Small business scams: a preliminary overview and investigation.

*Paull C. Weber, Ph.D.**
Lecturer, School of Management, Curtin University

Michael T. Schaper, Ph.D.
Adjunct Professor, School of Management, Curtin University

Stephen Teo, Ph.D.
Professor, School of Management, Curtin University

Louis Geneste, Ph.D.
Lecturer, School of Management, Curtin University

This paper provides an overview of the current level of understanding about scams perpetrated against small businesses, and also reports on a preliminary study which highlights various forms of the phenomenon. A scam is a form of fraudulent, illegal activity that invites potential victims to accept an offer which leads to the loss of financial, organisational or personal resources. The limited research evidence available to date suggests that small businesses are particularly vulnerable to this type of criminal activity, are less likely to report such events, are likely to be subject to repeat attacks, and are particularly susceptible to online approaches. The ten cases reported in this paper are suggestive of a relatively high level of occurrence and a surprisingly high level of ignorance of the risks that these scams represent. A future research agenda is outlined.

* Corresponding author Email: p.weber@curtin.edu.au

Businesses, like individuals, are sometimes the victims of crime. Yet, the current level of interest in, or knowledge about some crimes types committed against small business is very limited. There is one category of illegal activity in particular that can potentially touch all small firms, the business scam.

This paper provides an overview of the current state of knowledge about small business scams. It attempts to provide the reader with an understanding of the key issues surrounding scam activity, and begins by first defining the nature of a so-called "scam". It then outlines the different forms that a scam can take, some possible reasons why small firms are particularly susceptible to scams. It then presents some preliminary data

identifying the relatively high prevalence of scams, as well as a surprisingly high level of ambivalence and/or ignorance of the risk of being scammed in the small business community.

What is a scam?

The term "scam" is a relatively recent one, with some etymological researchers suggesting that it first appeared in the early 1960's, originating in entertainment carnival slang or argot (Dictionary.com 2010). Other sources, however, suggest that the history of the term is more obscure and poorly understood (Oxford English Dictionary 2010). Regardless of origin, the term "scam" connotes an arrangement, proposal or other activity which is, in some way or another, of dubious value or repute. As the online Dictionary.com site suggests (2010), it is "a confidence game or other fraudulent scheme, especially for making a quick profit; [a] swindle."

The UK Office of Fair Trading (2006: 12) has noted that there is no single definition of the word, and adopts a working explanation of such activity as "…an act of persuasion based on misrepresentation…a misleading or deceptive business practice where you receive an unsolicited or uninvited contact and false promises are made…"

A similar meaning has been put forward by the ABS (Australian Bureau of Statistics) (2008: 5), who suggest that it is "…a fraudulent invitation, request, notification or offer, designed to obtain someone's personal information or money or otherwise obtain a financial benefit by deceptive means." This latter definition explicitly introduces the notion that a scam is not simply an attempt to illicitly remove money from a potential victim: it can also include the misappropriation of personal information or other resources, which the scam operator then utilises for his or her own advantage at the expense of the victim.

However the definition may have evolved, the word is, almost inevitably, closely aligned with the concept of "fraud." Grabosky (1991: 9) proposes that this latter term refers to "…a dishonest and deliberate course of action which results in the obtaining of money, property or an advantage to which the recipient would not normally be entitled." Dictionary.com (2010) defines a fraud as "any deception, trickery," and a "breach of confidence, perpetrated for profit or to gain some unfair or dishonest advantage."

At first glance the two terms may appear to be similar and interchangeable. Indeed, they are sometimes used as synonyms of each other. This overlap is understandable, given that both scams and frauds seek to mislead and take advantage of their victims, often arise from the same underlying factors, and can sometimes be dealt with using the same preventative measures. However, there are some important differences between the two concepts of fraud and scam.

As the ABS definition suggests, a scam is a more limited type of dishonest action, based upon an *invitation to participate* in an activity. Victims are encouraged, mislead or induced to voluntarily interact with the perpetrator, and ultimately to willingly surrender over money, information or other valuable resources. In a scam arrangement, this requires the victim to accept and act upon the invitation; the victims' active participation is necessary before the deception can take place. Unlike a fraud, if the intended victim does not accept the offer, the scam cannot occur.

Another major point of difference is the origin of the illegal activity. A scam is always an *external* attack upon an individual or business; the perpetrator is not part of the organisation which he or she seeks to deceive. We therefore conceptualise the following scam definition: *A scam is perpetrated by an entity external to the business. The owner or another delegated decision maker within the business must in some way play an active yet*

unwitting role to participate in the deception, which ultimately leads to the loss of financial, organisational or personal resources.

The limited evidence which does exist appears to suggest that the level of victimisation is much greater for businesses than for households – in other words, business organisations are more likely to be a victim of crime than is a member of the general public (Fischer & Looye 2000; Hopkins 2002). Whilst such generalisations apply to the incidence of crime at large, in the end it may well be that the same also holds true in regards to the sub-set of scams.

Types of scams

Potential small business scams come in a variety of different forms. Classifying such activities can be somewhat problematic, as the nature of this behaviour often changes in response to the introduction of new technologies, regulatory prohibitions, active policing of fraud laws, and new consumer demands and preferences. Scam perpetrators are often also highly adept at quickly changing and adapting their schemes, which makes classification a continuing challenge.

There is considerable overlap between scams perpetrated against members of the general public and those against small firms and the self-employed, and many enforcement agencies can be seen to treat or report these scams in the same way (UK Office of Fair Trading 2006). Table One provides a summary of some commonly-encountered scams that nominally separates them into those that usually (but not exclusively) target the general public, small enterprises, or both groups of potential victims.

Table 1
A selection of common scams

Consumer-targeted	Chain letters Fake lottery (sweepstakes) winnings Investment scams Miracle cures/potions Mobile phone scams Nigerian fraud (money transfer) Online fake offers, auctions and prizes Pyramid schemes
Targeted at both small business and consumers	Boiler Room investment scams Employment opportunities/guarantees Fake charities Fake invoices Faxback/premium telephone call-backs Identity theft Phishing, banking & online account scams Unauthorised credit card use Work-from-home schemes
Small business-specific	Advance fee fraud Business opportunities Bust-outs Cramming Fake business directory entries False domain name registrations False magazine advertisement invoices Misleading invoices for office supplies Overpayments

A preliminary overview of scam categories has been conducted by the Australian Bureau of Statistics (2008), who have identified the following types of scam commonly used on consumers:

Financial advice: The provision of unsolicited financial product service offerings in the guise of information assistance, such as share purchases, investment seminars, real estate purchases, or other related financial transaction.

Chain letters: An invitation to send money to another recipient and forward the same letter on to other potential victims, on the presumption that they in turn will send money.

Phishing and related requests: An attempt to assume the on-line identity of a legitimate organisation (such as a bank or government agency), with the intent of convincing users to provide personal or organisational information such as bank account details, email addresses, and/or passwords. Variations of this scam include voice-based ("vishing") and SMS ("smishing") deceptions (House of Representatives 2010).

Advance fee fraud: An arrangement where a victim is promised a large return if they provide an initial upfront financial payment to the scammer. This is often also known as a "Nigerian fee scam" (House of Representatives 2010).

Lottery winnings: A hoax offer to share in the proceeds of a lottery if the victim surrenders over personal and banking information.

Pyramid schemes: Victims pay a fee to join a scheme in which subsequent earnings are dependent upon the prey also successfully recruiting other victims into the programme.

In addition to these, there are also a number of scams which are more specifically focussed on business operators:

Office supplies: An arrangement in which a scammer provide goods to the victim business, and charges for them, without the initial consent of the firm. These usually involves items that the firms regularly orders, giving rise to a misleading impression that the goods have been ordered from the genuine, legitimate supplier (ACCC 2008).

Directory listings and advertisements: An unsolicited request to pay for an advertisement in a magazine relating to, or to be listed in a directory relevant to, an industry. The advertisement and/or magazine in question is usually non-existent (ACCC 2008).

Internet and business registrations: Misleading letters and invoices issued to a business operator, claiming or requesting payment in return for registration of a business name,

internet name, or trademark that is similar to, but not identical with, the firm's genuine name (ACCC 2008).

Cramming: An invitation for the business operator to confirm basic business information (such as address and telephone details), accompanied by an offer to participate in an allegedly free service. The victim business is then enrolled in the service, but unknown to them, a fee is then charged for the service via the victim's telephone account (Gull 2004).

Self-employment projects: These are spurious offers to help an individual start trading as a one-person business (such as a resume-writing bureau), provided the victim pays the scammer a fee for information and initial potential clients; the clients and information are rarely provided (ACCC 2008).

Business valuations and prospective sales: This involves an approach to a firm enquiring if the proprietor is interested in selling the business, and solicitation of payment to obtain a valuation of its selling price. This fraud is targeted at business owners who wish to exit their current business venture. If the owner shows an interest in selling the firm, the fraud involves collecting a large payment from the owner in order to have a business sales price determined by the fraudster. Once the valuation has been performed and the fee paid by the business owner, the fraud perpetrator ceases all contact (Mintzer 2007).

Bust-outs: An invitation by a scammer to sell goods to a business entity operated by the scam artist. The scammer does not pay for the goods and eventually (when no more credit can be sourced) files for bankruptcy. The scammer then sells the goods on to another unsuspecting victim (Henderson 2003).

Overpayments: An arrangement in which a scammer orders goods or services electronically or by mail from a small business, but pays more than the required price for the product. The victim business is then contacted and asked to remit the difference back to the scammer, who subsequently turns out to be a non-existent business which has made its

original payment using an invalid, stolen or otherwise illegitimate credit card or bank account (Mintzer 2007). This kind of scam typically requests that the overpayment is refunded via a method that results in cleared funds being quickly made available to the scammer before detection occurs (ACCC 2010).

"Boiler room" financial and investment scams: These sophisticated and highly organised scams consist of a managed team of sales people who cold-call potential investors (victims), often claiming to operate out of financial centres such as Tokyo, London and New York. Their actual operations have been traced to countries such as Thailand and the Philippines. The business typically offers an investment opportunity and follows up with sophisticated prospectuses and web site details that lull the investor into a false sense of security and familiarity. It is not uncommon for individuals to hold more than one bogus investment with the organisation before the deception is discovered (Australian Securities and Investment Commission 2002).

Small business prevalence and reporting of scams

It has been suggested that the characteristic features of the small business sector make such firms more likely than large corporations to be the victims of scams, frauds, and other forms of crime (Masural 2004). There are a number of general interest publications in the business media that warn of potential scams (see, for example, Henderson 2003), but relatively few scholarly refereed publications (Taylor 2002).

Small business commentators and researchers claim that a small business is more likely to be scammed due to their less sophisticated prevention and detection mechanisms (Clout 2010; Perrone 2000) and financial recordkeeping and accounting controls (Wells 2003). In addition, the relatively thin profitability of most small firms can make it difficult to absorb the costs of a significant financial loss (Federation of Small Businesses 2009).

Moreover, small privately held firms are not subject to regular outside audit, thus removing a layer of external scrutiny (Wells 2003).

Evidence also suggests that businesses are relatively unlikely to report a crime event (Taylor 2002; Australian Institute of Criminology 2003). In the United Kingdom, for example, less than five percent of persons approached by a scam subsequently report this to authorities (UK Office of Fair Trading 2006). Similar behaviours have been observed in the USA, where it is estimated that only 15 percent of cyber-crime is reported to any law enforcement agency (Rantala 2008).

In part, this may be due to simple embarrassment at having been "caught out" or fooled by a con artist (House of Representatives 2010). It may also be due to the owners being unable to find the time to lodge a report (Perrone 2000). Another barrier to reporting is cynicism of the impact that their reporting effort will have upon the perpetrators (Taylor 2002; Federation of Small Businesses 2009). Finally, there may also be a concern amongst some owners for the likely rate increase that reporting the event may have on business insurance premiums (Mirrlees-Black & Ross 1995).

Armed with the general typology of scams as described and an understanding from the literature of small business scam reporting and prevalence the paper now examines some new data on scams within small businesses. The purpose of this preliminary research is to identify whether the typology proposed is operationally adequate and whether the challenges identified from the literature are evident in the field.

Methodology

Measuring the types, frequency and impact of small business scams is a somewhat difficult exercise at present. There are a number of different factors which can impact on the validity and reliability of scam research, and present some methodological barriers to

prospective researchers. Determining the cost of scams is also problematic. Some respondents may be inclined to report the opportunity cost of a scam (that is, the financial benefit they have foregone when they realise a promise made to them will not eventuate), whilst others focus on the actual cost of the scam to them (which can be measured by the money that they have actually outlaid, such as payment of fake invoices).

Given that scams are based on deception, fraudulent activity and misrepresentations, a victim of a scam may not realise that they have suffered a loss or other form of damage. In some cases, the scam in question may not be detected until well after the event, and so fall outside the reference period of any single timeframe study (ABS 2008). Notwithstanding these limitations, the data used provides an interesting first analysis of the scam phenomenon in Australian small business.

The data for this paper was collected as part of a broader small business benchmarking exercise. The businesses were all located in Western Australia and asked to provide information about what (if any) scams they had been exposed to, whether they had responded to such offers, and what loss they may have incurred as a result. These same respondents provide a range of other demographic and behavioural data for the benchmarking exercise and selected variables were used to compile a description of each case.

As a consequence of using of the benchmarking survey tool to gather this data, the sample frame was by design limited to the same criteria: non-government, for-profit small businesses employing less than 20 people that were registered in Western Australia. The data was collected using an online data collection method and respondents were recruited using a variety of industry organisations and available databases of WA small businesses (see www.smallbusinessbenchmarks.com and www.business.curtin/WASBB for further detail).

Results

Thirty two useable responses were received prior to the publication deadline for this paper. There were 18 male and 14 female respondents with an average age of 46 and an age range of 27 to 63. Results were recorded from 30 different industry classifications with two representatives from general management consultancy and information technology IT professionals. In terms of business structure, 21 had one only one owner, nine businesses had two owners and there were two businesses with more than two owners. The legal structure Pty Ltd (proprietary limited company) was most common (18 respondents) followed by nine sole traders and five partnerships. Ten of the respondents also offered more detail on their scam experience from an open ended question that asked them to describe the form and size of loss from any scam ever committed against them. The case particulars of these ten open responses are reported and briefly described below.

Case 1

A male information technology (IT) consultant born 1968 in Australia, educated to Year 12, with a female partner possessing an MBA. The business has a Pty Ltd (private proprietary limited) company structure and the partners work a combined 75 hours per week over five days. The business is home-based and had been running for four years. Annual turnover was $200,000 in 2010.

> *We purchased some technical books form a website adding up to about $200. We then went to use the card at a service station and the card had been over drawn. Our computers had been scrapped for usernames and fortunately the only ones they managed to use were the ones for the online book store. They tried to login and purchase all the books in the store totalling $2500 but the card was cancelled for unusual use. There was only the cost of cleaning our computers and upgrading our systems and software.*

Case 2

A male management consultant born 1954 in Australia, possessing post graduate qualifications (unspecified), with a female partner educated to MBA and Masters. The business has a Pty Ltd company structure, working an estimated 70 hours each week in a five day working week. This is a consultancy service based business that has been running

for 12 years with an annual turnover of $400,000 in 2010. This owner seemed quite confident that they were detecting scams before any loss was incurred.

> *I only see usual transparent internet scams, nothing else.*

Case 3

A male financial advisor born in 1957 in the United Kingdom who possesses a bachelor's degree in commerce, working a very high estimated 110hrs per week. The business has a Pty. Ltd. company structure and has been running for 16 years with an annual turnover of $700,000 in 2010. Similar to Case 2 this owner was quite dismissive of the risk of being scammed. Interestingly, this owner considered non-payment of invoiced accounts as a scam, believing that this was often done with prior fraudulent intent.

> *Apart from people not paying bills (probably never intended to), I have not had a problem with scams.*

Case 4

A female owner of a corporate travel agency born 1946 in Australia, educated to year 12. The business has a Pty Ltd company structure and trades for 40 hours per week to create an annual turnover in 2010 of $5,560,000. This business has experienced a significant scam event and was quick to report it to the police and persistent in following through to successful prosecution.

> *We were targeted by a user of fraudulent credit cards. We rarely engage with clients not known to us but in this instance the scammer was able to slip through our net as such. The cost to us was approximately $10,000. I tracked his movements through airline tickets we had issued for him and alerted the Australian Federal Police to his whereabouts. He was arrested, charged and is now serving a jail sentence. I prefer to think I was "chosen" to help bring the man to justice.*

Case 5

This female owner of a pet supplies and grooming business was born in 1984 and possesses a diploma level qualification. She has been operating the business for six years as a sole trader, working an estimated 60 hours each week in a six day week. Annual turnover of $42,000 was recorded for 2010.

> *I have had advertising companies ring saying I have agreed to advertising when I have not, then they send me to debt collectors, only when I advise them of ACCC involvement I hear nothing more from them.*

Case 6

The owner of this business is a female information management consultant born 1959 in the United Kingdom with post graduate qualifications (unspecified). She works 25 hours per week in this Pty Ltd. business for five days per week. She has owned and operated the business for 25 years and generates an annual turnover of $1,000,000. The owner seems to consider it her banks responsibility to deal with small scams committed against her (using her business credit details).

> *The company had supported some small community newsletters with small ads and our credit card was debited for an advert that had never been approved or occurred. It was only for $250. I queried it with the credit card company, gave them all the details and indicated that I would not take legal action as it would cost me more to do so that the amount I had been scammed. The credit card company dealt with the matter.*

Case 7

A female bridal and formal wear retailer born 1966 in Australia who possesses a bachelor degree (unspecified), with a male business partner educated to Year 12. The business has company and trust structure and the owners collectively work 50 hours per week over six days. The business turned over $400,000 in 2010. The current owners commenced trading in 2006. Although this business has previously lost business funds to a scam, they chose to report the event to a consumer protection agency, not the Australian Competition and Consumer Commission (ACCC).

> *Have had a number of "publications" contact the business stating that an order has been placed for advertising and the invoice needs to be paid. Initially, I signed up for a couple of these assuming they were legitimate! Total cost approx. $1000.00 and lots of time! I was told by another business owner that had experienced similar scams what they were and consequently did not fall for it again. I also contacted Consumer Affairs to report the scams and they referred me onto the appropriate authority. As the scams were mostly coming from Queensland, I spoke to somebody there. They seemed to be aware of the scam and took the details I gave them.*

Case 8

A male owner of a business registration advisory service, born 1950 in Australia who possesses a diploma level education). The female business partner born 1955 was educated to a certificate level at a technical college. The owners work a combined 50 hours per week in their Pty Ltd company to generate a turnover of $700,000 in 2010.

> *We have had the general "advertising" type scams and some using our online order forms. I have not tried to determine the time used to recognise and deal with the scams or reporting where we have determined necessary. Actual dollars lost I estimate to have been less than $2,000.*

Case 9

A male respondent born 1975 in Zimbabwe, educated to year 12 high school owns and operates an IT consultancy company (Pty Ltd) for 50 hours per week for nine years, generating a turnover of $1,300,000 in 2010

Our company credit card was frauded to the value of $300AUD.

Case 10

A male specialist electrical goods retailer born 1982 in a British Indian Ocean Territory who possesses a bachelor degree (unspecified), with a female business partner, also born 1982 and also holding a bachelor's degree. The owners worked a combined 120 hours to generate a turnover of $800,000 in 2010.

We have not lost any money, but waste some time with detection of scams.

Eight of these ten cases could be adequately classified within the scams typology developed, whilst two cases proved problematic. Case 9 used the term 'frauded' but the use a "company credit card" confirms it was a scam given that the owner is the sole director of his firm and does not have any employees. The other case that did not fit clearly within the definition of scams adopted was case 3 who could not differentiate between intentional non-payers (of outstanding accounts) and all other creditors who did not pay. This was a limitation of the survey instrument used, which (intentionally) did not provide respondents with a definition of a scam during this exploratory phase of the research.

Findings

The results show that 25 percent of respondents (eight from 32) have fallen victim to some form of scam activity within the past year. Another notable finding is that only 50 percent (16 cases) could confirm they had not been the victim of a scam within the past year, the remaining 25 percent (eight cases) were unsure. These preliminary findings do not allow more than speculation on why one quarter of the sample was unable to confirm

or deny that they had been scammed. It remains to be discovered whether they were confused, unconcerned, unable to detect, simply ignorant of scams or whether some other factors were at play.

Regardless of the cause or combination of causes, it would seem that this uncertainty is clearly deserving of further more targeted research. The unsure group would be of particular interest to law enforcement and scam prevention agencies as an opportunity to educate and raise awareness of small business scams.

Another notable difference between the yes, no and unsure groups was the turnover of the business. The average turnover of those who had been scammed in the past 12 months was $1,512,000 and a lower $986,000 for those who had not been scammed, compared to just $230,000 for the unsure group. If these numbers are indicative of a wider trend then it would seem that larger turnover businesses (and industries) offer more opportunities for scammers.

Only one of the eight yes respondents (12.5 percent) had a post graduate qualification whereas five of the sixteen (31.25 percent) non scammed respondents had post graduate qualifications. A further two owners who identified scams that they had experienced more than 12 months ago had post graduate qualifications. No inference should be drawn from the proportions observed in such small samples and further data would be required to make any claims of statistical significance/correlation. However,on

the face of it if these proportions hold true in larger samples it seems that tertiary education may lead to less risk of being scammed.

Case 6 clearly felt that responsibility for follow-up and action rested with their bank, not with the company or with enforcement agencies. This externalisation of responsibility may have an adverse effect upon the ultimate likelihood of small scale scams being reported.

Investigating beyond the question related to the prior 12 months, longer term losses were identified by 10 of 32 respondents that ranged from non-financial loss of efficiency through wasted time (case 10), to one case where over A10,000 had been lost in a single transaction. Because of sample size limitations, we cannot reliably extrapolate these findings to the entire small business community. However, as has been demonstrated, these responses came from a wide variety of business types, structures, owner demographics and industries. Therefore it would seem reasonable to assert that if these reported prevalence and severity of scams are at all representative of the wider small business population, then it would seem a fertile and important area for further research effort.

Future research

The results of this small preliminary study indicate that there is a high level of impact of scams upon small firms. The overall quantum of scam approaches made to small businesses continues to increase on a year-by-year basis (ACCC 2009). Despite the pervasive and probable significant nature of this business problem there is still much more that needs to be known about the nature of small business scam activity, how it operates, and its impact on firms. This is a field where timely research can assist policymakers, enforcement agencies, and small business organisations. As a possible starting point, the following avenues are all considered worthy of further investigation:

Which scams are prevalent? What are the most common types of scams? More data is needed to confirm whether or not this.

Does the nature of scams change from one time period (year) to another? To what extent do new scams emerge, and how long do existing scam practices remain in existence?

What is the impact of scams on the business? Measuring the actual dollar loss suffered by firms needs more analysis. This is especially important because many micro-firms and small businesses operate on low levels of turnover and net profit, and even a small financial loss to a scam can have a significant impact on their viability. In addition, it would be worthwhile examining what (if any) non-monetary costs a scam imposes on a business – such as loss of time in reporting and dealing with its consequences, the expense of devising new preventative strategies, and so forth.

Are some firms more likely to be victims than others? Previous researchers working in the area of crimes against small business, such as Fisher & Looye (2000), have already noted that a greater understanding is needed of the impact of firm size, location and other variables on the propensity to become a victim of crime. Developing an effective profile of potential scam victims could make it easier for enforcement agencies to work against future scam operations.

Are some industry sectors more prone to scam activity than others? Previous studies of crime in the small business sector (such as that by Perrone 2000) have shown that different types of commercial activity can be more, or less, susceptible to attempted illegal activity. Are particular business categories especially exposed to scams – and if so, which sectors are they and why?

Why do some owners and managers of small businesses fall for scams whilst other owners in a similar circumstance do not? There may be cognitive and/or behavioural differences

between groups that fall prey to a scam and those who do not. Discovering who these at risk groups are would allow a more focussed prevention strategy to prevail.

Revictimisation. Are scam victims more likely to become repeat victims, as some previous business crime research suggests (Perrone 2000), or are they likely to become "inoculated" against future attempts once they have already had to deal with the impact of being a scam target?

Who perpetuates scams? Fascinatingly, little is known about the individuals and organisations who attempt to scam small firms. Who are they, and why do they choose SMEs as their prey?

In addition to the specific questions raised above, researchers may also need to consider the most effective way to investigate small business scams. The existing literature and some of the evidence in this research has suggested that there is some reluctance by small business owners and managers to report being part of a scam. Are there particular methodological approaches which are more likely to result in greater response rates? Ideally, such tools should also encourage full, open disclosure, yet not be overly intrusive or time-consuming for the business operator.

Conclusion

Scamming is a persistent and comparatively widespread activity, and one which is very likely to continue to afflict the small business community for the foreseeable future. Scams can take a variety of different forms, and some of the particular characteristics of SMEs make them especially vulnerable to becoming victims. This paper has outlined what a small business scam is, many of the types of scam that exist and begun the task of understanding the prevalence and nature of this event within a small business context. However, there is still a significant paucity in the level of knowledge about scamming in

the small business community, and a consequent need to understand, measure, validate and track a number of key aspects of scam activity.

References

Australian Bureau of Statistics (2008) *Personal Fraud 2007*, Cat. No. 4528.0, Canberra: Australian Bureau of Statistics.

Australian Competition & Consumer Commission (2008) *The Little Black Book of Scams*, Canberra: Australian Competition & Consumer Commission.

Australian Competition & Consumer Commission (2009) *Targeting Scams: Report of the ACCC on Scam Activity 2009*, Canberra: Australian Competition & Consumer Commission.

Australian Competition & Consumer Commission (2010) *Scamwatch: Cheque Overpayment Scams [online]* <www.scamwatch.gov.au/content/index.phtml/tag/ChequeOverpaymentScamsCanberra> Accessed Sept 23rd, 2010.

Australian Institute of Criminology (2003) "Reporting of Crime against Small Business" *Crime Facts Info* No. 43, issued 18 February. Canberra: Australian Institute of Criminology.

Australian Securities and Investment Commission (2002) *International cold calling investment scams*, Canberra: Australian Securities and Investment Commission <http://www.asic.gov.au/asic/asic.nsf/byheadline/ASIC+Service+Centre+Addresses?openDocument> accessed on April 16th, 2011.

Clout, J. (2010) "SMEs Most Vulnerable to Fraudsters" *Australian Financial Review*, Tuesday 17 August, p.45.

Dictionary.com (2010) [online]< http://dictionary.reference.com/browse/scam > accessed 4th August 2010.

Federation of Small Businesses (2009) *Inhibiting Enterprise: Fraud and Online Crime Against Small Businesses* London: Federation of Small Businesses.

Fischer, B. and J. W. Looye (2000) "Crime and Small Businesses in the Midwest: An Examination of Overlooked Issues in the United States" *Security Journal* 13(1), 45–72.

Grabosky, P.N. (1991) *Controlling Fraud, Waste, and Abuse in the Public Sector*, Canberra: Australian Institute of Criminology.

Gull, N. (2004) "A Scam to Watch Out For" *Inc*, 26(4), 31.

Henderson, L. (2003) *Crimes of Persuasion: Schemes, Scams, Frauds* 2nd edn. Azilda, Ontario: Coyote Ridge Publishing.

Hopkins, M. (2002) "Crimes Against Businesses: The Way Forward for Future Research" *British Journal of Criminology* 42(4), 782–797.

House of Representatives Standing Committee on Communications, Parliament of Australia, *Hackers, fraudsters and botnets: Tackling the problem of cyber crime – the report of the inquiry into cybercrime* (2010) <http://aph.gov.au/house/committee/coms/cybercrime/report/full_report.pdf.> Accessed 14th March 2011.

Masural, E (2004) "SMEs and Crime: Evidence from the Netherlands" *International Small Business Journal* 22 (2), 197–205.

Mintzer, R. (2007) "Common Small Business Scams" *Entrepreneur*, January 25 [online] <http://www.entrepreneur.com/management/legalcenter/article173648.html> accessed 8th October 2010.

Mirrlees-Black, C. and A. Ross (1995) "Crime Against Retail Premises in 1993" *Research Findings* No. 26, December, London: Research and Statistics Department, Great Britain Home Office.

Oxford English Dictionary.com (2010) [online] (accessed 18th September 2010).

Perrone, S. (2000) "Crimes Against Small Business in Australia: A Preliminary Analysis" *Trends and Issues in Crime and Criminal Justice*, no. 184, Canberra: Australian Institute of Criminology.

Rantala, R. (2008) "Cybercrime Against Businesses, 2005", *Bureau of Justice Statistics Special Report* NCJ 221943, Washington DC: U.S. Department of Justice, [online] <http://bjs.ojp.usdoj.gov/content/pub/pdf/cb05.pdf > accessed 21st Sept 2010.

Taylor, N. (2002) "Reporting of Crime Against Small Retail Businesses" *Trends and Issues in Crime and Criminal Justice*, no. 242, Canberra: Australian Institute of Criminology.

UK Office of Fair Trading, United Kingdom (2006) *Research On Impact of Mass Marketed Scams: A Summary of Research Into The Impact of Scams on UK Consumers*. Publication OFT 883. London: Office of Fair Trading.

Wells, J.T. (2003) "Protect Small Business" *Journal of Accountancy* 195(3), 26–32.