DAVID LACEY AND SURESH CUGANESAN

# The Role of Organizations in Identity Theft Response: The Organization–Individual Victim Dynamic

**This study considers the role of organizations in relation to identity theft from three perspectives: as a site of identity use (and misuse), as detectors of identity theft, and ultimately, as a site where a fundamental social imperative exists to ensure responsible action is taken to address this form of criminality. Through investigating the organizational–individual victim dynamic, this article examines how organizations react to the possibilities of identity fraud and draws out the implications of this for individual consumers in scenarios of identity theft. The evidence presented leads to a critical examination of the issues confronting organizations in seeking to anticipate and respond to these criminal acts.**

Identity theft threatens the very essence of an individual's sense of self and his or her capacity to participate in society. The consequences of this form of criminality are significant and wide-ranging, with current assessments of its impacts exceeding billions of dollars each year (Cuganesan and Lacey 2003; Cabinet Office [U.K.] 2002; General Accounting Office [U.S.] 1998, 2002). Available evidence indicates that identity theft is becoming increasingly attractive for perpetrators vis-à-vis other forms of crime. In the United States, for example, identity theft is described as growing at a rate of 30% per year, with its losses estimated at reaching $8 billion by 2005 (Supreme Court of the State of Florida 2002). Although improved awareness and reporting may be partially responsible, these trends are nonetheless of concern to the individual consumer. The loss of funds and/or other forms of property, a tarnished credit history, and a criminal record are all potential outcomes for the identity theft victim, with ongoing consequences for the ability to secure employment, obtain goods and services on credit, travel freely, and participate in the wider society in a generally unencumbered fashion. In fact, merely seeking to reestablish an identity can result in ongoing denial of services for the victim, such as ac-

David Lacey is a research fellow at the Queensland University of Technology in Australia (dm.lacey@qut.edu.au). Suresh Cuganesan is a senior lecturer in the Macquarie Graduate School of Management at Macquarie University, Australia.

The Journal of Consumer Affairs, Vol. 38, No. 2, 2004
ISSN 0022-0078

cess to existing accounts and execution of existing contracts. Investigating identity theft and the current environment of responses is thus timely.

Although the formulation of identity theft responses is increasingly dominating the agenda of governments, policy formulators, legislators, and researchers, often overlooked is the important function of organizations in enabling and preventing identity theft. As discussed herein, the role of organizations in relation to identity theft is threefold: as a site of identity use (and misuse); as detectors of identity theft; and, ultimately, as a site where a fundamental social imperative exists to ensure responsible action is taken to address this form of criminality, an imperative based on the increasingly accepted notion that organizations are responsible for the long-term well-being and sustainability of the broader community (Executive Committee of World Business Council for Sustainable Development 2002; Maignan, Hillebrand, and McAlister 2002; Newson 2002). Consequently, it is important to consider organizational initiatives in formulating holistic policy responses to identity theft.

While focused on issues of identity theft, this article draws from a research program seeking to measure the nature, cost, and extent of the broader construct of identity fraud. *Identity theft* involves an individual falsely representing him- or herself as another real person for some unlawful activity (General Accounting Office 1998; *Identity Theft Assumption and Deterrence Act of 1998*). In contrast, *identity fraud* comprises both the illegal use of a real person's identity (identity theft) as well as that of a fictitious identity (Main and Robson 2001; Cabinet Office 2002). Thus, identity theft is a narrower subset of identity fraud. Of importance are the implications of this for the organizational–individual victim dynamic. For the individual consumer to be impacted, the crime must be one of identity theft. However, organizations can be victims of the misuse of both real and fictitious identities. As such, organizations develop their prevention, detection, and recovery responses in relation to identity fraud rather than identity theft specifically. Thus, in investigating the organizational–individual victim dynamic, this article examines how organizations react to the possibilities of identity fraud and draws out the implications of this for individual consumers in scenarios of identity theft.

In doing so, the article presents a conceptual map of the role organizations play in identity theft response and provides empirical evidence about the extent of organizational activities in this regard. The evidence presented leads to a critical examination of the issues confronting organizations in seeking to anticipate and respond to these criminal acts. The article concludes with an evaluation of the empirical data in light of the

observed need for more appropriate, socially responsible, and effective responses to identity theft by organizations, an evaluation that considers the individual consumer as a victim and considers the study's limitations and future directions for research in this field.

Although the results here are based on Australian organizations, it is contended that the implications are global. Current international concerns include the issuance of identity documents as in the U.K. (Home Office 2003) and the move towards biometrics-containing passports (see, for example, the U.S. *Enhanced Border Security and Visa Entry Reform Act* 2002). However, any system of identification is still reliant on organizations correctly issuing, securing, and authenticating these documents. Furthermore, organizations face relatively similar pressures (at least in Western economies) that impact their identity theft response, namely resource availability, the pressure to report growth, and difficulties in garnering outcomes through the judicial system (Gayer 2003; May 2002; Cabinet Office 2002). Finally, a number of organizations within the sample have a global presence. This article thus represents an important step toward understanding the role of organizations within the identity theft context and the impacts upon individual consumer rights internationally.

## ORGANIZATIONAL ROLES IN IDENTITY THEFT

Prior research on identity theft has been largely descriptive, enumerating identity theft cases, often as a precursor to discussions about potential solutions (see, for example, Givens 2000; Graycar and Smith 2002; Moore 2002; Willox and Regan 2002). An alternative strand of research has considered the efficacy of legislative penalties towards identity theft (Matejkovic and Lahey 2001; May 2002). While important from an awareness-raising and law reform perspective, significant questions remain about the role of organizations (including government agencies) in both contributing to and preventing identity theft on behalf of consumers.

### Organizations as Sites of Identity Use (and Misuse)

The role of organizations in modern commerce is well established (Silverman 1970). In the provision of goods and services, organizations are important users of individual identity. For example, prior to commencing a relationship with an organization, consumers are often required to register or "prove" their identity in order to transact with the organization on an ongoing basis. Similarly, in the post-registration phase, consumers are often required to "authenticate" their identity when transacting. In sum, or-

ganizations transact on the basic premise of identity, be it to provide access to unemployment benefits based upon the presentation of paper-based identity documentation, or to enable the transfer of funds electronically through a username and password authentication process. Therefore, organizations are important sites of identity use, but can also be sites of identity misuse. This might occur where organizations do not implement sufficient controls to detect stolen identities prior to transacting. Additional considerations include the ways in which existing customer information is stored (physically and electronically) and discarded.

## Organizations as Detectors

Significant periods of time often elapse prior to detection by individual victims of identity theft (FTC 2003a, 2003b). Indeed, detection of identity theft by the individual victim often occurs because they have been contacted by the organization where the identity was misused. Through the interrogation of data repositories, organizations are better able than consumers to become aware of suspicious activities and identity theft. For example, the nonpayment of credit cards or loans in financial services, or mobile phone bills in telecommunications, may act as initial "triggers of suspicion." Alternatively, the payout of higher-than-average benefits or multiple payouts for the same claim may alert insurance or social security organizations to real or false claims being made by persons other than the authorized policy holder or eligible recipient. Thus, it can be argued that organizations are central to the detection of identity theft and the communication of this to consumers who are victims.

## Organizations and the Social Imperative

That organizations need to effect a social responsibility is a widespread and increasingly accepted notion as exemplified within discourse on corporate social responsibility and triple-bottom line frameworks that measure corporate performance in financial, social, and environmental terms (Newson 2002; Turner 2001). It is argued that the social and environmental impacts of an organization's activities are just as important as its financial performance. Many commentators argue that organizations should do more to discharge their social responsibility (Executive Committee of World Business Council for Sustainable Development 2002; Maignan, Hillebrand, and McAlister 2002). Applied to the context of identity theft, the social imperative suggests that organizations move beyond compliance with extant regulations to acknowledge wider obligations. Reporting of

crime and identity theft to law enforcement is relatively low (Commonwealth of Australia 2000; Cuganesan and Lacey 2003). Furthermore, there is no requirement that organizations that detect identity theft inform industry counterparts and other key stakeholders for the purposes of improving practices to mitigate the likelihood of future events impacting individuals. Fundamentally, such actions may help in cases of repeat and persistent perpetrators, especially in light of evidence that the deterrence associated with the misuse of identity theft is insufficient (Cuganesan and Lacey 2003).

## RESEARCH METHODOLOGY

This research is based on 70 interviews of 1–2 hours duration with Australian public and private sector organizations. The interviews comprised two elements: a structured questionnaire for eliciting organizational responses to issues of identity fraud and identity theft, and an unstructured discussion on the issues and challenges facing organizations in responding to these crimes. Details of both elements are provided below following a discussion of the research sample.

Organizations were selected through the adoption of a risk-based identity theft prioritization model. Two key dimensions were considered: (1) the incentives of perpetrators to attack, and (2) the organization's scale and scope of operations. Firstly, existing data on the prevalence of identity theft were used to *a priori* select industries for participation that represented the highest risks for individual consumers (refer to Federal Trade Commission 2003a). 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, organizations that represented the diversity within each of the selected industries were targeted.

As such, the sample is intentionally nonrandom, reflecting those organizations that collect and disburse sizable financial benefits and other goods and services, and that rely upon identity registration and authentication in this process. It is not representative of the entire Australian business landscape. Rather, it focuses upon those areas that represent the highest identity theft risk to individual consumers. In all, 70 of Australia's larger organizations provided information and data about identity fraud and identity theft as presented in Table 1.

The targeted participants were each organization's Fraud Head of Department (or equivalent). Where appropriate, a 5-point Likert scale was

TABLE 1
*Sample Demographic by Industry*

| Respondent Classification | Number of Respondents | Percentage of Respondents |
|---|---|---|
| Financial services | 30 | 43% |
| Communication and infrastructure | 14 | 20% |
| General and health insurance | 11 | 16% |
| Retail | 2 | 3% |
| Government organizations | 10 | 14% |
| Other organizations | 3 | 4% |
| **Total** | 70 | |

used to capture survey responses. The structured questionnaire elicited responses on the following:

- the conduct of risk assessments
- training and other awareness-raising programs
- validation and other preventative techniques
- detection programs
- investigation frequency
- passage of information (internally and externally)
- reporting of occurrences

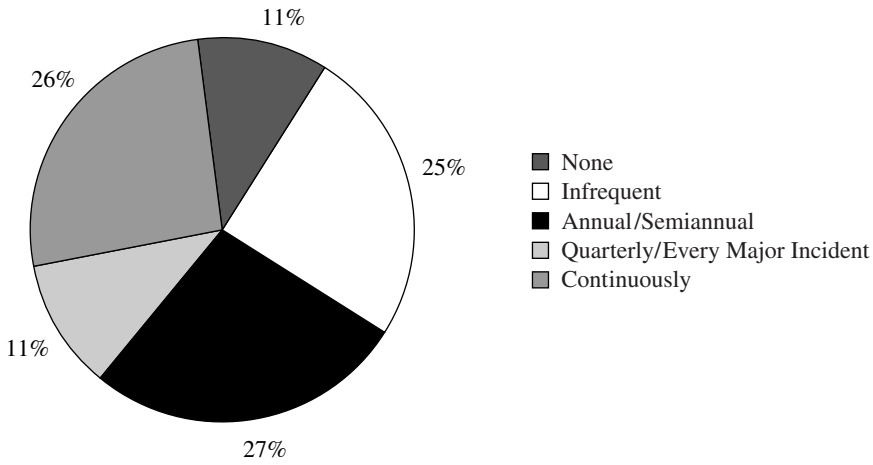
Subsequent to the questionnaire, a discussion of the issues faced by organizations in responding to identity theft was conducted. This was designed to elicit issues at three main levels: systemic factors such as legislation and responses from law enforcement; industry factors such as the volume of transactions that impinge on detection efforts; and organizational factors such as resource availability and the internal acceptance of the need for improved controls. The results of the questionnaire are presented and analyzed first, followed by a discussion of the issues and challenges confronting organizations in responding in the interest of the individual victims of identity theft.

## RESULTS

### Organizations as the Site of Identity Use (and Misuse)

To assess the extent to which organizations discharge their responsibilities given the potential for identity misuse, the research evaluated the (1) uptake and frequency of risk appraisals and assessments; (2) degree of

FIGURE 1
*Frequency of Identity Theft-Related Risk Assessments*




internal awareness raising; and (3) the nature and extent of preventative actions, processes, and controls.

Figure 1 reveals the frequency of identity theft-related risk assessments conducted by organizations and indicates the performance of such tasks on an annual or semiannual basis for the majority of participants. In fact, most of these assessments were the result of a risk assessment towards some other objective. For example, financial services institutions would perform risk assessments on online business, investigating, *inter alia*, hacking risks and the risks associated with checking credit histories in a real-time fashion. Similarly, a number of government organizations providing benefits and services were concerned with the risk of ineligible clients rather than identity theft per se. While not focused on identity theft, these risk assessments did indirectly consider identity theft and its organizational impacts.

Upon examining the extent of identity theft-related training of staff, most participants only conducted identity theft-related training during staff induction or not at all, as indicated in Figure 2. A small proportion claimed to provide frequent staff training on identity-related issues. Again, this was more prevalent in industries where the collection of identity documentation prior to transacting was a legislative requirement.

The converse trend appeared when evaluating awareness raising, as depicted in Figure 3. Over half the respondents raised awareness continuously or frequently, such as after every major identity theft event. In part, these results indicate that participants sought to supplement the absence of

FIGURE 2
*Extent of Identity Theft-Related Training Conducted by Organizations*

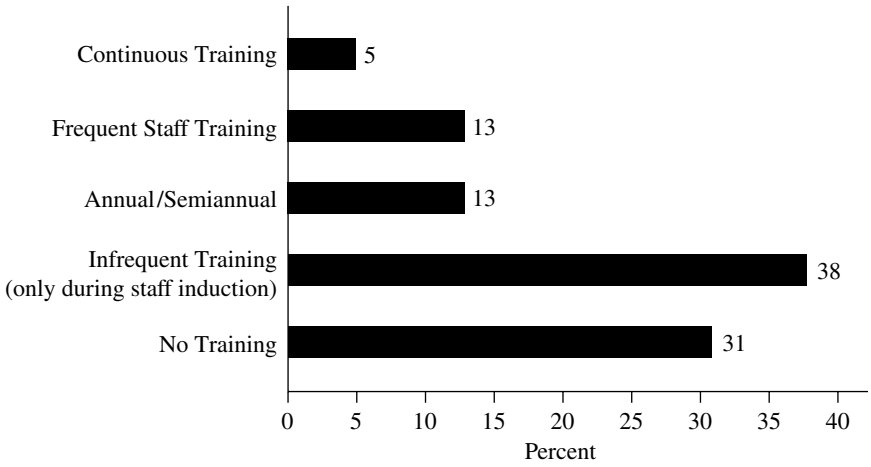
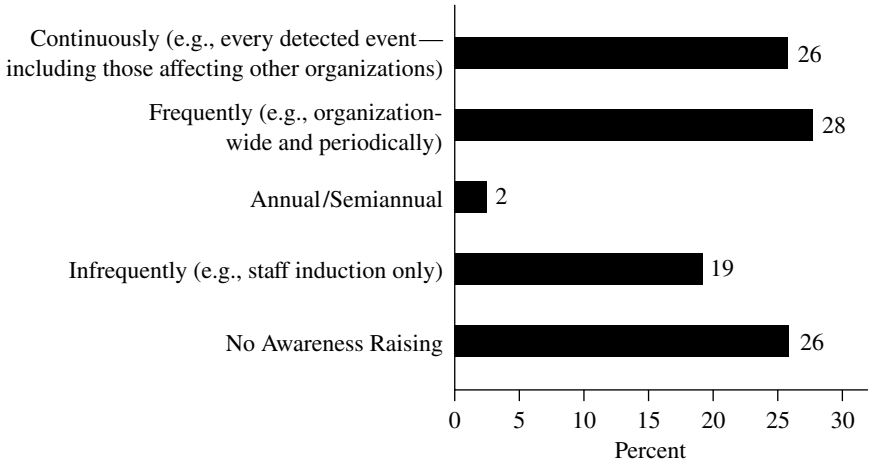
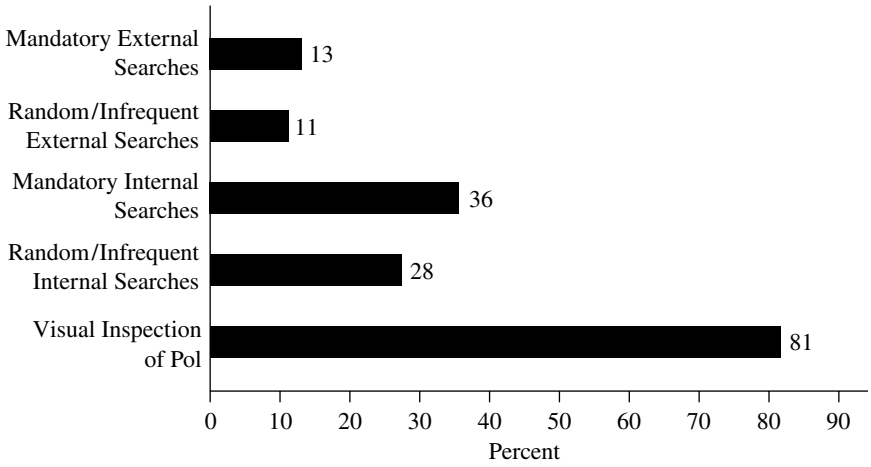



FIGURE 3
*Extent of Identity Theft-Related Awareness Activities Within Each Organization*




more routine training with ongoing alerts on the latest identity theft threats and manifestations. Issues for organizations included cost and availability of dedicated identity theft or fraud training programs, and the benefits of such training given high staff turnover levels in some industries and the extent to which existing business processes could be reconfigured to reflect increased identity theft competencies of staff.

FIGURE 4
*Participant Use of Prevention Controls and Processes*



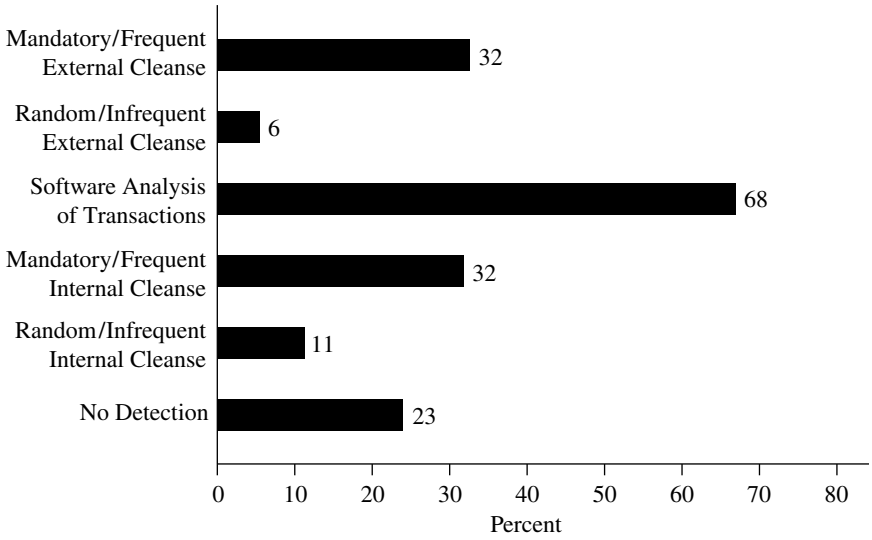

The final area of consideration in assessing the organizations' protection against identity misuse involves the controls in place when transacting with existing and new customers. As Figure 4 depicts, the most common forms of controls and processes include visual inspection of identity documents and tokens, such as birth certificates and driver's licenses. Some organizations indicated during discussions that certified, faxed, and photocopied documents and tokens were also acceptable, thus increasing the susceptibility to forgery.

The other most common type of preventative control involved the use of technologies to match identifying information against internal sources. The increase in validation services offered concurrently with the commoditization of identity information has resulted in increased data matching and verification processes among participants. Figure 4 also indicates that such processes are predominantly performed using existing internal databases, rather than those offered by identity brokers. However, discussions with participants indicated a strong intent to pursue external data validation options.

## Organizations as Detectors of Identity Fraud and Identity Theft

In assessing the role of organizations as *detectors*, this research considers the nature and use of processes and controls used to identify anomalous events, and whether organizations investigated these further, along with

FIGURE 5
*Participant Use of Detection Processes and Controls*




the level of internal data capture. As with prevention controls and processes, organizations as *detectors* implemented various physical and automated processes in seeking to identify and respond to anomalies or suspicious indicators. These included software analysis of transaction activities and database cleansing by external organizations.

Figure 5 provides an interesting comparison to the prevention activities performed by participants (Figure 4). It indicates that a greater uptake of data matching and cleansing is performed with external organizations after the transaction, as opposed to before. To gain further understanding of the likely reaction to these activities, participants were asked to indicate what percentage of the suspicious events and identifiers they chose to investigate. Surprisingly, 71% of respondents indicated that they investigate between 76% and 100% of all suspicious identity theft-related events. However, a further investigation revealed for the majority that this equated to making telephone inquiries only.

The empirical evidence presented points toward a high uptake of prevention activities, evidence of cross-referencing after the ensuing transaction, and follow-up investigatory work performed to establish whether an identity theft occurrence is the reason behind raised suspicions. This begins to paint a positive picture of the extent and levels of anticipatory activ-

ities performed by Australian organizations. Further consideration, however, is required of the discharge of broader social responsibilities.

## Organizations and the Social Imperative

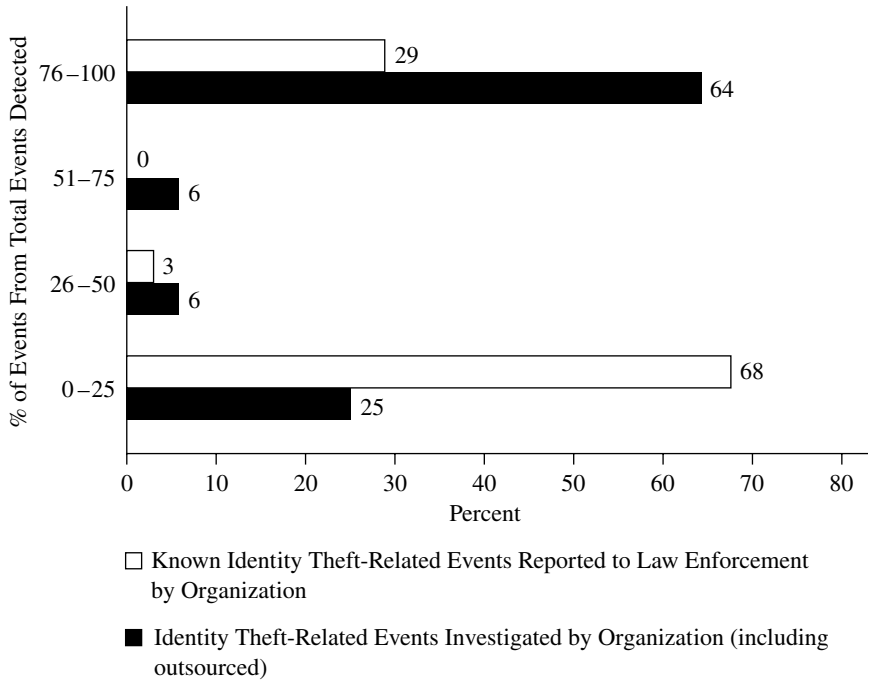
In assessing the acknowledgment and discharge of wider obligations, we considered the level at which organizations reported events to law enforcement authorities. As a victim, organizations may choose to write off the amount lost or seek to recover it through the use of third-party debt collectors. Indeed, these may be preferred alternatives based on cost-efficiency criteria and the notion that actions through the judicial system may be cumbersome and resource intensive and not yield outcomes in a timely fashion (Gayer 2003). Nonreporting may also occur due to perceptions that the admittance of identity theft occurring may adversely impact the organization's reputation (refer to Gal-Or and Ghose 2003, for similar arguments in relation to electronic crime). However, reporting to law enforcement facilitates the formal restorative processes for the individual victims as well as likely deterrence for perpetrators, and is hence reflective of wider societal obligations.

Providing some assessment of the discharge of the social imperative is the summary of results presented in Figure 6. These results suggest that while a clear majority of organizations within the sample indicated that between 76% and 100% of known or suspected identity theft or related fraud events were investigated by the organization (or outsourced to a third party for investigation), most of the events deemed to be identity theft or related fraud were not subsequently reported to law enforcement. When the total number of events detected was compared to the total number of events reported, a clear preference away from pursuing matters through the engagement of law enforcement and the judicial system is evident. In all, approximately 9% of the total detected identity theft and related fraud events provided by the sample were revealed by participants to have been reported to law enforcement.

These findings raise serious issues about the organization–individual victim dynamic of identity theft. The data collected indicates that, in seeking to reestablish their identities and gain judicial restoration, individual victims of identity theft are without the assistance of organizations. The extent to which these same organizations chose to inform known identity theft victims was not pursued.

In addition to the paucity of identity theft and related fraud reporting by organizations to law enforcement, less than half the sample indicated re-

FIGURE 6
*Percentage of Identity Theft-Related Events Investigated and Subsequently Reported to Law Enforcement by Victim Organizations*




ceiving identity theft-related information frequently, either on a formal or informal basis. Consequently, the extent of data capture and the ability to draw from the statistics generated on identity theft-related events experienced by the organizations limits the ability to learn from these events, seek to improve existing controls and processes, and ultimately, inform others dependent upon their documents, such as bank and utility statements. The following section explores possible reasons and influences in seeking to provide some context to the results presented.

## ISSUES AND CHALLENGES

Both internal and external influences exist that place pressure on the extent to which organizational victims act in response to identity theft events. Several issues and challenges exist that need further consideration in understanding the nature of organizational response to identity theft. These

can be both internal and external in nature, such as resource constraints, the nature and competitiveness of the industry, anticipated and likely response from law enforcement, and the complexity of understanding and applying privacy frameworks.

## A Lack of Resourcing

Like their international counterparts, Australian organizations rely upon their internal fraud groups to detect, investigate, and respond to identity theft occurrences. These groups in most cases are not well resourced, act in a support capacity, and on occasion are secondary considerations for input into changing processes, capabilities, and product and service offerings. For example, within the communications and infrastructure sector, the median number of fraud analysts (including managers) totaled three people, with an average of 65% of their time spent on identity theft-related work. Also of interest was the number of identity fraud and identity theft-related events per fraud employee. For this industry it was determined on average to be 395 detected events per fraud employee, reflecting the demands confronting these fraud groups.

Influencing this lack of reporting may be the relatively minimal resources being contributed to reacting to, and potentially learning from, these events when compared with what is being consumed in anticipation of identity theft and fraud. In fact, a cycle begins to emerge whereby organizations may implement controls and processes in anticipation of identity theft and fraud, but fail to adequately consider investigating and reacting to events subsequently detected. These observations indicate that the controls and processes employed by the majority of these organizations fail to evolve due to an absence of dedicated attention to exploring how criminals managed to exploit weaknesses and countercontrols.

## Growth and Efficiency Imperatives

The in-depth interviews revealed other internal influences that impact responses to identity theft. For example, marketing and sales departments would often offer lucrative incentives to transact or propose channel migration initiatives that would enhance transacting convenience—failing to understand the opportunities this could afford perpetrators of identity theft and fraud. Similarly, debt collection teams often wrote off bad debts without further enquiry as to the causes and without the involvement of fraud groups. This ultimately resulted in a portion of "undetected" identity theft

and fraud, and therefore, a lack of understanding about the real risks to processes, products, and services. For organizations, such outcomes are regarded as "cost-efficient," as highlighted in the situation of writing off unpaid credit card or mobile phone bills.

### Competitive Pressures

The survey design and sampling methodology sought to engage industries that offered products and services of high liquidity that were accessible to identity theft and fraud perpetrators. It became apparent that industries that suffered the most events and subsequent losses were often highly competitive (such as telecommunications and financial services), characteristic of a high-volume–low-value transactional environment. Participants revealed that they simply were not supported through resourcing to react to every event.

### Inadequate Law Enforcement Response

A number of issues were raised by participants about the lack of reporting of identity fraud and theft events to law enforcement. Firstly, most organizations thought that law enforcement response was inadequate. The time from reporting the identity theft or fraud, to the time of law enforcement investigation, subsequent prosecution, and outcome, was considered to be greater than 18 months by some participants. Secondly, organizations believed that the onus of collecting case briefs, interviews, witness and perpetrator statements, and other investigatory processes was on the organization, not law enforcement, consequently adding to the cost of the identity theft. Some participants stated that law enforcement would require a monetary fee to support additional investigations staff. In return, organizational victims would seek to sell information to authorities relating to particular events to assist them in other matters. The extent of these practices still remains unclear, but nevertheless indicates that the resourcing pressures evident with organizational victims is also applicable to law enforcement agencies.

### The Unclear Impact of Privacy Legislation

Varying degrees of understanding about issues surrounding privacy and identity fraud were encountered among participants. Operationally, some participants had developed arrangements whereby information sharing

about fraudulent identities was in place, reflecting their understanding and consideration of these issues. Evidence from participants indicated great diversity in the interpretation of the current privacy framework. A long debate surrounds the notion that privacy and control imposition are competing prospects. This has yet to be tested. The advent of biometric technologies, the extent to which organizations impose "know your customer" controls, and the provision of clear and direct guidance on privacy are all key issues requiring further exploration.

The above issues and challenges raise important questions for regulatory and public policy debate. Legislative introduction is one of the prevalent forms of change experienced in recent years in seeking to respond to the growing concerns about identity theft and identity fraud among Western countries. This type of change has manifested in diverse ways, including amendments to prescriptive legislation concerning the documents organizations must rely upon when verifying identities prior to transacting (e.g., the *USA Patriot Act* 2001; the *Financial Transaction Reports Act* 1988 [Australia]), in addition to the more obvious creation of specific offense categories (e.g., the *Identity Theft Assumption and Deterrence Act of 1998* [U.S.]). However, to date little is known about the impact of these legislative solutions, if any, in furthering organizational action on behalf of the interests of the individual consumer.

In fact, not only has the prescription of legislation and other regulatory impositions on organizations received little attention in both popular and scholarly work, so too has the analysis of the efficacy of measures put in place by policy makers in seeking to aid both organizational and individual victims of identity theft. In the absence of historical benchmarks both within Australia and overseas, it remains difficult to evaluate the effectiveness of such response measures. In the United States, as in the United Kingdom, Canada, Singapore, and a growing number of other countries, telephone line response centers, common affidavit and documentation frameworks, and the provisioning of specific identity theft offense categories, are beginning to emerge to assist organizations in providing identity theft victims with information on procedures that can help to reestablish their identity. However, where countries do have these measures currently in place, the goal appears to be one of improved information capture (see GAO 2002), rather than the evaluation of whether these mechanisms are both efficient and effective from the perspectives of the organizational victim and individual victim.

Although this study is unique in that it presents issues related to identity theft and, more generally, identity fraud from an organizational per-

spective, it also highlights the void in current research that seeks to identify synergies between profit-oriented action by organizations that in turn promotes identity theft mitigation—in other words, a common ground by which organizations can continue to strive for profits and other organizational goals, while simultaneously reducing the risk of identity theft occurring to their customers. To this end, great potential exists for future research to explore ways in which organizational strategy, such as Customer Relationship Management (CRM), can result in the achievement of socially responsible actions, such as identity theft mitigation, while maintaining an organization's overall aims of sales growth and, ultimately, profit gain. The extent to which organizations can reduce the incidence of being sites of misuse, and as it seems from the data, inaction, by applying theories and strategies that translate into individual consumer protection, requires a deeper understanding of each organization and the environment in which it operates. Contributing to this understanding would nevertheless help to inform debate as to the measures that organizations could adopt in seeking to mitigate the risk to the consumer.

## CONCLUSIONS, LIMITATIONS, AND FUTURE DIRECTIONS

The data analysis and discussion indicates that ensuring a responsible organizational response to identity theft and fraud for individual victims is complicated by many internal and external influences. Empirically the data provided reveal resource constraints, a lack of process and capability testing, and the predominance of activities performed in anticipation of identity theft and fraud. However, it was also revealed that shortcomings existed in the resourcing of those activities in reaction to identity theft- and fraud-related events, the paucity of reporting of events to law enforcement, and the subsequent moves towards identity theft and fraud *commoditization*. In all, the evidence obtained raises serious questions about the adequacy of response for individual victims in Australia, which can be applied on a global scale to organizations confronted by identity theft. Organizations are an inseparable part of identity theft, acting as users (and misusers), detectors and communicators, and consequently, possessors of an opportunity to act responsibly, which to a great extent has been overlooked by previous research.

In interpreting and generalizing the results of this article, its limitations must be considered. First, the survey is intentionally nonrandom, being focused on those industries that represent the highest identity theft risk for individual consumers. Within selected industries, however, the use of an

interview-based research method necessarily limited coverage of the population of organizations. While the targeting of research participants was based on ensuring the representativeness each industry's diversity, this remains a limitation to the generalizability of the results. A second limitation involves the unwillingness of participants to provide information on their actual response to identity theft where it may portray their organization in an unfavorable light or reveal sensitive information. While assurances of confidentiality and anonymity of response were made, respondent bias represents another risk to the validity of questionnaire and interview responses. Third, the results are based on observations of Australian organizations. While there is much to suggest that these issues transcend national and geographic boundaries, the extent to which they do so represents an area for further research internationally.

In sum, this article has provided evidence of the extent of organizational response to identity theft and fraud in Australia. As a consequence, a number of serious challenges to and pressures on organizations were identified. Addressing these requires consideration and assistance from other stakeholders, namely governments, industry bodies, and consumer advocacy agencies. Undoubtedly, organizations as "partner victims" of identity theft have an important role to play in supporting individual consumers as victims of this crime. Without their assistance, an individual victim faces the unenviable task of restoring his or her identity with little insights into how and where it was misused as well as the potential consequences of its misuse.

In considering how much responsibility and action is required from organizations as "stewards" of the identity of individual consumers, a number of important questions remain unanswered, as have been identified herein. Researchers can play an important role in identifying innovative approaches to measuring the performance of identity theft responses that already exist (or are beginning to emerge) in other fields, such as CRM, performance management, criminology, and the social sciences. The application of these will help to address the current and emerging challenge of assessing the effectiveness of identity theft response—the next step in understanding the organization–individual victim dynamic.

## REFERENCES

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

Commonwealth of Australia. 2000. The Changing Nature of Fraud in Australia. Canberra: Attorney-General's Department.

Cuganesan, Suresh and David M. Lacey. 2003. *Identity Fraud in Australia: An Evaluation of Its Nature, Cost and Extent*. Sydney: Standards Australia.

*Enhanced Border Security and Visa Entry Reform Act* (U.S.). 2002. HR 3525.

Executive Committee of World Business Council for Sustainable Development. 2002. The Business Case for Sustainable Development: Making a Difference Towards the Earth Summit 2002 and Beyond. *Corporate Environmental Strategy*, 9 (3): 226–235.

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

———. 2003b. *Identity Theft Survey Report*, United States, September. http://www.ftc.gov/os/2003/09/synovatereport.pdf.

*Financial Transaction Reports (FTR) Act* (Australia). 1988.

Gal-Or, Esther and Anindya Ghose. 2003. The Economic Consequences of Sharing Security Information. Paper presented at 2nd Annual Workshop on Economics and Information Security, Maryland, May 29–30.

Gayer, Jennette. 2003. *Policing Privacy: Law Enforcement's Response to Identity Theft*. California: Californian Public Interest Research Group.

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

———. 2002. *Identity Theft: Prevalence and Cost Appear to Be Growing*. Report to Congressional Requesters, GAO-02-363.

Givens, Beth. 2000. Identity Theft: The Growing Problem of Wrongful Criminal Records. Presented at SEARCH National Conference on Privacy Technology and Criminal Justice Information, Washington, DC, June 1.

Graycar, Adam and Russell Smith. 2002. Identifying and Responding to Electronic Fraud Risks. Presented at 30th Australian Registrars' Conference, Canberra, November 13.

Home Office (U.K.). 2003. National ID Card Scheme to Be Introduced. Media Release 307/2003, November 11. http://www.homeoffice.gov.uk/n_story.asp?item_id = 675.

*Identity Theft Assumption and Deterrence Act of 1998* (U.S.). Public Law 105–318.

Maignan, Isabelle, Bas Hillebrand, and Debbie McAlister. 2002. Managing Socially-Responsible Buying: How to Integrate Non-Economic Criteria into the Purchasing Process. *European Management Journal*, 20 (6): 641–648.

Main, Geoff and Brett Robson. 2001. *Scoping Identity Fraud*. Canberra: Commonwealth Attorney-General's Department.

Matejkovic, John E. and Karen E. Lahey. 2001. Identity Theft: No Help for Consumers. *Financial Services Review*, 10: 221–255.

May, George. 2002. Stop Thief! Are Credit Bureaus and Creditors "Silent" Co-Conspirators to Identity Theft? *Journal of Texas Consumer Law*, 5 (3): 72–80.

Moore, Ariana-Michele. 2002. ID Theft: Asia's Credit Bureaus Need More Proactive Role. *The Asian Banker*, October: 1.

Newson, Marc. 2002. Is Non-Financial Reporting Bottoming Out? *CA Charter*, 73 (7): 13.

Silverman, David. 1970. *The Theory Of Organizations*. London: Heinemann Education.

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

Turner, Mark. 2001. Emphasis Put on the "Triple Bottom Line." *Financial Times* [London], February 8.

*USA Patriot Act*. 2001. Public Law 107–56.

Willox, Norman A., Jr., and Thomas M. Regan. 2002. Identity Fraud: Providing a Solution. *Journal of Economic Crime Management*, Summer, 1 (1): 1–15.