Small Business SCAMS

▲ NATIONAL SURVEY 2012/13

Dr Paull Weber & Dr Louis Geneste

Curtin University, School of Management, Bentley.

T:+61 8 92667413 E: p.weber@curtin.edu.au

Acknowledgements

We would like to thank the management and staff of the ACCC for their support and encouragement in undertaking this study. In particular, the supportive words and deeds of Nigel Ridgeway, General Manager of Compliance Operations Group and Kim Parker, Manager of Compliance Strategies Branch. We also acknowledge the involvement of members of the ACCC Small Business Consultative Committee, who encouraged their members to contribute their experiences to the study.

Thank you also to Russell Smith of the Australian Institute of Criminology for his initial advice and confirmation of the existence of this gap in knowledge on small business scams. We also appreciate the work of our own staff member Cassandra Callus who managed the communications with our industry association collaborators and kept our stakeholders informed of progress.

Finally, thank you to the ACCC Deputy Chair Michael Schaper who first identified the lack of research in this area and encouraged us to undertake this project.

_ _ _ _ _ _ _ _ _ _ _

Executive Summary

This survey is the first national attempt at specifying the small business scam as a distinct category of scam worthy of focussed research endeavour. It is the first phase of a longer term proposal to understand how small business owners behave when scam risks are presented to them; it also attempts to identify which types of scams represent the most common and most serious risks of loss. The assumption implicit in this study is that there are differences in the type of scam that small businesses are exposed to and in their various responses to scam attempts, when compared to consumers. The study enlisted the assistance of many small business associations, and was conducted Australia-wide over the period May-December 2012.

A total of 291 businesses responded to the survey, and the sample of small businesses surveyed represented every ANZSIC class of business. It encompassed businesses with annual turnovers that ranged from $10,000 to $20,000,000 per annum. Approximately 2/3 of respondents were male and 1/3 female, which is broadly representative of the small business population in Australia.

192 respondents provided sufficient detail for the purpose of the full analysis intended. Several predictors of scam propensity were included in the study. These potential risk factors included turnover, experience of prior loss, routine activity theory, industry type, self control, select personality traits, generalised business risk and some demographic markers.

Owners reported the most prevalent scam attempts as lotteries and sweepstakes, advance fee frauds and free 'spam' type offers. There was evidence that social media is gaining ground as a communication medium to deliver the scam messages but email is still the dominant medium of delivery, apart from false billing and fax-back scams. Beyond the 15 common categories, another 17 types of scam were described by respondents.

In response to this barrage of scam attempts business owners are developing their own rules to manage this risk. We summarize these into a list of 32 strategies being deployed by small businesses to foil the scammers.

The financial loss through scams in our sample ranged from $100 to $10,000 per annum and the time spent dealing with the consequences was estimated as high as 100 hours. The dollar value of losses is somewhat lower than the norms reported by the ACCC's Scam Watch but that is to be expected, given our data collection method we were unlikley to have self reports of major fraud communicated via an online survey.

There appears to be some link between financial risk taking and increased scam propensity. General business risk taking does not seem to be related to the level of scam loss, but there is a somewhat greater quantum of loss exhibited by respondents who take higher financial risks. Respondents who took lower financial risks also demonstrated higher confidence levels in identifying a scam before a loss is incurred.

A major finding of this research is that Routine Activity Theory is a useful predictor of scam propensity (scam amount lost). There was a significant relationship between the amount of money lost and the degree of online activity that the business was involved in. It seems that having a heightened online presence leads to greater risk of loss and/or more money lost. This is perhaps not a surprising finding, but none the less important to provide evidence of another hotspot. That is, businesses that transact online and indeed have a significant online presence can expect to attract the attention of scammers who will want to 'fish where the

fish are'! In addition to this, remote purchasing behaviours which had an 'unguarded' aspect to them (such as shopping online, speaking with an unknown telemarketer or responding to an infomercial) were shown to have a relationship with the quantum of loss.

We also developed an innovative test of gullibility via a heat map based question which identified 19 respondents who selected an option that was by all measures too good to be true. These respondents would be candidates for further in-depth analysis of the thought processes that led to this choice. The 19 respondents also self-assessed as being somewhat less confident of identifying a scam, confirming that self assessment of capability may be appropriate in this case.

The growing problem of scams committed against small business is shown in this report to be at such epidemic levels that the current lack of specific research attention cannot be allowed to continue. For such an entrenched problem we may not be able to find a cure, but we must begin to diagnose the 'symptoms' and develop effective 'vaccines' to take a more proactive stance. At present, the vast majority (84%) of the variance on scam prevention expenditure can be explained by the amount of prior losses incurred. Loss prevention, it seems, is far less common than dealing with the fallout after the loss has been incurred. In laymans terms - yes the horse may have already bolted, but there's still more left to protect in the stable.

– – – – – – – – – – –

CONTENTS

1.Background

Scamming is a phenomenon which is becoming increasingly prominent in the public consciousness, and the incidence of which appears to continue to grow more audacious and pervasive. In Australia alone, for example, the number of scams reported to the national enforcement agency, the Australian Competition and Consumer Commission, more than doubled to reach some 83,000 incidents in 2011, with commensurate reported losses of $85 million (ACCC 2012).

Scams committed against small business are a significant draw on the limited resources available to the owner(s) of a small business. For example, one correspondent gave a particularly reflective and informative response:

> *"As an online business with our own payment portal, we are regularly targeted (3+ times a week)… I have taken extensive steps to ensure that our payment gateway is as heavily secured as can be achieved… This mitigation comes at the cost of about $10,000 to $15,000 per year in proactive mitigation. If we were not extremely security conscious,* ***I can confidently say we would have had our entire customer credit card databases stolen multiple times since we started three years ago"****.*

In further support of this sentiment, we can personally attest to the growing plague of email delivered scam approaches, even within this project. We observe that the most common type of enquiry we experienced to the dedicated email account for this project was from people wanting to share their wealth with us, help us become smarter, richer, happier, and all for very little money or effort! In short, scams that were all too good to be true.

In something of an ironic twist, even the legitimate winner of the competition associated with the survey was himself wary enough about having "won a prize" to make independent email contact to confirm this was not, in fact, also a scam.

Small business in particular and society in general is losing productivity and the capacity to trust as a result of the scammers. The problem is global and significant, but our focus is on a hitherto uninvestigated subspecies of scam victim, the **small business scam victim.**

1.1 Challenges in Understanding Small Business Scams

The problem with small business as a policy and research target is well known, but seldom well articulated. The small business owner and the small business entity sit conceptually somewhere between a large corporation and an employee, dependent upon the research question and the objective. So when it comes to a question such as how they might be impacted by scams, do we mean scams committed against the owners or against the organisation? Further complicating matters is the reality that there is no difference in a legal sense (trading entities with corporate or individual owners) and in other cases there is no difference in practice (sole directorship companies that behave like sole propietorships). In addition, in any small business that employs people, it is important to establish whether we are investigating the actions and behaviours of owners or of employess or both. The diagram below depicts these choices:

Figure 1: The dual nature of small business scams

In this study we are focused on small businesses where the owner makes most of the strategic decisions in the business, but at times, he or she may actually delegate some of this decision making to employees and will often delegate routine process decisions that also have a risk of scam loss associated with them. Therefore, the study was targeted at owners and some key employees that had delegated authority in regards to decisions on processes and risks that may be scam related. For example, the owner would be the person we need to understand if assessing a loss incurred through taking a high risk strategic direction, but not necessarily for the error in making a payment to a fictitious service provider. Readers interested in a deeper treatment of this issue may wish to read "Understanding Small Business Scams" in the November 2012 issue of the *Journal of Enterprising Culture* (Schaper and Weber, 2012).

1.2 Theoretical Perspectives on Scam Propensity

In recent years, two theories have emerged which have a particularly pertinent bearing upon this study, self-control theory (SCT) and routine activities theory (RAT) (Holtfreter, Reisig and Pratt 2008; Van Wilsem 2011). These theories are explained below.

1.2.1 Self-Control Theory.

Self-Control Theory is a recently applied lens through which to examine why some consumers are scammed and others are not (Holtfreter, Reisig and Pratt 2008; Holtfreter et al 2010; Van Wilsem 2011). It argues that individuals who lack self-control are not concerned about their long-term behavioural consequences. When the opportunity arises, these individuals are more likely to engage in activities that provide them instant gratification for little effort (Holtfreter et al 2010; Van Wilsem 2011). While a lack of self-control will not in itself mean an individual will be targeted by a scammer, people with poor impulse control will engage more often in activities that will expose them to a scammer (Van Wilsem 2011). So if an individual is prone, due to a lack of self-control, to pursue online deals that promise big pay-offs, eventually they are logically and mathematically more likely to fall victim to a scam.

Self-control theorists contend that self-control remains relatively unchanged over one's life course, having being set before adolescence (Tittle, Ward and Grasmick 2003). Given that a lack of self-control remains relatively stable throughout one's life, an individual with poor impulse control is also at heightened risk of being a repeat victim of scams (Van Wilsem 2011).

Another development of SCT has been the work of Langenderfer and Shimp (2001), who have proposed a theory of consumer vulnerability to scams that incorporates the effects of self-control, gullibility, susceptibility to interpersonal influence, scam knowledge and 'visceral influences'. These visceral factors are described by Loewenstein (1996) as having direct hedonic impact (via emotions such as lust, greed and fear). In addition, some victims are likely scammed because they are so eager to receive the payoff on offer that they pay little attention to the scam's details and ignore cues that are obvious to others not so driven by the desire (Langenderfer and Shimp 2001). While visceral factors may drive an individual to fall prey to a scammer, it is argued that it is the victim's lack of self-control that is primarily responsible. For example, an individual with low self-control seeks immediate gratification and faces a greater likelihood of involvement in scam activities (Holtfretter, Reisig and Pratt 2008).

Alternatively, some repeat victims of scams have been shown to develop a self-conscious emotion that leads to self-blame and an exaggerated fear of being fooled or duped. This emotional state is called "sugrophobia" (Vohs, Chin and Baumeister 2007). This feeling of being duped leads to a heightened commitment to never fall prey to the same scam again. It is observed that high sugrophobes will likely be vigilant and skeptical of future deals whereas low sugrophobes may not even realize in some instances that they have been duped. Recent research also suggests that a person with both low self-control and low sugrophobic tendencies will probably not report the event, to avoid being labeled as a 'sucker' if they fall for a somewhat 'obvious' con (Vohs, Chin and Baumeister 2007). This presents an argument that perhaps experiencing a scam might make an individual more wary of future potential scams. So while theorists argue that a lack of self-control remains stable during one's life, negative experiences from scams might also lead to restraint on the part of one sub-group of small business owner. Indeed, some studies have found that individuals who suffer the negative consequences of low self-control do end up improving their self-control over time (Tittle, Ward and Grasmick 2003).

Self-control theory can help explain why a small business owner might fall victim to a big "pay-off," but does not explain why one falls victim to scams like the directory entry or unauthorised advertising scam, which offer no extra profit or incentive beyond complying with a request for payment from a perceived legitimate source. Focusing on why small businesses are scammed only provides one angle with which to view susceptibility and perhaps a more holistic approach is needed which examines why scams propensity varies between businesses in the first place. Routine Activity Theory does offer a partial explanation for this variability of the quantum of loss to scams.

1.2.2. Routine Activity Theory.

Routine Activity Theory (RAT) offers a partial explanation for the level of scam activity in a particular industry sector or geographic location that may add predictive power to any composite measure of scam propensity (Cohen and Felson 1979). The theory proposes that most criminal acts require the convergence of three key elements: motivated offenders (i.e. scammers), suitable targets, and a lack of capable guardians against crime (Cohen and Felson 1979; Hutchings and Hayes 2009; Pratt, Holtfreter and Reisig 2010). This theory proposes that the probability of victimization increases with a concomitant increase in time spent in 'harm's way'. This risk is heightened when there is no protection by capable internal or external guardians.

RAT predicts that a crime is more likely to occur in circumstances where (1) the victim is in the wrong place, (2) at the wrong time, and (3) little is being done by anyone to protect them.

Most of the early work in RAT has concentrated on identifying demographic characteristics of individuals that display a tendency to place themselves in high risk situations. The evidence from this perspective suggests that minorities, males and single persons are more susceptible to crime in general as a consequence of RAT (Holfretter, Reisig and Pratt 2008). In addition, frequent internet based activity has been identified as a risk factor for cybercrime victimisation using routine activity theory RAT (Yar 2005; Holtfreter, Reisig and Pratt 2008; Hutchings and Hayes 2009; Pratt, Holtfreter and Reisig 2010; Van Wilsem 2011).

Routine Activity Theory helps explain why some crimes occur and prescribes the conditions that will lead to the crime opportunity. For example, recent research adopting RAT as a framework has shown that the risk of a consumer being scammed increases by 50% if the victim uses internet banking and/or email/instant messaging and by another 30% if online shopping and downloading of software is occurring (Reyns 2011). Following the logic of RAT, high e-commerce activity businesses are predicted to be at greater risk since these businesses are likely to be more visible to cybercriminals. Like many criminals, scammers are opportunity seekers (Farrar 2011) and scams are somewhat opportunistic crimes (Brody, Mulig and Kimball 2007), so scammers, it seems, will tend to 'fish where the fish are'.

2.Methodology

This survey utilised a web based survey software developed using the Qualtrics system of survey design (www.Qualtrics.com). A hyperlink to this online survey was embedded in recruitment messages sent via participating organisations that agreed to help recruit businesses to the study. Suggested communication scripts were provided to participating organisations for positioning on their websites, within their newsletters, social media and other networks/ events as well as (in some cases) via outbound recruitment emails to their membership. Details of the scripts used can be found in the appendices of this report, beginning on page 40

2.1 Participating Organisations

The following list of organisations took part in the participant recruitment exercise:

- Air Conditioning and Mechanical Contractors Association
- Association of Wall and Ceiling Industries Australia and New Zealand
- Australian Chamber of Commerce and Industry
- Australian Dental Association
- Australian Federation of Travel Agents
- Australian Food and Grocery Council
- Australian Institute of Horticulture
- Australian Newsagents Federation
- Australian Retailers Association
- Business Enterprise Centres Australia
- Combined Small Business Alliance
- Consult Australia
- Council of Small Business Organisations of Australia
- Curtin University Alumni
- Dry-cleaning Institute of Australia
- Economic Development Australia
- Hairdressing and Beauty Industry Association
- Hosted Accommodation Australia
- Master Builders Association
- Motor Traders Association
- Optometrists Association
- Pharmacy Guild of Australia
- Real Estate Institute of Australia
- Wine Grape Growers Australia

There were other organisations contacted by the research team who indicated they would informally pass on these recruitment details but did not confirm how and if they had done so. Because we do not know how many outbound emails are sent in this arms-length process we cannot provide an estimate of response rates.

2.2 Sample Characteristics

ANZSIC Industry Division	Number
Agriculture, Forestry and Fishing	6
Manufacturing	7
Construction	7
Wholesale Trade	3
Retail Trade	**39**
Accommodation and Food Services	6
Transport, Postal and Warehousing	4
Information, Media and Telecommunications	3
Financial and Insurance Services	4
Professional, Scientific and Technical Services	**18**
Administrative and Support Services	1
Education and Training	4
Health Care and Social Assistance	**19**
Arts and Recreation Services	8
Other Services	**29**
No response provided	34
Total	192

Table 1: Industry representation patterns

The method of sampling is known as convenience sampling and it inevitably leads to some bias in the industries sampled, dependent upon how effective individual association recruitment efforts were. To check for such bias we asked respondents to use an ANZSIC classification tool to determine what industry they belong to. The tool is simple enough to use but does require some user effort. Therefore, to avoid loss of data through respondent dropout, completion of this section was made optional. Of the 192 useable responses 158 provided an ANZSIC classification. The breakdown of ANZSIC divisions (Table 1) does favour retail and professional services but all industry divisions are represented.

In total there were 291 respondents who started the survey during the survey period. As is typical for such a study, there were a variety of reasons and triggers for non-completion that reduced the pool of useable responses to 192. Table 2 details this attrition and the reasons for exclusion:

Reason/point of exit	Number	Balance
Started	291	291
Not a small business by our definition	46	245
Not decision makers in the business	4	241
Answered no questions after commencing and qualifying	26	215
Dropped out at the turnover question (before answering it)	10	205
Dropped out after demographics but before any behavioral questions began	12	193
Junk input, response deleted	1	192

Table 2: Survey attrition patterns

2.3 Owner Demographics

Focusing on the 192 complete and partially complete responses, there were 124 (64.58%) male and 66 (34.37%) female respondents with 2 respondents preferring not to answer. The sample appears to closely mirror the national small business owner gender profile of 68.5% male and 31.5% female (ABS, 2007). The educational qualifications of decision makers are also quite well spread with 32 (16.67%) having a high school (or less) education, 45 (22.34%) technical college, 66 (34.89%) university undergraduate degrees, 37 (29.27%) with a Masters or PhD and 12 (6.25%) describing their education as 'other'. Given the sampling method of using existing small business professional networks, the biases towards higher levels of education in the anonymous snowball sampling methods used are anticipated and deemed acceptable.

2.4 Business Turnover

In terms of predicting scam propensity, our preliminary research identified turnover as a potentially important influence on scam propensity from the demand side. It was proposed that criminals will tend to target their scams to businesses that have more money to part with, to 'fish where the fish are'. In other words, businesses with characteristics that indicate to the scammers that they will have high turnovers (and hence intermittently higher bank balances) will be targeted more frequently and for larger amounts.

Turnover (n=192)	Frequency	Percent (%)
< $10,000	14	7.3
$10,000 - $24,999	9	4.7
$25,000 - $49,999	12	6.3
$50,000 - $99,999	26	13.5
$100,000 - $199,999	20	10.4
$200,000 - $299,999	18	9.4
$300,000 - $399,999	3	1.6
$400,000 - $499,000	19	9.9
$500,000 - $599,999	8	4.2
$600,000 - $999,999	10	5.3
$1 million - $2.5 million	28	14.6
$2.5 million - $5 million	7	3.6
Greater than $5 million	13	6.8
Total (2.5% no response)	187	97.6

Table 3: Turnover by range category

As is often the case with voluntary surveys of small business, many respondents were not initially prepared to divulge turnover. However, in anticipation of this problem, turnover data was requested as both an actual $ figure per annum and as a categorical response. Detailed scrutiny of the actual turnover data from all respondents determined that it would be possible and reasonable to replace missing values in the actual turnover data with the midpoint of the associated category range. Table 3 provides the turnover of respondents and the frequency of respondents with the corresponding turnover range. Errors of interpretation made by respondents were able to be corrected by comparing the two related measures of turnover. This transformation was performed on 20 cases for missing data and 19 cases for incorrect data input, thus permitting further analysis on the entire data set using the dollars per annum turnover data.

Whilst we had hypothesized that turnover may be a predictor of scam loss, this proved on this occasion to be a difficult variable to identify relationships with, due mainly to the skewed nature of the sample. A significant majority of respondents had turnovers of less than one million dollars. Unfortunately, a smaller group of much higher turnover businesses (between 1 and 20 million dollars) proved difficult to adjust for and yet were too influential to delete from the study. Therefore, the efficacy of turnover as a predictor of scam propensity remains an open question to be followed up on in the next phase of the research.

2.5 Business and Owner Characteristics

Characteristic (n=192)	Mean	Range
Years business owned	12.91	0-62
Hours operated per week	55.24	3-168
Weeks trading per year	50.43	30-52
Number of employees (actual, not Full Time Equivalent)	3.98	0-49
Age of respondent	44.96	14-70

Table 4: Business and owner characteristics

The data shown in table 4 suggest we are dealing with respondents with quite a typical spread and representative characteristics. Data from the Australian Bureau of Statistics (2012) confirm that as of June 2011, 93.5% of all businesses occurred in the 0-4 employee range. This compares favourably with a mean number of employees in the survey population of 3.98 employees. The responses received are from a relatively experienced cohort of owners with an average of nearly 13 years in the business (at just 45 years of age) and operate the businesses as a fulltime business in the main. Given these broadly representative characteristics, we can be confident that the data collected is representative of small business owners and their businesses and that any observations or suggestions made are coming from experienced owners. It is not possible to disaggregate the results on an industry by industry basis as we had hoped since there were not sufficient responses from any one ANZSIC class to make any stand-alone analysis valid. Instead, the report and analysis will focus on the characteristics and behaviours of the entire sample.

3. Findings & Analysis

Awareness of what is 'out there' in terms of prevalent scams and through which communication channel the organisation will be approached is arguably the vital first step in effectively protecting the business from loss, knowing where to look for the risks. Therefore, one of the main aims of this study was to provide indications of prevalence of the various types of small business scam and the common modes of delivery of the scam message. This is achieved in the study by examining the relative frequency of recent exposures (within the last year) to the various scam types (prevalence) and then identifying the three most common mediums used to make the approach. Table 5 indicates the proportion of respondents that were aware of a scam attempt against their business in the past year and then ranks the three most common mediums utilised to make the approach. It should be remembered that being aware of a scam approach is a subset of all actual scam attempts since some attempts will go unnoticed, so these proportions should be treated as MINIMUM levels of prevalence.

Scam Description	Prevalence*	Medium 1	Medium 2	Medium 3
Advanced Fees (inc. Nigerian Scams) n=132	68.75%	Email (120)	Phone (4)	Mail (4)
Fax-back premium phone numbers, n=59	30.73%	Fax (34)	Email (10)	SMS (6)
False billing (advertising & directories), n=112	58.33%	Mail (38)	Email (32)	Fax (19)
False billing (office supplies), n= 54	28.12%	Email (17)	Mail (15)	Phone (12)
False billing (domain names), n= 80	41.67%	Email (38)	Mail (23)	Fax (9)
Credit-card not present, n =56	29.17%	Email (38)	Person (5)	Other(4)
Bank account phishing, n=97	50.51%	Email (90)	Phone (4)	-
Overpayment refund scams, n=65	33.85%	Email (56)	Phone (4)	Other (2)
Error allowing Hacker access, n=47	24.45%	Email (28)	SocMedia(11)	Phone (6)
Spam 'free' offers, n=122	63.54%	Email (110)	Fax (4)	SocMedia(2)
Investment/real estate seminars, n=104	54.17%	Email (65)	Phone (17)	Fax (7)
Job/employment/business opportunities, n=103	53.65%	Email (84)	Phone (5)	Fax (5)
Lottery and Sweepstakes-unexpected prizes, n=136	70.83%	Email (114)	Mail (8)	SMS (6)
Chain letters and pyramid schemes, n=95	49.48%	Email (82)	Mail(5)	SocMedia(3)
"other" scams (user defined), n= 32	16.67%	Phone(13)	Email (10)	Mail (3)
Sample norms (n =192)	**44.93%**	**Email**	**Phone**	**Mail**
**** The proportion of survey respondents who have noticed this type of scam approach in their business within the past year.***				

Table 5: Scam activity and medium of communication

The 'other' category had 32 scams reported that respondents did not feel met the category criteria in the survey. In summary they were:

- Solving computer problems
- Representing an official body seeking donations
- Contract tender inducements/tips
- Requests for details of products (then switches to scam after relationship formed)
- Overcharge on phone accounts
- Betting systems

- Threats to cause loss/harm
- Fake purchase(s) with no other apparent motive than to cause mischief
- Search Engine Ranking (secrets revealed)
- Business Identity theft (pretending to be a known organisation-phishing but not for bank account, just aiming to steal identity)
- 'strange' probing phone calls-non specified
- Safety inspections, unauthorized.
- Market intelligence offers (dubious quality)
- Email intercepts between client and supplier-changing delivery instructions.
- Fake grants info
- Claiming wrong change given (in person)
- Fictitious events (with participation fees).

One scam description in particular highlighted the complex nature of scams and the lengths to which the scammers will go to deceive. The name and details of the business are deleted to maintain privacy, but here is the recent experience they had:

"[The] a*ttacker somehow gained access to my suppliers' computer or email account and was able to intercept emails coming from me to the supplier and from the supplier to me. For both my supplier and me the email address on the intercepted incoming emails was correct, but when I hit reply, OR my supplier hit reply to send to me, the email address changed very slightly to go to this hacker instead, so he would then change it and forward on. Using this technique, the attacker was able to intercept an email from my supplier sending me a deposit invoice, change the bank account details & forward onto me, I then made the money transfer to this incorrect account and forwarded my supplier the payment receipt for them to check the details, the attacker also intercepted this email, changed the details on the receipt to be correct like the suppliers and forwarded on so he approved it and we suspected no problem until it was too late when the money did not come through, the invoice amount was for over AUD4,500 which is a huge loss to my brand new business, not yet launched and our banks are not very helpful in this situation as technically they have not made any error - this scam is extremely clever and something more businesses should be aware of if dealing with offshore suppliers."*

This example highlights the value of keeping up to date with current scam trends and attempts. This form of identity theft is not new, although the technical aspects may be. Regardless of the novelty of the scam, this new small business has suffered financial and reputational damage during start-up and seems to still be having problems getting any redress or assistance. Stories such as this certainly add weight to the development and dissemination of start-up educational material in this area.

3.1 Losses Incurred and the Rules of Thumb Used to Avoid Them

This survey is a nationwide sample of business owners who elected to share their experiences with us and as such it was anticipated that the proportion of organisations actually experiencing a scam loss may have been somewhat over-reported. This is despite our recruitment communications explaining that we were seeking responses from non-scammed businesses as well. Overall, 139 of the 192 respondents to this survey (72%) reported having been approached by a scammer within the preceding year. Of the 192 businesses in the survey only 11.97% reported an actual financial loss from scam events. The average loss amongst those scammed in the preceding year was $1258. In terms of the type of loss reported, it would appear that the

survey method was more effective at capturing high frequency but relatively low loss scam reports, with the largest scam loss disclosed being $10,000.

We interpret this reporting pattern as suggestive of small businesses taking the time to tell us about the scam experiences that they have endured that do not necessarily lead to financial loss. However, they do spend significant time and money in protecting themselves from the scammers and are keen to share their experiences and strategies for reducing the risk. The following list is a summary of the ways in which business owners are developing their own heuristics (rules of thumb) to beat the scammers:

- Spam interception and internet security software installed on all internet connected devices
- Be wary of too good to be true deals and rushed high pressure deadlines
- Understand how money will be transferred and what recourse to the recipient the business will have. Be especially careful of any transaction where the transferring bank/organisation does not disclose recipient details.
- Never respond to the scammer, that just tells them you are 'real'
- Don't agree to advance payment requests
- Frequent updates and audits of IT systems by qualified professionals
- Check supplied details (such as phone number).
- Ask for secondary ID
- Assign the task of vetting suspect emails /approaches to someone who has the right level of industry experience and knowledge. It's not just about being tech savvy, wisdom and prior experience counts.
- Require purchase orders for every expense (set minimum $ limit)
- Never provide bank account details to unknown entities
- Use a separate debit card with a small available balance for online purchases, thus limiting the maximum loss.
- Be suspicious of any contact from any supposedly well-known organisation that wants to give you something.
- Google the offer including the word scam in your search
- Develop a shared list of known problems/risks. One owner described this as their "internal Bull Meter", another felt they were more likely to be approached from certain geographic locations. Yet both said, whatever the rule of thumb, be prepared to change it as the risks change.
- Requests that don't fit normal patterns of business (large orders, strange timing, vague language, no industry jargon used)
- Employee retention, keep staff with experience rather than turnover to less experienced. Wisdom in employees
- Check Scamwatch
- Use googlemaps (streetview) to see what is at the address claimed.
- Hang up on calls where auto dialer delays are evident
- Pay by credit card where some bank and credit card protection exists. Even have a card with a separate bank or create a separate legal entity to further protect main assets.
- Develop a list of websites that list scams
- Speak to a colleague in the industry
- Consider only taking international orders by advance payment using cleared funds (such as telegraphic transfer)

- Have a single approver of new expenditures and a single person who responds to any email/sms/phone contact that is suspicious **and** ensure that person remains well informed of current threats.
- Beware of faulty grammar or poor context
- Use Skype to see overseas contacts in person
- One person said "We do not deal with Western Union money transfers"
- Ask for ABN and/or ACN and verify it
- Use cameras and voice recording and make it known you use them
- Ask for references and check them
- Ask questions that show evidence of context, weather, time of day, local current affairs etc.

Interestingly, there was not a single response that suggested proactive information dissemination (helping other businesses avoid the scam). This is likely an area where businesses rely on their industry associations and organisations such as the ACCC (scamwatch) for advice. Business associations could take a leadership role in this regard and we see some evidence of this potential within the organisations that assisted us with this survey.

3.2 The Cost of Small Business Scams.

As well as the loss experienced, businesses expend time reporting and resolving scam losses. The survey identified the maximum financial and organisational resource wasted on this nonproductive error across all respondent experiences, these maximum losses are reported below in table 6.

Time and/or money lost last year (2012) on specific scam types	Maximum $	Maximum Hours
Advanced Fee/up-front payments (inc. Nigerian Scams)	$5000	8
Fax-back premium phone numbers	$500	3
False billing (advertising & directories)	$8800	20
False billing (office supplies)	$200	2
False billing (domain names)	$500	5
Credit-card not present	$9000	40
Bank account phishing	$5000	100
Overpayment refund scams	$500	30
Error allowing Hacker access	$10000	38
Spam 'free' offers	$10000	80
Investment/real estate seminars	$100	1
Job/employment/business opportunities	$500	15
Lottery and Sweepstakes-unexpected prizes	$1000	80
Chain letters and pyramid schemes	$0	10
"other" scams (user defined)	$5700	250

Table 6:Time and money expended on scams

In the following section we delve deeper into the owners' traits and behaviours to begin to unpick the relationship between the business owner and the prevalence and type of scams that they might fall for. We cannot really understand, from this type of survey, the deeper emotional and attitudinal effects on the owner that result from falling victim to a scam. However, we do detect in the language used by some of our respondents a loss of confidence and loss of trust. There is one compelling piece of evidence of this erosion of trust in business presented under the heading 'trust in others' below.

3.3 Owner Personality Traits

There were some personality traits which were considered candidates to impact upon the likelihood of being scammed. Risk propensity was deemed to be the central trait of interest and is dealt with separately. Initial investigation of the problem also suggested that a person's capacity and willingness to trust others and be open to new experiences may feed into their propensity to be scammed.

3.3.1 Trust in Others

Two statements sought to measure this from a small business perspective. These statements were "Most business people believe in fair, honest trading" and "Most people are basically honest in their dealing with others". These two items were subjected to factor analysis and the one factor solution explained a very high 87.45% of all variance at a significance level of 0.001. This confirms that both items can be summed to the one measure which we called Trust in Others. In these two items we see very strong evidence of the damage to business relationships and owner attitudes that is being done by the small business scam epidemic. In perhaps the strongest statistical relationship within the whole study we note the strong relationship between how much money owners have lost in the last year and their level of trust in others. **It appears that over 50% of the variation in an owners willingness to trust others can be explained by the level of money lost *(r=0.522, p<0.05)*.** In other words, there was a strong negative relationship between the level of money lost by the respondent and the level of trust in others. The more money the respondent has lost in the past, the less they trusted others. We feel confident in making this causal statement although our analysis does not mathematically preclude the opposite interpretation. It is not logical to draw the reverse conclusion — that those who trust others more will lose less.

3.3.2 Openness to Experience and Opportunity Recognition.

Research into the behavior of small business owners will often broach the subject of opportunity recognition. Opportunity recognition in this sense is the identification of an idea that combines various factors or resources in a way that is expected to generate a profit. It was considered likely that some scam scenarios will play into the opportunity recognition process as the stereotypical 'opportunity that's too good to be true' may also be for some, 'too good to miss'. Some of this propensity to recognize opportunities may be situational and difficult to measure, but a large proportion of this propensity has been shown in the past to be a stable 'hard-wired' genetic trait of the individual. In fact, recent studies in entrepreneurship show that 45% of the variance in opportunity recognition capability is genetic and that up to 61% of the differences between people in the related concept of openness to experience is also explained by genetic makeup (Shane et al, 2010). Investigating this was achieved parsimoniously through two statements "When opportunity knocks, it should be grabbed" and "There is occasionally 'easy money' in business."

There were some patterns of correlation that emerged here which are worthy of deeper investigation in future studies. **Gender was correlated with opportunity recognition, with men being more predisposed to**

'grab' (take a risk) at the opportunity than women (*r = .163, p<0.05*). We do not contend here that this is either a bad or a good thing, just simply a gender difference that is also identified in the literature (male risk taking). However, if we consider that there was also a relationship between opportunity recognition and business turnover **(*r = .144, p<0.05*)** it is plausible that **this makes a male owner more attractive to the scammers, having (on average) more cash in the bank and more likelihood of grabbing that 'once in a lifetime' opportunity that the scammer is offering**.

'Too good to be true'. Finally, it is perhaps reassuring (for prevention agencies) to note that there was a **significant negative relationship between the belief that there was occasional 'easy money' in business and recognising a scam (without loss) in the past year *(r= -.144, p<0.05)***. It would seem that a healthy dose of skepticism about the existence of 'easy money' does lead to higher levels of scam detection and loss prevention.

3.4 General Business Risk Propensity (GBRP)

This concept measures the risks that the owner takes when running a business. It is a function of rational choices made having regard for the uncertainty of the outcomes as well as the likelihood and perceived value of each possible outcome (Hung & Tiangpong, 2009). This variable is made up of five items that describe the level of risk that a person takes in a business context. Analysis of the reliability of this scale shows it has a Cronbachs' alpha of 0.713, a good reliability score. However, there was no significant relationship detected between GBRP and any of the scam loss indicators used in this study. It transpires that the type of risk taking behavior that has a stronger relationship with scam loss is the more narrowly defined financial risk. This 'non finding' is still important since it suggests that (in our sample at least) the losses incurred are not a result of generally high risk taking behavior. **From an education and policy perspective it would appear that a focus on financial risk mitigation would be more efficient and effective use of resources than on more general risk mitigation in business**. See the discussion on financial risk self-control for more on this finding.

3.5 Routine Activity

Routine Activity Theory (RAT) predicts that a crime is more likely to occur in circumstances where the victim is in the wrong place, at the wrong time, and little is being done by anyone to protect them. In the small business context we hypothesized that the 'wrong place' may actually be transacting and communicating online as this has previously been shown to be risky behavior in a consumer crime context. We also make a distinction between business activities and personal activities online, since personal activities are expected to be more likely to increase the risk of some forms of scam, such as the Nigerian scam that rely on a level of relationship building.

We find that a significant relationship exists between the quantum of funds lost in the prior year and the level of online activity that the business is involved in. This relationship is of moderate strength and is highly significant (*r = .231, p<0.01)*. The relationship only holds for Business RAT (BRAT), no significant relationship exists with Personal RAT (PRAT). This finding suggests that adopting more **business** related online practices is correlated with an increased scam risk and thus to greater potential losses. It also suggests that a higher volume of routine activities are conducted by business owners in their small business than in private, highlighting why it's important to treat small business scams as a different phenomenon to general consumer scams.

However, opportunity is not enough for a crime, there must also be intent or at least the lack of sufficient caution. What makes a business owner who finds themselves in a risky scam environment actually succumb to the scam? It is proposed that it is a lack of self-control in such situations that is one catalyst for loss. Therefore, we hypothesized that low self-control would also be related to the likelihood of financial loss. This theory is investigated next.

3.6 Self-Control Theory (an accomplice to the RAT)

When considering the impact of RAT upon small business scam losses, one might ask why a business owner would be more likely to be tempted to take a risk simply because they were in the wrong place (transacting online). Self-control theory addresses this concern by helping to identify the sub group of owners who are pre-disposed to temptation by a 'too good' offer. Self-control theory indicates that when an 'opportunity' arises (being in the wrong place), individuals with lower self-control are more likely to engage in activities that provide them instant gratification for little effort, the classic lure of the scam that is 'too good to be true'. This circumstance, mixed with high levels of business risk taking behavior and a suitably motivated scammer make a heightened risk of loss apparent.

3.6.1 Financial risk self-control

In order to quantify financial risk taking self-control we follow the guidance of Holfreter et al (2008) by using a measure of financial risk self-control consisting of two questions that reduce to a common latent factor via principal component analysis. This technique results in a single factor emerging that explains 81% of the variation in scores on financial risk self-control. This factor structure is almost identical to the results obtained by Holtfreter et al (2008), suggesting the measure is a stable one across different populations. In addition, when compared with the general business risk propensity (GRBP) measure a moderate bivariate correlation of .515 was noted, suggesting that financial risk self-control is related to GRBP but is not the same thing.

To further analyse financial risk self-control we classified all respondents into two groups referred to lower and higher financial risk taking and separated the two groups at the mean of the standardized scores (i.e. one group lower than the mean and the other above the mean). This resulted in 101 respondents being classified as lower financial risk takers and 91 as higher financial risk takers. In the low financial risk group, businesses lost an average of $1048 last year (where a loss was reported) whereas in the higher financial risk taking group the loss was higher at an average of $1737.

Interestingly, the lower risk taking group also reported slightly higher levels of confidence in identifying a scam. It seems that this simple two item self-report measure of financial risk self-control may have some predictive capability in identifying owners less confident of identifying a scam and simultaneously more likely to lose greater sums of money, **potentially a costly intersection of capability, trait and outcome. We consider this a finding worthy of future investigation with larger samples of small business scam victims but draw no conclusions here.**

3.6.2 Remote Purchasing (unguarded risk)

In this research we deployed a 4-item scale that related specifically to indicators of low self-control when dealing with remote purchase transactions (referred to as unguarded exposure by Holtfretter et al 2008)

where some risk of being deceived would be evident because of the lack of direct and/or prior contact with the seller. The questions that make up the scale are:

In the past year have you:

1. Responded to a telemarketer that you have not previously done business with?
2. Purchased from an internet web-site?
3. Ordered a product after seeing an infomercial on TV?
4. Ordered a product from unsolicited mail that you had not previously purchased from?

These 4 items are additive, with the scores for each question summed to one overall score. The proposition is that low scores on this scale indicate vulnerability to being scammed since scams are by nature cold calls that are trying to sell something without any prior evidence of performance or established trust. Within this sample there is a moderate relationship between unguarded exposure and the amount of money businesses have lost to scams in prior years. **The linear regression technique used identifies that unguarded exposure via remote purchasing accounts for nearly 30% of all of the variation in the amount of money lost to scammers.** If this pattern of results can be shown to be causal then this scale would make an excellent component in a tool to test for vulnerability of business owners to scams.

The developers of this scale (Holtfreiter, Resig & Pratt, 2008) also point to another and/or additional reason for this relationship holding. They observe that "…victimization research generally indicates that perpetrators choose potential victims based on visible indicators of vulnerability"(Holtfreiter et al, 2008, p. 192). In this context, the scammers may well be focusing on victims who have shown prior predisposition to transact remotely. Essentially, it would not be much of a stretch of the imagination to envision criminals developing lists of scam vulnerable business owners using legitimate purchases as 'bait' transactions. In the context of routine activity theory, this concept reflects the level of 'unguarded' exposure to potential scammers.

Whether the relationship is cause or effect is not the main issue here. What matters is that policymakers within government may have in this simple set of questions a way of identifying at-risk groups of business owners before the loss occurs, i.e. a preventative tool. In addition, these questions do not appear to be directly challenging or questioning the owners' gullibility or intelligence, making them simple and non-threatening to administer in practice.

We acknowledge that the relationship between scam loss and remote purchasing behavior unearthed in this study is exploratory and not yet definitive in predicting scam propensity. However, it certainly deserves deeper and more focused attention as it holds promise as a simple yet effective and significant predictor of scam propensity.

3.7 Gullibility

Gullibility describes a tendency to accept things at face value without critical analysis, which often allows a person to be duped or manipulated by others (Greenspan, 2009). This concept is difficult to test for in the context of an online survey. However, we developed an approximation of gullibility by presenting a significant prize ($10,000,000) and then tracked which participants opted to enter the competition using a heat map to track the mouse click points of respondents. Entrants were forced to make a decision within 30 seconds on which reward they would choose to enter a competition for, a big prize, a small prize or they could opt to exit with no entry for a prize. After they had made a choice the experimental nature of the exercise was revealed and they were asked to explain their choice. The choices were categorized into three decisions:

1. Chose the big prize ($10,000,000)
2. Chose the real prize (a small tablet computing device valued at $400)
3. Opted not to select either prize, thus missing the genuine opportunity (they were later given a second chance)

These three options are (we contend) decision points along a continuum of gullibility. It is logical to expect some prize for participation in a survey, but very unlikely that the prize could be in the millions of dollars, yet the results show that 19 respondents (12%) opted to select the big prize whereas 72 respondents opted for the real prize and 66 cautious individuals opted for no prize at all. Of the 19 who we identified as having lost money in prior years, 11 opted not to select a prize, only 3 selected the real prize and 4 selected the big prize. This is consistent with the earlier discussion around sugrophobia, these respondents may well have a heightened fear of loss stemming from prior experience that stops them from taking reasonable risks to win a prize.

It is noteworthy that the 19 respondents who opted for the big (too good to be true) prize also rated themselves lower in their capacity to identify a scam than the rest of the sample. **It may well be that the best way to identify such 'at risk' business owners is to simply ask them to self-rate their capabilities.**

3.8 Other Observations

3.8.1 A case of being wise after the event

In order to understand what businesses were doing to prevent scam loss, we tallied all current scam prevention expenditure and effort across all categories of scams and compared that to actual scam losses in the past. It transpired that there was a very strong positive association between losing money in the past and subsequent expenditure of time and money on prevention. The data shows that 80% of expenditure on scam detection and 78% of time invested in prevention is predicated by the quantum of prior loss experienced. These relationships were statistically significant at the 0.01 confidence level. This means we can be 99% confident that more than 80% of future scam prevention effort and expenditure is associated with prior loss experiences. A case of once bitten, twice shy.

In support of this observation we also note a relationship exists between confidence in identifying a scam and prior loss. When asked how confident business owners were in identifying a scam, there was a significant negative relationship between prior loss and confidence in identifying a scam *($r = -.201$, $p<0.05$).*

It remains a logical (but unproven) extension of this observation that businesses are not taking sufficient precautions until or unless they experience an actual loss. The other more optimistic but less likely interpretation is that the majority of businesses do not experience an actual loss because they already take sufficient precautions. At the very least this observation should prove useful for policy makers in designing and targeting their prevention messages to those most at risk.

3.8.2 Victimisation hotspots.

From the pool of respondents who lost money in the year preceding the survey (2012), seven were businesses that also reported having had prior year losses as well. These serial victims lost an average of $1991.43 in prior years. Comparing this with the other businesses that did not lose money last year (perhaps they learned a lesson?) shows a lower average loss of $1176.69 for the no loss group. Unfortunately the smaller size of these sub-groups of financially impacted victims does not permit any determination of significance of the difference, but the size of the difference is substantial, with repeat victims losing 41% more on average than those who did not experience additional losses.

There is also a pattern evident in the victimization rates when compared with organisational turnover, again caution should be taken in interpreting the differences because they could just be chance with the sample sizes involved**. However, it seems plausible that there are two subgroups emerging, those who learn from their mistakes, spend more on prevention and do not fall for the scam again and a somewhat smaller group who are repeat victims who do loose more funds in subsequent scam attempts.**

4. Conclusion

This study has gathered a great deal of evidence on just how intensely and diversely small businesses are being bombarded by various scams. The study also makes some advances in our understanding of the probable indicators and predictors of becoming a scam victim. This is still very much an opening salvo in what will be an ongoing battle to reduce the risk of scam loss to small business.

The specific expected outcomes of this study were:

1. *To identify the prevalence of various forms of scams, just how common were they?* It transpires that in the past year over 70% of all respondents had experienced a scam attempt and most of these had experienced multiple attacks. A list of the 15 most common forms of scam was developed and yet there were still a further 17 scam types described that fell outside of the categories adopted.

2. *Identify how the various scams messages are typically being delivered:* Email remains the most common form of scam delivery medium, suggesting spam filters and email management protocols will continue to be important prevention tools. Social media is beginning to have more of an impact, particularly as a medium for hackers to gain information and access. The main scam arriving in the post is the false billing scam. This scam type was identified by a majority of scam targets as arriving by mail, but email delivered false bills were nearly as prevalent.

3. *Catalogue the ways that small business are practically dealing with the growing risk of being scammed*. We identified 32 categories of heuristics that owners have adopted to beat the scammers and share these within the report.

4. *Develop and test a range of potential predictors of scam propensity to build a scam propensity tool or risk profile*. This is an ongoing project with this study providing a number of leads for appropriate indicators of scam propensity that will require further testing and analysis. The list of potential indicators are detailed in table 7 below, describing each measure or construct used and providing a brief comment on the potential of each to help predict future scam propensity. It is our intention to now seek funding and institutional support to test these and other emergent predictors on a larger purposive sample of small business scam victims, to move closer to the goal of developing a small business scam propensity index.

Construct/measure	Potential to assist in predicting Small Business Scam Propensity
Remote purchasing	Good. Predicts 30% of value of $ lost
Gullibility heat map	Good at identifying those who may fall victim to long odds gamble type scams. Needs further testing on more known victims of similar scams
Self-rating of scam propensity	Too early to tell. Needs to be tested against a larger group of victims. But early indications are promising.
Past loss as a predictor	By inference, businesses that have not been scammed would appear to spend much less time or money on prevention, therefore increasing their future loss propensity
Industry specific risks	Not able to confirm from this sample. Industries that have higher reliance on internet based sales and transactions may be indirectly at risk via RAT. Retail probably at a heightened risk of hacking scams because of client credit card details held. Turnover also varies by industry and this may hold some predictive capacity.
Size of loss	Repeat victims appear to lose more $ than one off victims
Trust in others	Seems to have utility to predict repeat victims, again a larger sample is needed.
Opportunity recognition	May be a gender-related variable. Has potential to identify risk-taking males who own businesses with relatively high turnover as a scammers 'preferred' target
General business risk	Does not predict scam loss as well as the more context specific financial risk self-control measure, but may yet be useful in a larger sample and framework.
Routine activity	Very Good: Level of business online activity predicts 23% of variance in funds lost. Importantly it is **Business** online activities that are significant, not personal activities. This is direct evidence of the need to treat SB scams as a separate case to consumer scams.
Financial risk self-control	Moderate capacity to identify high and low risk groups.
Turnover	Too early to tell. Needs to be re-examined in another sample with more heterogonous turnover levels.

Table 7: List of potential scam propensity predictors

We hope that these observations and the tool yet to be developed will be useful in assisting to identify which small businesses and which scams should be the focus of policy and enforcement effort. We are not so naïve as to expect our efforts to stop the scammers but we do intend to make earning a dishonest living from the honest hard work of Australian small businesses a little harder than is currently the case.

The first step in achieving this aim would be to encourage all who read this report to pass it along to small business owners and associated industry groups. The next step is to ensure that every time we come across a new scam in our inbox, letterbox or web page that we take the time to report it to the authorities through services such as scamwatch (www.scamwatch.gov.au).

5.Future Research

Thus far, our research agenda has shed some light on the relationships between type of scam, scam prevalence and some behavioural cues known to affect scam propensity, but much more is left unknown. The long term aim of this project is to develop a model, or at least a range of indicators, of scam propensity (a business's likelihood of being scammed) that will have predictive value for identifying business types, locations and owner characteristics of those more likely to become victims of future scams. With this knowledge it will be possible to target future education and preventative measures at those where it will have the greatest impact on reducing overall economic and emotional loss.

To pursue this objective it will be necessary to undertake deeper more targeted enquiry regarding the behaviors of the scammed business and owner by interrogating a range of cases of known loss. This next step is necessary for sense making of the patterns that emerged from the first prevalence survey and to test the predictors on a larger sample of known scam victims.

At present we have made observations from a sample of respondents that may or may not have lost time or money to a scammer, to which we are attaching meaning and reason. This approach is a valid beginning which needs now to be followed up with a more targeted method that focusses solely upon those who have experienced losses and on losses that are of greater magnitude and variety. We hope to work with federal bodies such as the ACCC scamwatch to reach out to small business scam victims to do just that in the next phase of this research.

6.References

Australian Bureau of Statistics. (2007). Counts of Australian Businesses, Including Entries and Exits, Cat 8165.0. Canberra: ABS.

Australian Bureau of Statistics. (2012). Counts of Australian Business Operators (2011) Report Number: 8175.0. Canberra: ABS.

Brody, R.G., Mulig, E. and Kimball, V. (2007) "Phishing, pharming and identity theft" *Academy of Accounting and Financial Studies Journal*, Vol. 11 (3), pp. 43-56.

Cohen, L. E. and Felson, M. (1979) "Social change and crime rate trends: a routine activity approach" *American Sociological Review,* Vol. 44, pp. 588-608.

Farrar, J. H. (2011) "Fighting identity crime" *Bond Law Review*, Vol. 23 (1), pp. 88-101.

Holtfreter, K., Reisig, M. D. and Pratt, T.C. (2008) "Low self-control, routine activities, and fraud victimization", *Criminology,* Vol. 46 (1), pp. 189-220.

Holtfreter, K., Reisig, M. D., Piquero, N. L. and Piquero, A. R. (2010) "Low self-control and fraud: offending, victimization, and their overlap" *Criminal Justice and Behavior,* Vol. 37 (2), pp. 188-203.

Hutchings, A. and Hayes, H. (2009) "Routine activity theory and phishing victimisation: who gets caught in the net" *Current issues in Criminal Justice,* Vol. 20 (3), pp. 433-452.

Langenderfer, J. and Shimp. T. A. (2001) "Consumer vulnerability to scams, swindles and fraud: a new theory of visceral influences on persuasion" *Psychology & Marketing,* Vol. 18 (7), pp. 763-783.

Reyns, B. W. (2011) "Online routines and identity theft victimization: further expanding routine activity theory beyond direct-contact offenses", *Journal of Research in Crime and Delinquency*. DOI: 10.1177/0022427811425539.

Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). "Routine Online Activity and Internet Fraud Targeting: Extending the Generality of Routine Activity Theory". *Journal of Research in Crime and Delinquency*, Vol.47 (3), pp.267-296. doi: 10.1177/0022427810365903.

Tittle, C. R., Ward, D. A. and Grasmick, H. G. (2003) "Gender, age and crime/deviance: a challenge to self-control theory" *Journal of Research in Crime and Delinquency,* Vol. 40 (4), pp. 426-453.

Van Wilsem, J. A. (2011) "Bought it but never got it: assessing risk factors for online consumer fraud victimization" *European Sociological Review,* Vol. 27 (3), pp.1-11.

Vohs, K., Chin, J. & Baumeister, R. 2007. Feeling duped: emotional, motivational and cognitive aspects of being exploited by others. *Review of General Psychology,* Vol. 11**,** pp. 127-141.

Schaper, M. T., & Weber, P. (2012). Understanding Small Business Scams. Journal of Enterprising Culture, 20(03), pp. 333-356.

Shane, S., Nicolaou, N., Cherkas, L., & Spector, T. D. (2010). "Do openness to experience and recognizing opportunities have the same genetic source?" *Human Resource Management*, 49(2), 291-303.

Yar, M. (2005) "The novelty of 'cybercrime': an assessment in light of routine activity theory" *European Journal of Criminology,* Vol. 2 (4), pp. 407-427.

7. Appendices

7.1 Questionnaire Screenshots

Participants in this study were recruited via emails sent from trusted sources such as industry and small business associations that they are members of or by clicking on the web link to the survey in newsletters or on websites. At no stage was Curtin provided with the email distribution lists used to communicate the recruitment request.

Here is the member recruitment email text:

Curtin University research project: Understanding Small Business Scams

Recent international research shows that the majority of small businesses have lost money and time to scammers. Are you at risk?

Do you know what the common and emerging scam risks are for small businesses like yours and just what the level of loss is in your industry?

By completing this survey you will be assisting us and your industry in developing an understanding of small business scams in Australia, the proportion of small businesses that have fallen victim to these scams, the reasons why they accepted, and most importantly, what can be done to prevent it from happening in the future.

Even if you have not experienced a scam loss yet your involvement may provide important clues about why you have not been targeted.

If you are willing to assist please click on the link here to begin http://curtinbusiness.asia.qualtrics.com/SE/?SID=SV_djauP8WPTlpfY1e, or visit www.business.curtin.edu.au/business/small-business to learn more.

There is a prize incentive for participation.

The following pages provide screen images of the online questionnaire. Some functionality cannot be displayed in a static screen shot, such as the timed completion screen for example. The first page constitutes an online version of an information sheet. An opt-in or opt-out decision was required prior to any data collection. The decision is a yes no choice made after reading the first page of the survey.

Curtin Business School
Research to help *Slam Small Business Scams*

Curtin University of Technology

Understanding Small Business Scams in Australia

The Australian Competition and Consumer Commission *ScamWatch* suggests that owners of small businesses and their staff need to remain vigilant...

If it looks too good to be true...it probably is!

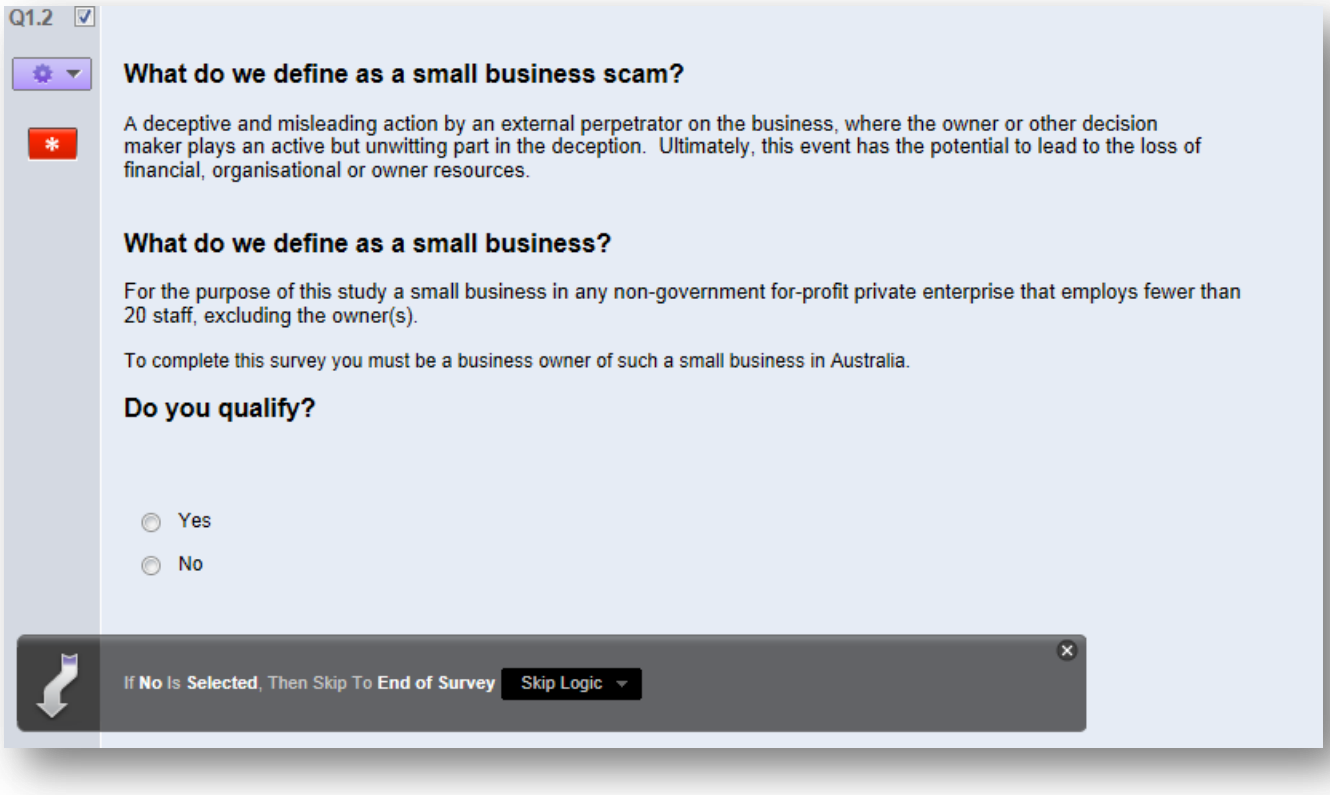
If you own a small business, we need to hear from you, regardless of whether or not you have been scammed

About the Study

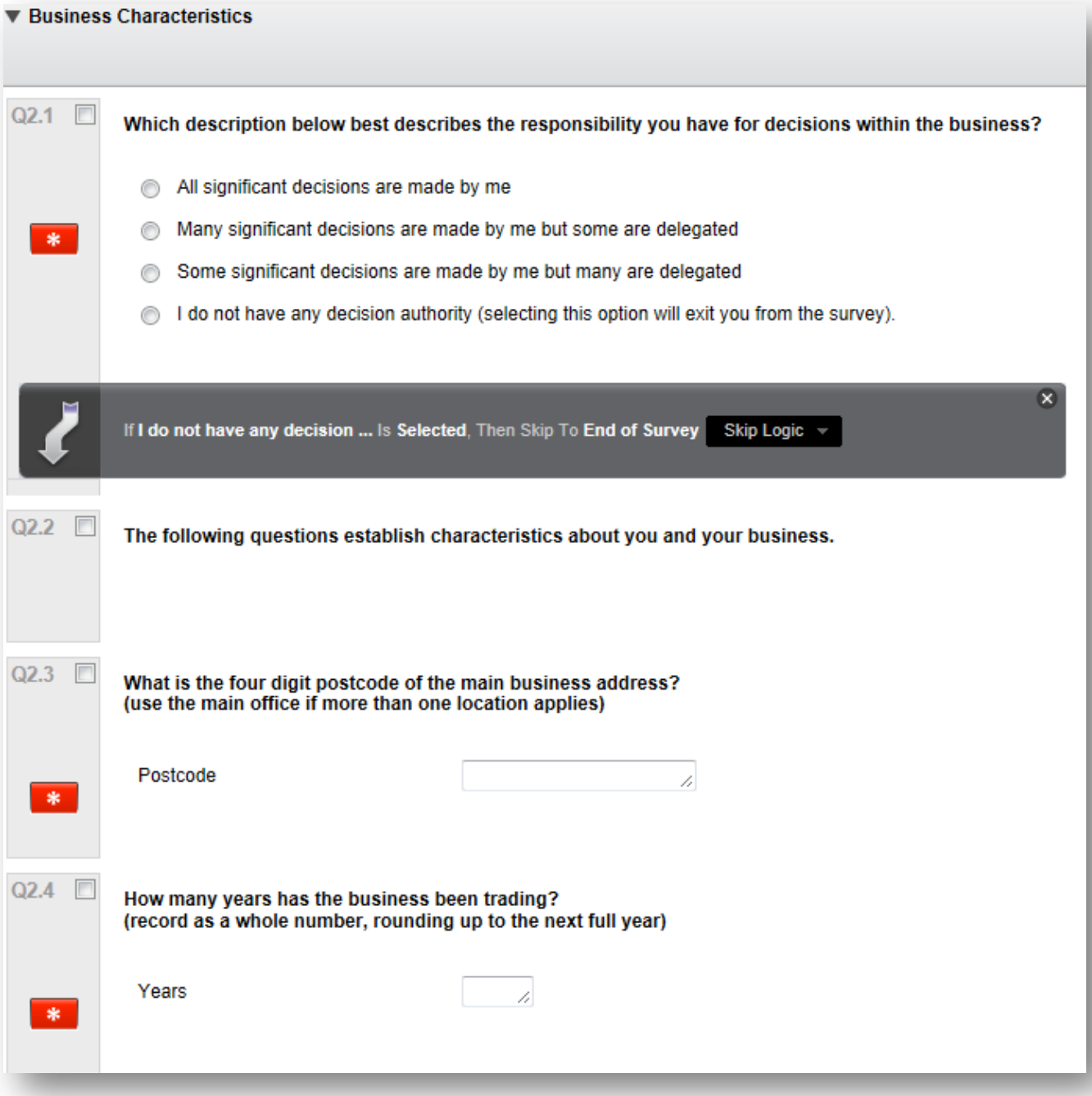
Small businesses face particular problems dealing with scams that differ from consumer and larger firm challenges. This study contrasts small businesses that have lost resources to scams with those who have not, searching for patterns that may assist with identifying strategies to reduce future losses. The data will be collected from multiple industries throughout Australia. We intend to publish aggregated reports to highlight scam victimisation rates to assist in targeting education and risk mitigation strategies.

The protection of your privacy is very important to us. Therefore, data gathered from this study will only be published after any identifying information has been removed. Whilst your contribution to this study is important and greatly appreciated, you will remain free to withdraw at any time. **If you have any concerns or questions please contact the research team via email to: smesurvey@curtin.edu.au or by telephone to Dr Paull Weber +61 8 92667413. You are also free to contact the Human Research Ethics Committee Secretary should you wish to make a complaint by phoning +61 8 9266 2784 or emailing hrec@curtin.edu.au or in writing C/- Office of Research and Development, Curtin University of Technology, GPO Box U1987, Perth WA 6845. Quoting the ethics review approval number SOM-15-2012**

7.1.1 QUALIFYING QUESTION



7.1.2 BUSINESS AND OWNER CHARACTERISTICS



Q2.10

In the last financial year, what was the turnover of your business?
(report this number as thousands (000's) of dollars).

Example: for a turnover of $50,000 ***enter 50***, for a turnover of $1,000,000 (one million) ***enter 1000.***

You may, if you chose, skip this question. However, we implore you to complete this question as it is an important factor that we want to investigate. We reiterate, your results will not be revealed or published in an individually identifiable way

Thousdands (000's)

Q2.11

As a cross-check, please select the category that best describes your business turnover for the last financial year

- < $10,000
- $10,000 - $24,999
- $25,000 - $49,999
- $50,000 - $99,999
- $100,000 - $199,999
- $200,000 - $399,999
- $300,000 - $399,999
- $400,000 - $499,000
- $500,000 - $599,999
- $600,000 - $999,999
- $1 million - $2.5 million
- $2.5 million - $5 million
- Greater than $5 million
- I prefer not to disclose

Q3.1

What year were you born?

2004

Q3.2

What is your gender?

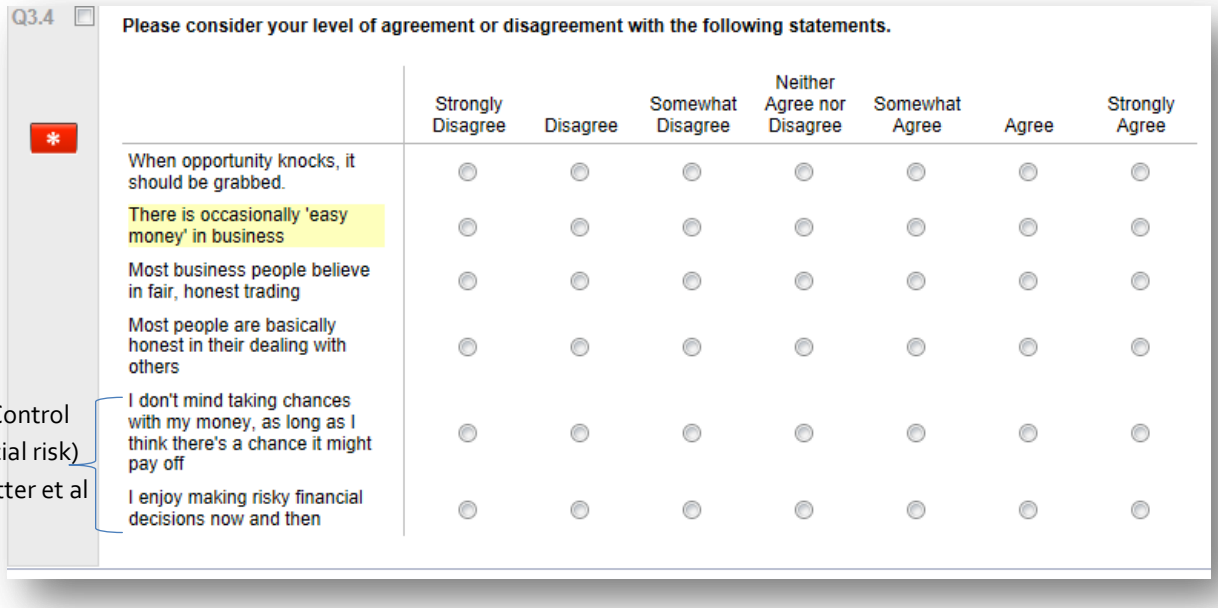
Male | Female | I prefer not to answer

Q3.3

What is the highest level of education you have completed?

- Less than High School
- High School
- Some Technical College or Tafe
- 3-year Undergraduate Degree
- 4-year Undergraduate Degree
- Masters Degree
- Doctoral Degree
- Other (describe)

7.1.3 PERSONALITY TRAITS



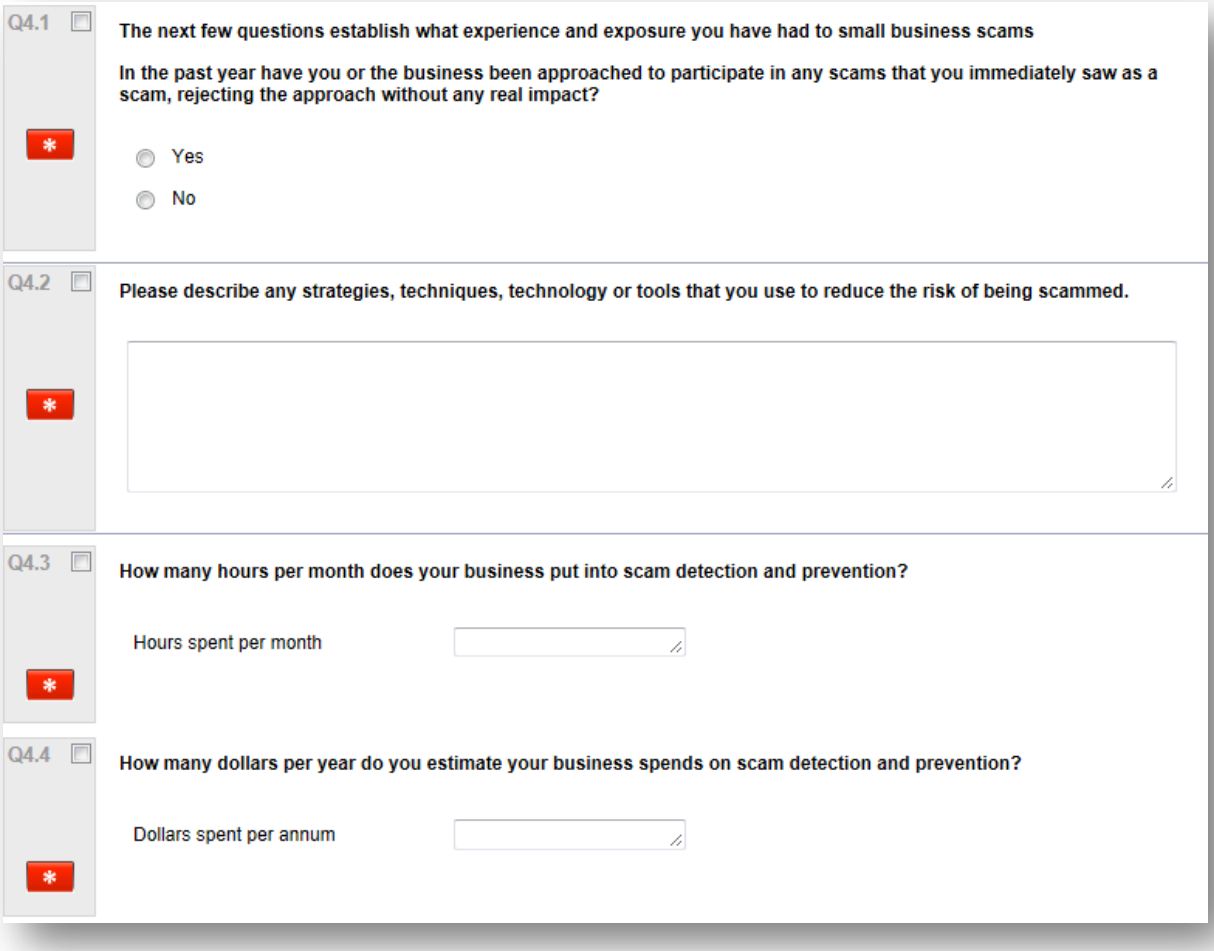
Q3.4

Please consider your level of agreement or disagreement with the following statements.

	Strongly Disagree	Disagree	Somewhat Disagree	Neither Agree nor Disagree	Somewhat Agree	Agree	Strongly Agree
When opportunity knocks, it should be grabbed.							
There is occasionally 'easy money' in business							
Most business people believe in fair, honest trading							
Most people are basically honest in their dealing with others							
I don't mind taking chances with my money, as long as I think there's a chance it might pay off							
I enjoy making risky financial decisions now and then							

Self-Control (financial risk) Holtfretter et al

7.1.4 EXPOSURE TO PRIOR SCAMS INCLUDING DETAILS OF QUANTUM, TYPE AND MEDIUM



Q4.1

The next few questions establish what experience and exposure you have had to small business scams

In the past year have you or the business been approached to participate in any scams that you immediately saw as a scam, rejecting the approach without any real impact?

- Yes
- No

Q4.2

Please describe any strategies, techniques, technology or tools that you use to reduce the risk of being scammed.

Q4.3

How many hours per month does your business put into scam detection and prevention?

Hours spent per month

Q4.4

How many dollars per year do you estimate your business spends on scam detection and prevention?

Dollars spent per annum

Q4.5

Do you recall any scam attempts against your business in the past year?
If so, please indicate what method of communication the scammer first used.
(you will need to select more than one category where you experienced multiple scam approach modes)

*If you are unsure what a particular type of scam is, **hover your mouse cursor over the category title** and a more complete description will appear (definitions ex ACCC little black book of scams 2012).*

	Fax	Mail	Email	SMS	Social Media	Land line	In person	Other
Advance fee/up-front payment (inc. Nigerian Scams)	○	○	○	○	○	○	○	○
Faxback premium phone numbers	○	○	○	○	○	○	○	○
False billing (advertising and directories)	○	○	○	○	○	○	○	○
False billing (office supplies)	○	○	○	○	○	○	○	○
False billing (domain names)	○	○	○	○	○	○	○	○
Credit card-card not present	○	○	○	○	○	○	○	○
Bank account phishing	○	○	○	○	○	○	○	○
Overpayment refund scams	○	○	○	○	○	○	○	○
Computer hacking (where an error allowed the hacker access)	○	○	○	○	○	○	○	○
Spam and 'free' offers on the internet	○	○	○	○	○	○	○	○
Investment seminars and real estate	○	○	○	○	○	○	○	○
Job and employment (including business opportunity)	○	○	○	○	○	○	○	○
Lottery and sweepstakes and unexpected prizes	○	○	○	○	○	○	○	○
Chain letter and pyramid schemes	○	○	○	○	○	○	○	○
Other (please describe)	○	○	○	○	○	○	○	○
I do not recall	○	○	○	○	○	○	○	○

Q4.6

Estimate how much money and time you lost last year to each scam type that you identified in the previous question. If you lost a days work and $500 that would be 5 = $500 in the first column and 10 hours (if you spent a 10 hour period resolving the problem)

	Hundreds of dollars($)	Hours
Advance Fee/Up front payment (inc. Nigerian scams)		
Faxback premium phone numbers		
False billing (advertising and directories)		
False billing (office supplies)		
False billing (domain names)		
Credit card- card not present		
Bank account phishing		
Overpayment refund scams		
Computer hacking (where an error allowed the hacker access)		
Spam and 'free' offers on the internet		
Investment seminars and real estate		
Job and employment (including business opportunity)		
Lottery and sweepstakes and unexpected prizes		
Chain letter and pyramid schemes		
Other (describe)		

Q4.7

If you want to tell us more about your specific case please use the free form text box below to describe in as much or as little extra detail as you wish. This question is optional.

Q4.8

Please describe any other types of loss, other than time or money that scams have caused.

*

7.1.5 E-COMMERCE ACTIVITIES, PERSONAL AND COMMERCIAL

Q5.1

We now focus e-commerce activities. How often do ***you personally*** do any of the following?

*

	multiple times every day	once a day	once a week	once a month	once a year	only once or twice ever	never
Order a product/service by filling out a form on the web							
Create or update a personal web page							
Listen to a radio or video broadcast online							
Make a telephone call or video call via your computer							
Access social media (Facebook or similar)							
Access social media (Twitter or similar)							
Share music or video online							

Q5.2

How often does *your business* undertake any of these internet-based activities?

*

	multiple times every day	once a day	once a week	once a month	once a year	only once or twice ever	never
Make a sale via your own E-commerce solution (shopping basket on your website)							
Make a sale using a third party online sales platform (such as E-bay)							
Purchase goods and services for your business online							
Use internet based video conferencing (such as Skype) for business purposes							
Access social media (such as Twitter or Facebook) for business purposes							
Communicate with customers via email							
Communicate with staff via email							
Other activity (describe)							

7.1.6 REMOTE PURCHASING BEHAVIOURS

Remote Purchasing Holfretter (Unguarded exposure to Purchasing, additive index)

Q6.1 In the past 12 months have you responded to a telemarketer that you had **not** previously done business with?

Yes No

Q6.2 **In the past 12 months have you purchased something from an Internet website?**

Yes No

Q6.3 **In the past 12 months have you ordered a product after seeing a television advertisement or infomercial?**

Yes No

Q6.4 In the past 12 months have you ordered a product after receiving an unsolicited piece of mail from a company with whom you had **not** previously done business?

Yes No

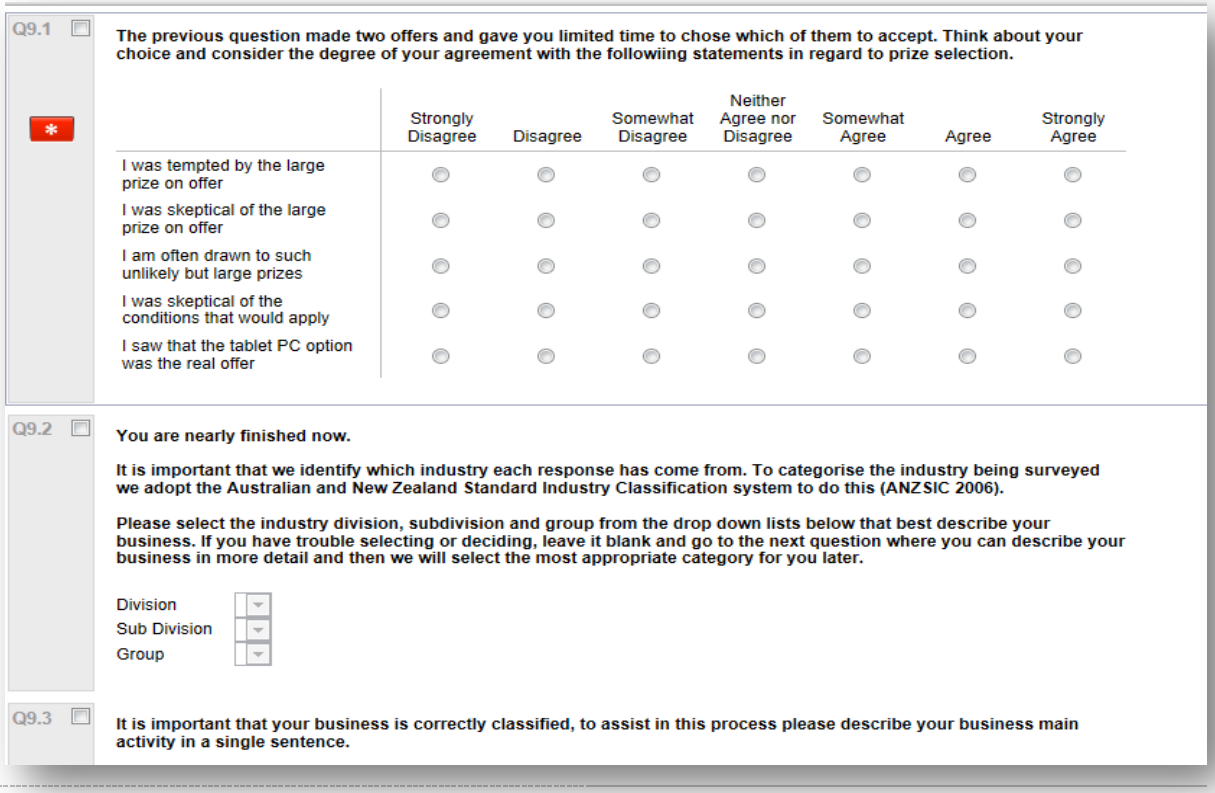
7.1.7 GENERAL BUSINESS RISK PROPENSITY

Q7.1 **What is your position in regard to the risk level of business decisions that you make?**

	Very inaccurate description	Inaccurate description	Somewhat inaccurate description	Neutral	Somewhat accurate description	Accurate description	Very accurate description
I like to take chances, although I may fail.							
Although a new thing has a high promise of reward, I do not want to be the first one to try it.							
When I have to make a decision for which the consequence is not clear, I like to go with the safer option although it may yield limited rewards.							
I like to try new things, knowing well that some of them will disappoint.							
To earn greater rewards, I am willing to take higher risks.							

7.1.8 GULLIBILITY/LONG ODDS ATTRACTION

7.1.9 EXPERIMENT DISCLOSURE AND ANZSIC CODE SELECTOR



7.1.10 CONFIDENCE IN DETECTING SCAMS AND PREFERRED SOURCES OF ASSISTANCE

Q10.1

On a scale of one to ten, how confident are you that you can identify a scam when you see one?

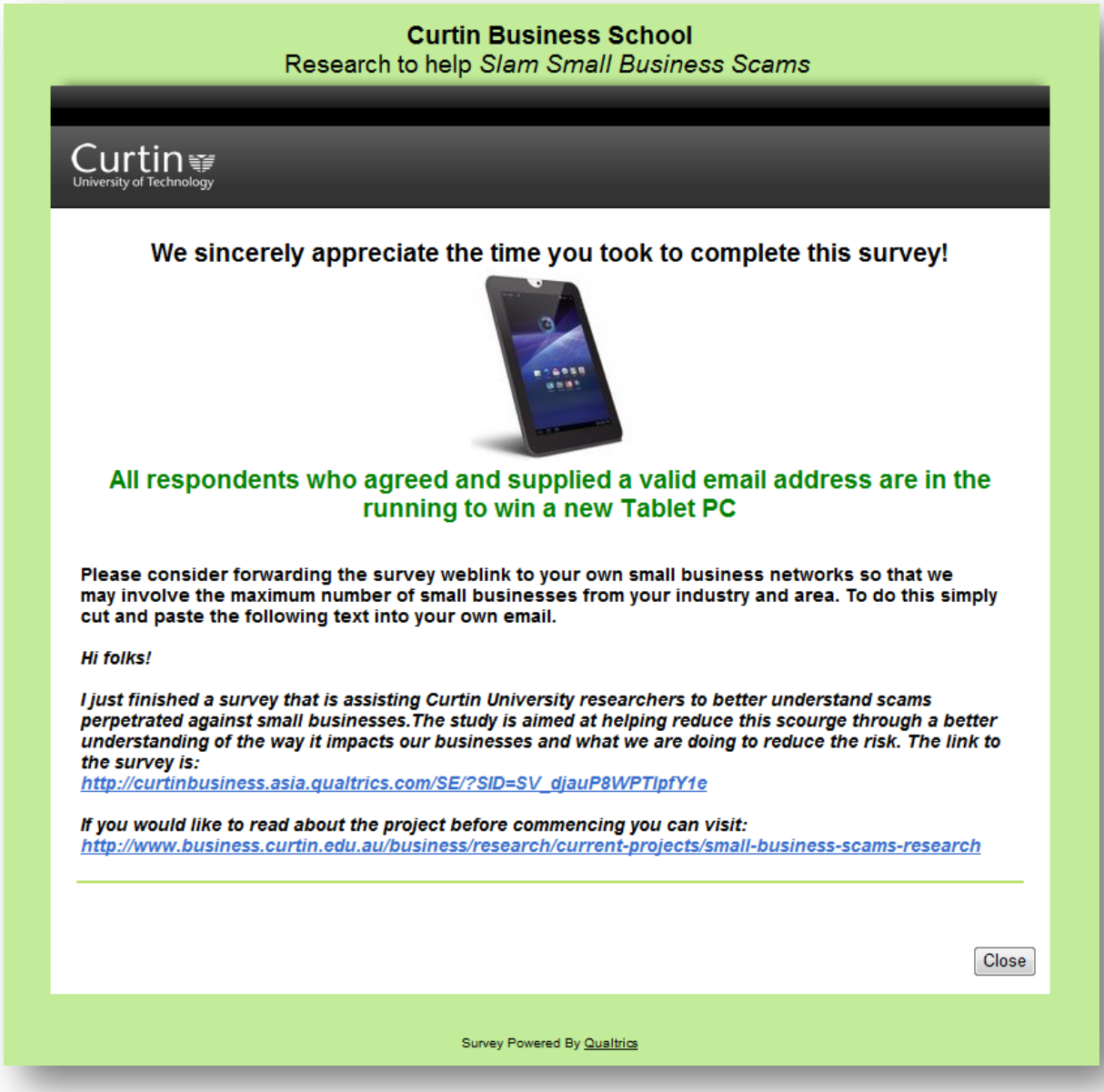
Drag the lever below the dial to the number that you think matches your level of confidence (where zero is no confidence and 10 is perfect confidence)

Q10.2

Who would you be most likely to seek advice from if you were unsure whether an approach that was made to you was legitimate or a scam?

- Your industry association
- ACCC ScamWatch
- The police
- The state consumer protection agency
- A family member
- A friend
- A fellow business owner
- A business advisor (banker, accountant, lawyer, consultant etc)
- Other (describe)

Opt-in email addresses were collected for the purpose of a prize draw and to forward a copy of this report.



The winner of the prize was advised and their prize of an Apple iPad was forwarded in April 2014 along with details of the report to all who expressed an interest.

7.2 Exhibits

The survey participants were recruited via participating organisations by positioning messages on their websites, within their newsletters, social media and other networks/ events as well as (in some cases) via outbound recruitment emails to their membership.

The following pages detail the range of mediums, messages and channels that were utilised in spreading the details about the project. Because of the networked (snowball) methodology employed we do not have any data on the number of SMEs that would have received this message. This is primarily due to privacy concerns (we were not able to access the email lists of partnering organisations), but it is reasonable to assert that it was a significant national awareness exercise in its own right in relation to the existence and variety of Small Business Scams.

Suggested text for email recruitment

(participating organisations customize and on-forward to their mail lists)

Curtin University research project: Understanding Small Business Scams

Recent international research shows that the majority of small businesses have lost money and time to scammers. Are you at risk?

Do you know what the common and emerging scam risks are for small businesses like yours and just what the level of loss is in your industry?

By completing this survey you will be assisting us and your industry in developing an understanding of small business scams in Australia, the proportion of small businesses that have fallen victim to these scams, the reasons why they accepted, and most importantly, what can be done to prevent it from happening in the future. Even if you have not experienced a scam loss yet your involvement may provide important clues about why you have not been targeted.

If you are willing to assist please click on the link here to begin http://curtinbusiness.asia.qualtrics.com/SE/?SID=SV_djauP8WPTlpfY1e, or visit www.business.curtin.edu.au/business/small-business to learn more.
There is a prize of a new Tablet (PC or ipad) available as an incentive for your participation

Suggested text for newsletters and extended website commentary

Curtin University Launches the Small Business Scams Prevalence Study

Are you a business owner at risk of being scammed?

Do you know what the common and emerging scam risks are for small businesses and just what the level of loss is in your industry?

Research overseas suggests that the majority of small businesses will sooner or later burn money and time to scammers. A recent study conducted by the Federation of Small Business in the UK showed that 54% of small businesses had been a victim of some form of online crime or fraud. ***Yes, that's right more than half!*** *Here in Australia recent data released by the Australian Bureau of Statistics indicates that over one third of Australian consumers were exposed to a scam in 2011, with roughly one in ten of those exposed losing money to the scammer.*

What about small businesses in Australia? Do they get scammed as much, more or less than individual consumers?

Curtin University in Western Australia undertook a preliminary survey of WA businesses in 2010/11 which suggests that the rate of loss from businesses is potentially ***five times that of consumers****. In addition, you may be surprised to hear that* ***one in eight small business owners*** *was unable to determine whether they had been scammed or not. So, if you are unsure, you are not alone.*

Results point to a potential relationship between the prior experience of the business owner; the turnover of the business; the type of business; e-commerce capabilities of the owner and the business in determining scam risk propensity. These indicative WA results are now being investigated to see if they hold true at the national level across multiple industries and regions.

So, if you have not experienced a scam loss yet you may be in the lucky minority, you may be very careful, it might be your turn next, or you may simply be unaware of money already lost. Regardless of whether you believe you have been scammed or not you should invest 15 minutes of your time to complete the Small Business Scams survey. Whilst completing this task ***you will actually learn more about the many types of scams that are around.***

We encourage you to participate in this study. The results are likely to be of benefit to understand scams in our industry if enough members get involved.

ACTION:
If you are able to assist now you can click on the link below to begin:
http://curtinbusiness.asia.qualtrics.com/SE/?SID=SV_djauP8WPTlpfY1e
Or *you can visit www.business.curtin.edu.au/business/small-business to learn more first.*

There is a prize of a new Tablet (PC or ipad) available as an incentive for your participation. The survey opened on May 3rd 2012 and will run until September 2012, with results released later in the year.

All individual level data is confidential and only the aggregate results will be released.

Selected examples of communications used

7.2.1 ECONOMIC DEVELOPMENT AUSTRALIA

Scam Busters

Not until Curtin Business School approached us did we realise the huge volume of programs and time and effort that is being ploughed into containing scammers and trying to eliminate them. While no one is honestly thinking they will eliminate scammers completely we can make life difficult for them by fewer and fewer of us falling victim to their devious ways!

The Australian Competition and Consumer Commission (ACCC) have set up a web site devoted to it: Scamwatch and there you will see just how many forms scams can take. They include Investment Scams, Job & Employment scams, Banking and Online account scams, Mobile phone scams, Lottery and Competition scams and of course the infamous Money transfer or 'Nigerian' scam plus many others.

Curtin Business School are set on finding out how big a problem this is Read more

7.2.1 AUSTRALIAN FEDERATION OF TRAVEL AGENTS

Curtin University Launches Small Business Scams Prevalence Study

Do you know what the common and emerging scam risks are for small businesses and just what the level of loss is in our industry?

Research overseas suggests that the majority of small businesses will sooner or later burn money and time due to scammers. A recent study conducted by the Federation of Small Business in the UK showed that 54% of small businesses had been a victim of some form of online crime or fraud. **Here in Australia recent data released by the Australian Bureau of Statistics indicates that over one third of Australian consumers were exposed to a scam in 2011, with roughly one in ten of those exposed losing money to the scammer.**

Curtin University in Western Australia undertook a preliminary survey of WA businesses in 2010/11 which suggests that the rate of loss from businesses is potentially **five times that of consumers.** In addition, you may be surprised to hear that **one in eight small business owners** was unable to determine whether they had been scammed or not.

Results point to a potential relationship between the prior experience of the business owner; the turnover of the business; the type of business; e-commerce capabilities of the owner and the business in determining scam risk propensity. These indicative WA results are now being investigated to see if they hold true at the national level across multiple industries and regions.

Regardless of whether you have been scammed or not, we encourage you to invest 15 minutes of your time to complete the Small Business Scams survey. Whilst completing this task **you will actually learn more about the many types of scams that are around.** The results are likely to be of benefit to understand scams in our industry if enough members get involved.

Simply click on the link below to begin: http://curtinbusiness.asia.qualtrics.com/SE/?SID=SVdjauP8WPTlpfY1e

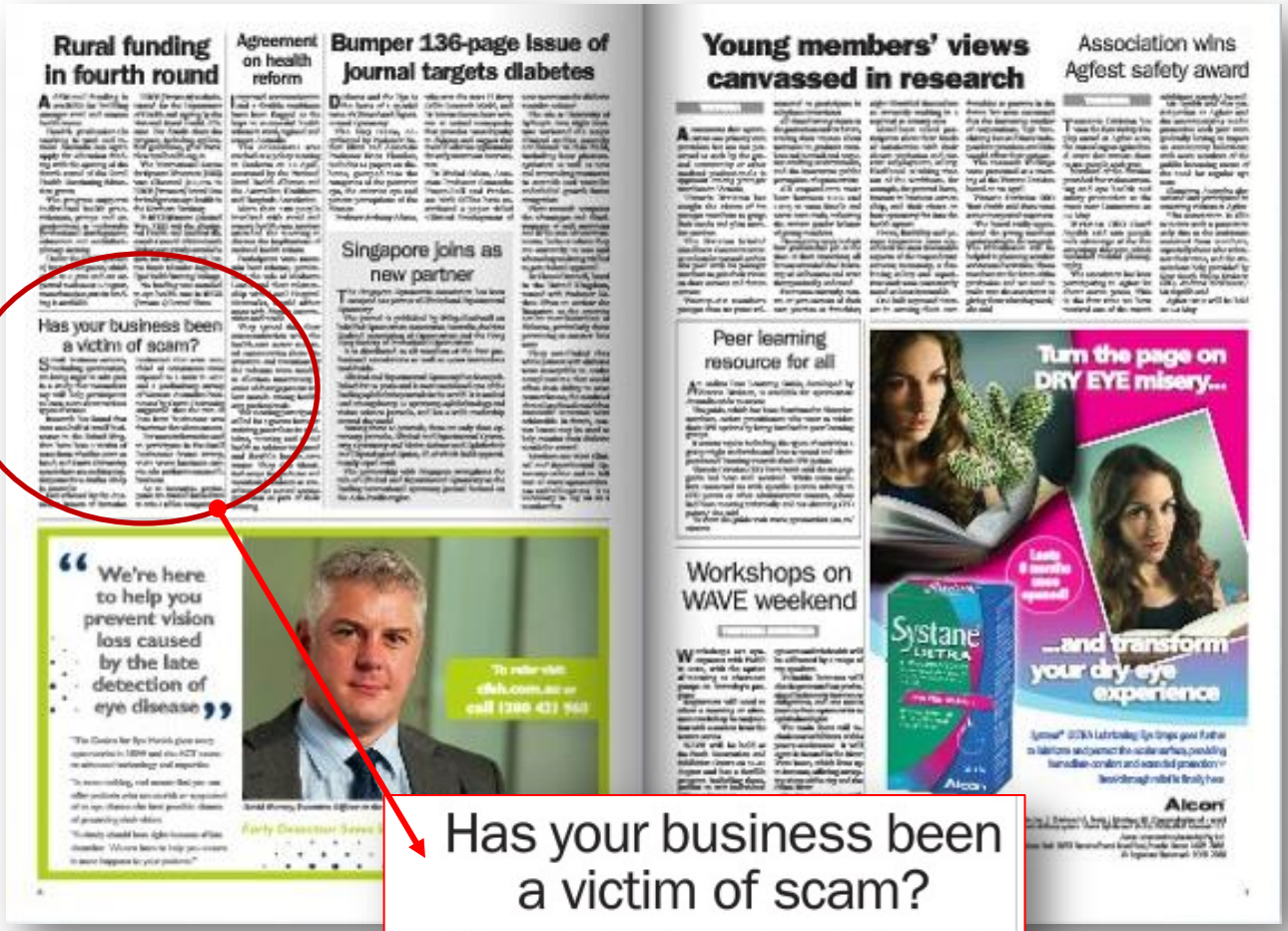
Or visit www.business.curtin.edu.au/business/small-business to learn more.

One lucky participant will win a Tablet PC as a prize for participation. The survey will run until September 2012, with results released later in the year.

All individual level data is confidential and only the aggregate results will be released.

The Australian Federation of Travel Agents Ltd • ABN 72 001 444 275 • Level 3, 309 Pitt St Sydney NSW 2000 • afta@afta.com.au

7.2.3 OPTOMETRISTS ASSOCIATION



Has your business been a victim of scam?

Small business owners, including optometrists, are being urged to take part in a study that researchers say will help participants to learn more about various types of scams.

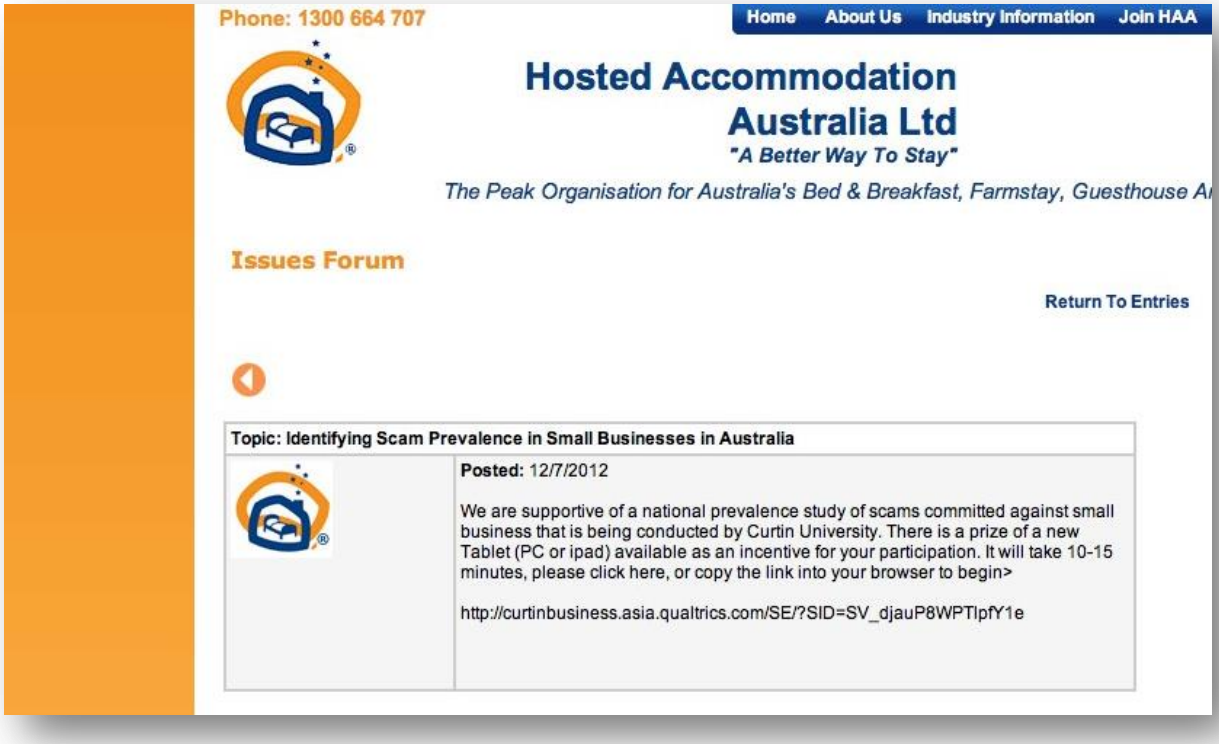
Research has found that over one-half of small businesses in the United Kingdom have been a victim of some form of online scam or fraud, and Curtin University researchers are seeking participants for a similar study in Australia.

Data released by the Australian Bureau of Statistics indicated that over one-third of consumers were exposed to a scam in 2011 and a preliminary survey of Western Australian businesses by Curtin University suggested that the rate of loss from businesses was five times that of consumers.

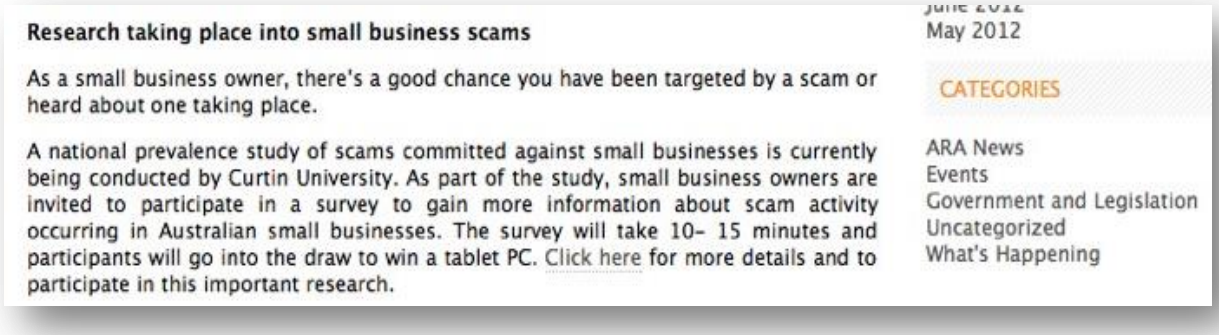
For more information and to participate in the Small Businesses Scams survey, visit www.business.curtin.edu.au/business/small-business.

As an incentive, participants are entered into a draw to win a tablet computer.

7.2.4 HOSTED ACCOMMODATION AUSTRALIA



7.2.5 AUSTRALIAN RETAILERS ASSOCIATION



7.2.6 PHARMACY GUILD

Small business scam study

Curtin Business School in Western Australia is conducting a project to investigate the prevalence of scams committed against small businesses in Australia.

Despite the reality that there are about two million small businesses in Australia, no research has ever been undertaken in this country to better understand the level of scam risk.

Recent research conducted in the United Kingdom in 2009 showed that over half of small businesses had been a victim of some form of fraud or online crime in the preceding year.

The project is funded by a Linkage with Business seed grant from Curtin Business School. The long term aim of the project is to develop strategies to reduce the level of risk and prevent future attacks from scammers.

The Australian Competition and Consumer Commission supports this project. The Guild, along with a number of other national small business industry associations, who are members of the ACCC Small Business Consultative Committee, have also expressed interest in and support for the research work and survey being undertaken by the Curtin Business School .

A survey can be filled out online and pharmacists are encouraged to participate as members of the small business community.

Fill out the survey here.

The ACCC keeps a list of all current scams to be wary of updated at Scam Watch.

7.2.6 REAL ESTATE INSTITUTE OF AUSTRALIA

BEWARE OF SCAMS

Real estate agents, like all small businesses, are the target of scammers.

One of the most common scams is false billing with an estimated one in six small businesses that have reported this activity to the Australian Competition and Consumer Commission (ACCC) having lost money. The amount lost by small businesses has been estimated to be around $1m in 2010.

False billing scams target businesses to trick them into paying for unwanted or unauthorised listings or advertisements in magazines, journals, business registers or directories. Common scam tactics are to send a business a subscription form disguised as an outstanding invoice to get the business to sign up for unwanted ongoing advertising services.

Other common scams targeting small business include: banking and online phishing scams; job and employment scams including business opportunities, and; fax back scams. A faxback scam can offer you anything from fantastic deals, business directory entries and competition entries—all you have to do is send a fax back to a premium rate number (usually starting with 19). Premium rate faxes can be charged at more than $6.00 per minute. The scammers make sure your fax takes several minutes to get through, resulting in a high phone bill.

One relatively recent scam targeted at agents managing rental properties involved a fax asking for details of non-resident landlords. The letter with the Australian emblem in the corner suggests that once the details are forwarded rental income will be available without paying any Australian tax. Details sought include Australian passport details. The ATO feels that the scammer's objective is identity theft.

Surveys conducted by the Australian Institute of Criminology show an overall trend away from scam delivery by mail towards the use of email and telecommunications such as landlines, mobile phones and SMS, to contact potential victims. These results may indicate that scammers are adapting to consumer uptake of new technologies such as smartphones and/or that scammers are moving away from 'traditional' methods as potential victims become more aware of these. The surveys also show that although a higher percentage of respondents reported receiving a scam in 2011 (94.2% compared with 89.0% in 2010), the percentage that responded to the scam was lower (25.2% in 2011 compared with 29.3% in 2010). Similarly, fewer respondents reported a financial loss or loss of personal information as the result of a scam in 2011 compared to 2010. In 2011 almost 60% of respondents were female, and the largest age category of respondents was 45-54 years. The highest proportion of respondents came from New South Wales.

7.2.7 THE CONVERSATION

http://theconversation.edu.au/click-here-for-bankruptcy-scamming-and-small-businesses-7084

Click here for bankruptcy! Scamming and small businesses

AUTHOR

Paull Weber
Senior Lecturer, Small Business and Entrepreneurship at Curtin University

DISCLOSURE STATEMENT

Paull Weber does not work for, consult to, own shares in or receive funding from any company or organisation that would benefit from this article, and has no relevant affiliations.

The Conversation provides independent analysis and commentary from academics and researchers.

Founding and Strategic Partners are CSIRO, Melbourne, Monash, RMIT, UTS and UWA. Members are Deakin, Flinders, Murdoch, QUT, Swinburne, UniSA, UTAS, and VU.

According to Australia's consumer watchdog, small businesses are particularly vulnerable to online scams. Flickr/Dan Hankins

A significant proportion of these reports come from small businesses but no specific small business data is available from existing Scamwatch reports.

According to Dr Michael Schaper, ACCC deputy chairman and chair of the Australasian Consumer Fraud Taskforce, small businesses