Community, (Canberra, Canberra, House of Representatives, Thursday, 26th September 2002). For example, identity fraud was highlighted as 'a priority issue' in the Commonwealth, States and Territories agreement on terrorism and multi-jurisdictional crime on 5th April 2002.

20. B. Givens, "Identity Theft: The Growing Problem of Wrongful Criminal Records" (2000) SEARCH National Conference on Privacy Technology and Criminal Justice Information, Washington, D.C., June 1

21. A Graycar, and R Smith, "Identifying and Responding to Electronic Fraud Risks" (2002) 30th Australian Registrars' Conference, Canberra, November 13

22. A.-M Moore, "ID Theft: Asia's Credit Bureaus Need More Proactive Role." (2002) The Asian Banker October 1

23. N Willox, and TM Regan, "Identity Fraud: Providing a Solution" (2002) Journal of Economic Crime Management 1(1) 1-15

24. Op cit. see Cabinet Office, 2002

25. Op cit. see General Accounting Office, 1998

26. Op cit. see General Accounting Office, 2002

27. JE Matejkovic, and KE Lahey, "Identity theft: no help for consumers" (2001) Financial Services Review 10 221-255

28. G May, "Stop Thief! Credit Bureaus and Creditors "Silent" Co-conspirators to Identity Theft?" (2002) Journal of Texas Consumer Law 5(3) 72-80

29. Federal Trade Commission, Information on Identity Theft for Consumers and Victims From January 2002 Through December 2002 (United States 2003) http://www.consumer.gov/idtheft/reports/CY2002ReportFinal.pdf

30. Ibid. Misuse of identity information was found to be most prominent in credit-card fraud (42%), telecommunications and utility fraud (26%), bank fraud (17%), general employment seeking (9%), government documents and benefits (8%) and fraudulent loans (6%).

31. Carlin, T. M. & Finch, N., (2005), "Performance in Flux - An Investigation of New Public Financial Management Reform in Action", http://ssrn.com/abstract=902200.

32. RG Eccles, "The Performance Measurement Manifesto." (1991) Harvard Business Review 69(1) 25-29

33. J Fisher, "Use of nonfinancial performance measures" (1992) Journal of Cost Management Spring 31-38

34. RS Kaplan, and DP Norton, "The Balanced Scorecard - Measures that Drive Performance" (1992) Harvard Business Review 70(1) 71-79

35. Op cit. see General Accounting Office, 1998, for further evidence of this.

36. Op cit. see General Accounting Office, 2000, for further evidence of this.

37. Op cit. see Kaplan and Norton, 1996.

38. AP Mitchell, Sikka and H Willmott, "Sweeping it under the Carpet: The Role of Accountancy Firms in MoneyLaundering" (1998) Accounting, Organizations and Society 23(5/6) 589-606

39. L Parker, "Back to the Future: The Broadening Accounting Trajectory" (2001) British Accounting Review 33 421-453

40. Op cit. see Dickinson and Lere, 2003.

41. Op cit. see Peacock and Tanniru, 2005.

References

1. Cabinet Office, Identity Fraud: A Study, (London: Economic and Domestic Secretariat, Cabinet Office, 2002).

2. Suresh Cuganesan, and David Lacey, Identity Fraud in Australia: An Evaluation of its Nature, Cost and Extent (Sydney, Standards Australia, 2003).

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

4. General Accounting Office, Identity Theft: Prevalence and Cost Appear to be Growing, (Report to Congressional Requesters, United States, GAO-02-363, 2002)

5. E Fry, "Drug Money." (2004) CFO April http://www.cfoweb.com.au/stories/20040401/20022022p.asp

6. Malmi, T. (1997). "Towards explaining activity-based costing failure: accounting and control in a decentralized organization." Management Accounting Research 8: 459-480.

7. A Rafiq and A Garg, "Activity-Based Costing and Financial Institutions: Old wine in new bottles or corporate panacea?" (2002) Journal of Cost Management 15(2)

8. RD Banker, G Potter and D Srinivasan, "An empirical investigation of an incentive plan that includes nonfinancial performance measures" (2000) The Accounting Review 75(1) 65-92

9. S Perera, G Harrison, and M Poole, "Customer-Focused Manufacturing Strategy and the Use of Operations-based non-financial Performance Measures: A Research Note." (1997) Accounting, Organizations and Society 22(6) 557-572

10. CD Ittner, and DF Larcker, "Innovations in Performance Measurement: Trends and Research Implications." (1998) Journal of Management Accounting Research 10 205-238

11. RS Kaplan, and DP Norton, The Balanced Scorecard-Translating Strategy into Action (Boston, Harvard Business School Press,1996)

12. Elkington, Cannibals with forks: the triple bottom line of 21st century business (Oxford, Capstone, 1999)

13. E Peacock, and M Tanniru, "Activity-based justification of IT investments" (2005) Information & Management 42(3) 415-424

14. V Dickinson, and JC Lere, "Problems evaluating sales representative performance?: Try activity-based costing." (2003) Industrial Marketing Management 32(4) 301-307

15. National Criminal Intelligence Service, "Role of Identity Fraud in Underpinning Serious and Organised Crime." (2003) 27 February: http://www.ncis.co.uk/briefing/270203

16. Supreme Court of the State of Florida, "Statewide Grand Jury Report: Identity Theft in Florida" (First Interim Report of the 16th Statewide Grand Jury, Case No: SC 01-1095 2002)

17. Ibid. 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.

18. Op cit. see Suresh Cuganesan, and David Lacey, 2003

19. House of Representatives Standing Committee on Legal and Constitutional Affairs Crime in the Community, (Canberra, Canberra, House of Representatives, Thursday, 26th September 2002). For example, identity fraud was highlighted as 'a priority issue' in the Commonwealth, States and Territories agreement on terrorism and multi-jurisdictional crime on 5th April 2002.

20. B. Givens, "Identity Theft: The Growing Problem of Wrongful Criminal Records" (2000) SEARCH National Conference on Privacy Technology and Criminal Justice Information, Washington, D.C., June 1

21. A Graycar, and R Smith, "Identifying and Responding to Electronic Fraud Risks" (2002) 30th Australian Registrars' Conference, Canberra, November 13

22. A.-M Moore, "ID Theft: Asia's Credit Bureaus Need More Proactive Role." (2002) The Asian Banker October 1

23. N Willox, and TM Regan, "Identity Fraud: Providing a Solution" (2002) Journal of Economic Crime Management 1(1) 1-15

24. Op cit. see Cabinet Office, 2002

25. Op cit. see General Accounting Office, 1998

26. Op cit. see General Accounting Office, 2002

27. JE Matejkovic, and KE Lahey, "Identity theft: no help for consumers" (2001) Financial Services Review 10 221-255

28. G May, "Stop Thief! Credit Bureaus and Creditors "Silent" Co-conspirators to Identity Theft?" (2002) Journal of Texas Consumer Law 5(3) 72-80

29. Federal Trade Commission, Information on Identity Theft for Consumers and Victims From January 2002 Through December 2002 (United States 2003) http://www.consumer.gov/idtheft/reports/CY2002ReportFinal.pdf

30. Ibid. Misuse of identity information was found to be most prominent in credit-card fraud (42%), telecommunications and utility fraud (26%), bank fraud (17%), general employment seeking (9%), government documents and benefits (8%) and fraudulent loans (6%).

31. Carlin, T. M. & Finch, N., (2005), "Performance in Flux - An Investigation of New Public Financial Management Reform in Action", http://ssrn.com/abstract=902200.

32. RG Eccles, "The Performance Measurement Manifesto." (1991) Harvard Business Review 69(1) 25-29

33. J Fisher, "Use of nonfinancial performance measures" (1992) Journal of Cost Management Spring 31-38

34. RS Kaplan, and DP Norton, "The Balanced Scorecard - Measures that Drive Performance" (1992) Harvard Business Review 70(1) 71-79

35. Op cit. see General Accounting Office, 1998, for further evidence of this.

36. Op cit. see General Accounting Office, 2000, for further evidence of this.

37. Op cit. see Kaplan and Norton, 1996.

38. AP Mitchell, Sikka and H Willmott, "Sweeping it under the Carpet: The Role of Accountancy Firms in MoneyLaundering" (1998) Accounting, Organizations and Society 23(5/6) 589-606

39. L Parker, "Back to the Future: The Broadening Accounting Trajectory" (2001) British Accounting Review 33 421-453

40. Op cit. see Dickinson and Lere, 2003.

41. Op cit. see Peacock and Tanniru, 2005.