Online Credit Card Fraud against Small Businesses

Kate Charlton
Natalie Taylor

Research and Public Policy Series

No. 60

Australian Institute of Criminology

Australian Institute of Criminology
Research and Public Policy Series

No. 40 *Homicide in Australia: 2000–2001 National Homicide Monitoring Program (NHMP) Annual Report,* Jenny Mouzos, 2002

No. 41 *Drug Use Monitoring in Australia: 2001 Annual Report on Drug Use Among Police Detainees,* Toni Makkai and Kiah McGregor, 2002

No. 42 *Deaths in Custody in Australia: 2001 National Deaths in Custody Program (NDICP) Annual Report*, Lisa Collins, 2002

No. 43 *Hatred, Murder and Male Honour: Anti-homosexual Homicides in New South Wales, 1980–2000*, Stephen Tomsen, 2002

No. 45 *Review of Victoria Police Crime Statistics*, Carlos Carcach and Toni Makkai, 2002

No. 46 *Homicide in Australia: 2001–2002 National Homicide Monitoring Program (NHMP) Annual Report*, Jenny Mouzos, 2003

No. 47 *Drug Use Monitoring in Australia: 2002 Annual Report on Drug Use Among Police Detainees*, Toni Makkai and Kiah McGregor, 2003

No. 48 *Serious Fraud in Australia and New Zealand*, 2003

No. 49 *Sport, Physical Activity and Antisocial Behaviour in Youth*, Leesa Morris, Jo Sallybanks and Katie Willis, 2003

No. 50 *Deaths in Custody in Australia: 2002 National Deaths in Custody Program (NDICP) Annual Report*, Lisa Collins and Muzammil Ali, 2003

No. 51 *A Safe and Secure Environment for Older Australians*, Marianne James, Adam Graycar and Pat Mayhew, 2003

No. 52 *Drugs and Crime: A study of Incarcerated Male Offenders*. Toni Makkai and Jason Payne, 2003

No. 53 *Contract Killings in Australia*, Jenny Mouzos and John Venditto, 2004

No. 54 *ACT Recidivist Offrenders*, Toni Makkai, Jerry Ratcliffe, Keenan Veraar and Lisa Collins, 2004

No. 55 *Homicide in Australia: 2002–2003 National Homicide Monitoring Program (NHMP) Annual Report,* Jenny Mouzos, 2004

No. 56 *Women's Experiences of Male Violence: Findings from the Australian Component of the International Violence Against Women Survey*, Jenny Mouzos and Toni Makkai, 2004

No. 57 *Regulation: Enforcement and Compliance*, Richard Johnstone and Rick Sarre, 2004

No. 58 *Drug Use Monitoring in Australia: 2003 Annual Report on Drug Use Among Police Detainees*, Lee Milner, Jenny Mouzos and Toni Makkai, 2004

No. 59 *Sentencing the Multiple Offender: Judicial Practice and Legal Principle*, Austin Lovegrove, 2004

No. 60 *Online Credit Card Fraud against Small Businesses*, Kate Charlton and Natalie Taylor, 2004

Online Credit Card Fraud against Small Businesses

Kate Charlton
Natalie Taylor

No. 60

Research and Public Policy Series

Australian Government
Australian Institute of Criminology

ISSN 1326-6004

Charlton, Kate.
Online credit card fraud against small business.

Bibliography.
ISBN 0 642 53846 8.

1. Credit card fraud – Australia. 2. Internet fraud – Australia. I. Taylor, Natalie, 1964- . II. Australian Institute of Criminology. III. Title. (Series : Research and public policy series ; 60).

364.168

Published by the Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601
Tel: (02) 6260 9221
Fax: (02) 9260 9201
e-mail: aicpress@aic.gov.au
http://www.aic.gov.au

Edited and set by Sarah Christensen
Australian Institute of Criminology

Foreword

While the online retailing environment has provided businesses with an unparalleled opportunity to expand their customer bases and improve profits, it has also increased the vulnerability of businesses to online credit card fraud. The degree to which Australian businesses experience online credit card fraud, and the losses associated with such fraud, have not previously been properly quantified. This is due to both a paucity of research in this area and a tendency in previous surveys to use convenience samples and a range of different business types.

This report presents findings of an empirical study which used random stratified sampling of five types of small business in Australia. The study investigated proportions of online retailers within each business type, the prevalence of online credit card fraud among these retailers, financial losses due to online credit card fraud, knowledge about financial liability from online credit card fraud, preventive strategies used, and attitudes toward financial institutions.

The report provides a review of Australian and international research into online credit card fraud, as well as invaluable information relating to fraud risks and prevention strategies. The findings are intended to be of use to businesses that are considering retailing online, as well as a useful resource for policy-makers and researchers interested in the online retailing environment.

Toni Makkai
Director
Australian Institute of Criminology

Acknowledgments

The research reported in this paper was funded by the National Crime Prevention Program, Australian Government Attorney-General's Department, as part of a larger Crimes Against Small Business project.

This work could not have been undertaken without the cooperation of 1,078 small business retailers across Australia. We would like to thank them for their time and assistance in completing the telephone survey.

The authors would also like to acknowledge the comments provided on earlier drafts by AIC colleagues, the National Crime Prevention Program and external referees. In particular, thanks are extended to Dr Toni Makkai for her invaluable comments.

Disclaimer

This research report does not necessarily reflect the policy position of the Australian Government. While every effort has been made to ensure the accuracy of the information provided in this report at the time of printing, the nature of the online environment means that the use of, and guidelines for, online technology and fraud prevention measures are continually evolving. Independent advice should be sought before relying on the information provided in this report.

Contents

List of tables

List of figures

Glossary of terms

Cardholder	The legitimate owner of the credit card used to purchase goods or services from the business.
Chargeback	The amount of the transaction which the cardholder disputes, which is then removed from the bank account of the business in order to reimburse the cardholder. In this report, this amount is equated with the amount incurred from an incident of fraud.
Chargeback fee	A fee imposed on the retailer by their financial institution, in the event that a chargeback is issued.
'Clicks and mortar'	A business which trades online as well as having an actual physical store for customers to visit and purchase goods.
Customer	The person making the online purchase (not necessarily the cardholder).
EFTPOS	Electronic funds transfer at point of sale.
Electronic authorisation	The authorisation of a purchase using a designated credit card, which verifies that the account linked to the card is active and has sufficient funds to allow for the purchase. This can be done over the internet using a bank-facilitated web link (while the customer waits) or at a later stage by the retailer, using either a manual EFTPOS machine or by contacting an authorisation hotline. This process does not verify the identity of the customer, nor does it process a withdrawal from the customer's account.
Online trading	The sale of goods and/or services over the internet. Customers must enter and submit their credit card details online; the sale will often proceed without the retailer and customer ever having personal contact. Excluded from this definition is the practice of retailing through a central web site operated by another party, either a franchise head office or an external company, such as Interflora. It should be noted that the term 'online trading' does *not* refer to buying or selling shares over the internet. It also does not refer to accepting credit card details via email.

Online credit card fraud	A fraudulent purchase made online which is either not submitted by the legitimate cardholder or later claimed to be fraudulent by the cardholder.
'Pure clicks' business	A business which operates solely through online trading, without the need for a store.
Small business	A business employing fewer than 20 full-time personnel (ABS 2001). The terms 'retailer', 'trader' and 'proprietor' are used interchangeably in this report and all refer to a small business.

Scope of the report

Given that fraud is a wide-ranging term that encompasses a variety of crimes, it is important to identify the specific type of fraud which this report examines. Online credit card fraud – the crime investigated in this study – cuts across three broad categories of fraud:

- credit card fraud – for example, telephone credit card fraud or over-the-counter fraud;
- financial fraud – for example, misappropriation of funds (KPMG Fraud Survey 2002); and
- internet fraud – for example, auction fraud, letter scams (National White Collar Crime Center & FBI 2003).

The current research does not address all three of these broad types of fraud. Rather, it focuses exclusively on online credit card fraud perpetrated against small businesses that accept credit card purchases over the internet.

Executive summary

In 1999 the Australian Institute of Criminology (AIC) conducted a survey of crimes against small businesses in Australia which was funded by the National Crime Prevention program. The crimes that were covered included burglary, vandalism, shoplifting, cheque and credit card fraud, employee theft, employee fraud, assault, armed and unarmed robbery, and theft of and from vehicles. It did not cover online credit card fraud. The present study bridges this gap by examining the extent of online credit card fraud against small businesses in Australia.

The aims of the present study were to:

- provide a review of what is known about online credit card fraud;
- quantify the extent of online credit card fraud against small businesses in Australia within particular business types;
- identify factors that increase the risk of being a victim; and
- identify recommendations for improving online trading practices and reducing fraud.

Telephone interviews were conducted with 1,078 small businesses in five business types across Australia in April 2003. Small businesses were deemed as those that employed less than 20 full-time staff. The five business types chosen were those considered to be most likely to engage in online trading. These were:

- florists;
- booksellers;
- toy and game traders;
- computer hardware retailers; and
- recorded music retailers.

Trading online

Trading online varied across business type as follows. Eleven per cent of florists traded online, as did 17 per cent of booksellers, 15 per cent of recorded music retailers, 11 per cent of toy and game retailers and 13 per cent of computer hardware retailers.

Across the whole sample, 13 per cent of small businesses currently trade online and, of those not online, just over three-quarters (77%) believe that it is likely or very likely that they will commence online trading within the next two years. The vast majority of online traders are satisfied with the practice of online trading (89%) and intend to continue trading

in this way (93%). Just over half (56%) indicated that online trading had significantly increased sales.

Different business types were influenced by different factors when it came to trading online. Computer hardware retailers and booksellers were more likely to trade online if they believed that the risks posed by online credit card fraud were outweighed by the benefits of trading online. Florists, recorded music retailers and booksellers were more likely to trade online if they employed more staff. Most business types were more likely to trade online if they believed that the costs/time involved in online trading were reasonable.

Use of online fraud prevention measures

Online traders can try to minimise online credit card fraud through electronic authorisation and/or manual screening of transactions. Electronic authorisation involves confirming through financial institution systems that the card being used to make the purchase is active and has sufficient funds available. This can be done automatically (through an automatic link on the retailer's web site to bank systems) or manually (involving either a phone call to the bank for authorisation or processing on an EFTPOS terminal).

Online traders most commonly processed electronic authorisations manually (67%), with 25 per cent utilising automatic electronic authorisation systems while their customers waited online. Eight per cent only occasionally or never confirmed transactions electronically.

For increased protection, online traders are advised to screen transactions manually. Manual screening involves checking details of transactions or taking other steps to try to confirm the identity of the cardholder. This study found that:

- 55 per cent of online traders always phoned or emailed the customer to confirm the order;
- 41 per cent kept a database of good and bad online customers;
- 30 per cent always rejected suspicious orders; and
- 12 per cent consistently confirmed customer addresses in the phone book.

Online credit card fraud

The lifetime prevalence of online credit card fraud among online traders was as follows:

- 28 per cent of florists;
- 43 per cent of booksellers;

- 26 per cent of recorded music retailers;
- 33 per cent of toy and game retailers; and
- 30 per cent of computer hardware retailers.

Overall, 32 per cent of online traders had been a victim of online fraud at some stage. The figures for lifetime prevalence were considerably higher than the proportion of online traders who had been victimised in the past 12 months; these figures ranged from between 12 per cent (florists) and 22 per cent (booksellers) of each business type. Online traders were significantly more likely to report experiencing fraud if the proprietor was male, if the business attributed a higher percentage of their overall turnover to online trading and if they believed that manually screening orders reduced business productivity.

Repeat victimisation

Repeat victimisation from online credit card fraud was identified as an issue, with 51 per cent of all online traders who had ever experienced fraud experiencing more than one incident over a two-year period (2001 and 2002). Overall, 18 per cent of online credit card fraud victims accounted for 38 per cent of all incidents.

Reporting to police

Consistent with previous research showing that credit card fraud is heavily under-reported, this study found that:

- 35 per cent of incidents were reported to police in Australia in 2001; and
- 21 per cent of incidents were reported in 2002.

Perceptions of online credit card fraud

A small number of online traders reported that their experience of fraud victimisation was higher than their initial expectations (6%). Just under one-third (32%) believed that it was about the level they had expected, while just over half (56%) reported that the level of online fraud they had experienced was lower than they had expected. Hence the experience of online fraud was less than most online retailers had expected prior to trading online.

Knowledge about liability for online fraud

In contrast to over-the-counter credit card transactions, where businesses are not liable for fraudulent purchases, online traders are responsible for recouping losses associated

with online credit card fraud. Retailers who were currently trading or had previously traded online were more aware of their financial liability with respect to online credit card fraud (77%) than those who had never sold goods online (53%). However, knowledge of financial liability also increased with the actual experience of online credit card fraud. Eighty-eight per cent of victims were aware that the business would bear the primary responsibility in the event of fraud losses, compared to 73 per cent of past or current online traders who had never been victimised.

Finding out that fraud has occurred

Only six per cent of online traders had discovered the fraud themselves. The vast majority were advised of the fraud by their financial institution (91%). However, the amount of time that elapses before a trader is advised of a fraud can be lengthy. Half of the fraud victims were not notified for two months or more. Delays in notification of an incident of fraud can mean that a business may process several transactions on the same credit card, resulting in higher and continuing losses due to fraud.

Losses associated with online credit card fraud

Mean losses per victim (where the business was unable to recoup the loss) in Australia in 2002 varied across business type, starting from $100 for recorded music retailers up to $3,500 for booksellers. These losses can be considerable for an individual business, given that approximately 60 per cent of online fraud victims reported an annual turnover of less than $500,000.

Recommendations for better online trading practices

Fraud prevention measures were more likely to be put in place after an incident of fraud had occurred rather than before. Based on the findings from this survey, it is recommended that:

- online traders should be actively encouraged to implement fraud prevention measures *before* fraud occurs, as one incident of fraud may predispose a business to a repeat incident;
- online traders should be encouraged to utilise not only basic electronic authorisation, but also manual screening techniques, to minimise the risk of being a victim of online credit card fraud;

- financial institutions, where possible, should streamline their fraud notification procedures so that online traders are advised of a fraud as soon as financial institutions become aware of it;
- information about online fraud liability should be clearly articulated to potential online traders to ensure that they are aware of such liability; and
- online traders should be actively encouraged to report incidents of online credit card fraud to police. More regular reporting to police will allow for more accurate data to be collected about online fraud. Such information can assist police in identifying patterns of fraud being perpetrated against particular traders and will assist police to develop targeted policing strategies in relation to online fraud.

Section 1: Introduction

Why the need for this report?

In recent years, the online computing environment has afforded exciting new opportunities to buy and sell goods and services for both businesses and individuals. At the end of 2003, there were 4.5 million household subscribers and 696,000 business/government subscribers to the internet in Australia (ABS 2004). Moreover, the number of credit card transactions processed in Australia increased from 42.9 million in 1999 to 85.6 million in 2003 (Australian Payments Clearing Association 2003). In the United Kingdom, the number of people making internet card payments (using a credit or debit card) increased 50 per cent between 2002 and 2003, to 18 million (APACS 2004). This growing customer use of the internet and credit cards has provided businesses with the chance to expand their customer bases, provide quicker and more efficient service and reduce overheads.

With such a dramatic uptake of online trading, however, have come increased risks of online credit card fraud (Smith & Urbas 2001). In particular, businesses that trade online are more vulnerable than ever before to the risk of credit card fraud and associated losses. However, for online traders, not only do the risks of fraud increase, but their liability also increases. Because online transactions are of a 'card not present' nature, financial institutions are reluctant to cover such losses, thus the burden falls on the trader (Gibbons 2001; Lang 1999; Parliament of Victoria 2002). However, no serious attempt has yet been made to quantify, within clearly defined parameters, the nature and extent of online credit card fraud against businesses (particularly small businesses). The present report is intended to fill this gap.

Why are businesses that trade online at risk of online fraud?

The anonymous nature of online transactions can make the trading environment vulnerable to credit card fraud (Attorney-General's Department & OSCA 2000; Gibbons 2001; Shankar & Walker 2001). This type of crime is easily facilitated by the lack of any personal contact between the retailer and customer (Gibbons 2001; Smith 1999; Westpac 2000) during an online transaction. In an attempt to entice customers to trade online, the practice of protecting customers from being held financially responsible for fraudulent use of their credit card has been favoured. Assuming the transaction was reported as fraudulent to the customer's financial institution and it has been agreed that the customer did not contribute to the losses (Abru 2000), financial institutions do not generally hold customers liable. This has understandably occurred in order to encourage consumers to purchase goods online and to have confidence that they will not be held liable for fraud.

Fraudulent transactions, however, have to be paid for by someone. In the physical environment there are three standard procedures that can protect retailers to some degree:

- the customer's signature can be matched to the signature on the card;

- the card is swiped through an EFTPOS terminal meaning that the card is physically present (evidence of the purchase); and
- an authorisation code is automatically obtained from the customer's financial institution where approval for the purchase means that sufficient funds are available in the customer's account and the card has not been reported as lost or stolen.

These three processes together provide the business with a degree of protection. Fraudulent purchases that arise from this process are generally not considered the responsibility of the retailer (Gibbons 2001).

In the case of online transactions there is no signature and the actual card is not sighted or swiped through a terminal. Generally, all that the customer provides over the internet is the credit card number and expiry date. While an authorisation code may still be sought and obtained by the trader through a web link-up using a bank-operated internet payment authorisation service, this authorisation simply means that the card is still 'active' and has sufficient funds to cover the purchase. It does not confirm the identity of the customer or that the customer is the owner of the card (Westpac 2000).

What happens when online fraud occurs?

Financial institutions are unwilling to accept the additional risks associated with online credit card fraud. This means that the losses associated with fraudulent online purchases are borne by online traders who accept payment for goods online (Gibbons 2001; Lang 1999; Parliament of Victoria 2002). When a cardholder claims that a purchase was fraudulent and not undertaken by them or an authorised party, their financial institution generally takes them at their word and the retailer is required to submit to a chargeback (a refund of the price of the goods from their bank account to the cardholder's) even though they do not receive the goods back in return. The only recourse for online traders who receive a chargeback is to try and pursue the matter privately with the customer – a difficult, costly and time-consuming process.

How widespread is online credit card fraud?

Although some research has been conducted in relation to online credit card fraud against businesses, it is sparse, contradictory and often methodologically flawed. In particular, there are two key pieces of information needed to determine risks or prevalence of online credit card fraud:

- the number of businesses trading online within a particular business type; and
- the number of online traders within that type who have experienced fraud.

There have not yet been any studies internationally or within Australia examining this issue through sampling businesses randomly from a known sampling frame that would allow for reliable estimates to be derived. Figures that have been published may be estimates of the proportion of online transactions which are fraudulent and these are usually provided without an explanation of their source or its reliability (Abru 1999; Attorney-General's Department & OSCA 2000; Shankar & Walker 2001). Other figures may have been derived from empirical sources, but sampling frames and methods vary considerably and few sample randomly from defined populations (Cybersource 2003; Experian 2001).

In summary, sources estimate online credit card fraud at between five and 25 per cent of all internet transactions (Abru 1999; Attorney-General's Department & OSCA 2000; Cybersource 2003). Although risk factors for fraud have not been widely investigated, it has been suggested that since fraudsters are likely to provide incorrect details relating to the name, billing address or delivery address of the cardholder, businesses that do not undertake confirmation of this information are at an increased risk (Experian 2001). Online traders overseas have been surveyed with respect to their fraud prevention efforts and it has been found that 55 per cent of online traders in the UK employ various manual screening techniques (Experian 2001) and 71 per cent confirm address details using the formal address verification service in the United States (Cybersource 2002).

Why do we need to identify the levels of risk of online fraud?

Knowledge relating to the prevalence and risks of online credit card fraud will allow businesses to make informed decisions about whether or not to trade online. Such knowledge can also feed into policy by providing a solid empirical evidence base about how widespread fraud might be, what percentage of online traders are at risk and the potential extent of losses. Without such knowledge it is difficult to determine how much attention and/or funding should be allocated to the prevention of online credit card fraud, or which types of online trader need to be targeted for added protection.

The aims of the empirical study

The central research questions in the present study were:

1. How many (and what proportion) of each type of business currently accept payment for goods over the internet?

2. How many (and what proportion) of online retailers in each business type experienced at least one incident of online credit card fraud during (a) 2002, (b) 2001 and (c) since trading online?

3. What are the financial losses suffered by retailers as a result of online credit card fraud in Australia?
4. How many incidents of online credit card fraud are reported to police in Australia?
5. What factors influence the business to decide to sell goods online?
6. What are some of the risk factors associated with online credit card fraud?
7. How many (and what proportion) of retailers are aware that losses associated with online credit card fraud are borne by online retailers?
8. On average, how long does it take for online credit card fraud victims to be advised of an incident of online fraud?
9. To what extent do retailers employ preventive measures to reduce the likelihood of online credit card fraud and what types of preventive measures do they use?
10. What are retailers' perceptions of online retailing, financial institutions and online credit card fraud?

Section 2: Overview of AIC online credit card fraud survey

There is no centralised register of businesses that currently trade online from which to draw a sample for survey purposes. However it was assumed that if people purchase a particular type of good over the internet more often than other types of goods, then retailers who sell those products may be more likely to trade online. Therefore, five business types that have been identified as more popular with internet shoppers were included (Adey 1999; Shimmin 2000; US Census Bureau 1999). Businesses within each of these types were randomly selected from Australia On Disc (the electronic version of the Yellow Pages directories). The businesses were stratified by the five selected business types (see Appendix 1 for detailed information about the methodology). Only businesses which accepted credit card payments on their own web site were classified in this study as trading online.

The questionnaire was administered over the telephone by a Roy Morgan trained interviewer, using the computer-assisted telephone interviewing technique (CATI). The questionnaire is provided in Appendix 2. At least three call-backs were made to those businesses which could not be contacted, with more if necessary to achieve the required samples. The average length of time to complete the questionnaire was 11 minutes.

In total 1,078 small businesses were interviewed, evenly distributed between the five business types. The overall response rate was 62 per cent. For purposes of better representing the retailers in these five types across Australia, the data were then weighted by business type (see Appendix 1), providing a total number of small businesses in these five business types of 6,657 across Australia.

In this report, weighted data have been used when providing descriptive statistics to indicate estimated frequencies for all retailers in the five business types across Australia (for example, losses, number of incidents and so on). Where statistical analyses are conducted, the effective sample size (weighted data for original sample) has been used to ensure statistical significance has not been inflated. Therefore, in this report:

- weighted data are used to provide descriptive information for the population and this is indicated when numbers are given for retailers 'across Australia'; and
- where tests of significance are calculated (for example, regression analyses), the sample has been weighted for better representativeness, but scaled down to the effective sample size.

Demographics of businesses included in this survey (including sex of the retailer, business size, annual turnover and remoteness of business location) are provided in Appendix 1.

Section 3: Online retailing practices

How many businesses trade online?

Data which are available relating to the number of businesses trading online in Australia have previously been released from three sources:

- the Australian Bureau of Statistics (ABS 2003) estimates that five per cent of all retailers (large and small) in Australia have a facility for buying and selling products over the internet;
- the Yellow Pages (2003) e-business report states that 32 per cent of their small business respondents currently receive payments online; and
- a study by the Australian Centre for Retail Studies (ACRS 1999), which surveyed 1,500 members of the Australian Retailers Association, found that approximately 60 per cent of general and specialty non-food retailers traded over the internet.

These statistics are inconsistent. The reason for this lies in the sampling frames used. The ABS study examined retailers but of a variety of sizes; the Yellow Pages report looked at small businesses but not specifically retailers; and the ACRS study used a convenience sample and did not randomly sample from a defined population (businesses who were members of the Australian Retailers Association were asked to respond to a survey regarding e-commerce and the sample comprised those businesses who returned surveys – the response rate was 19 per cent).

Because of the different sampling frames and methodologies used, it was not possible (based on past research) to identify the proportion of small retailers in Australia who currently accept payment for goods online through their own web site. The present AIC online credit card fraud survey was specifically focused on five types of retailer (who were likely to trade online) and this strategy was aimed at producing solid figures relating to the extent of online trading within particular retail categories.

AIC online credit card fraud survey 2003

It appears that, despite the surge in interest in online retailing in recent years, the vast majority of these types of businesses still sell their products through more traditional means (face-to-face, mail order, telephone order and so on). The number of businesses who indicated that they previously but no longer accepted payment for their products over the internet was small for all categories (one per cent, averaged across all five industries). Overall, 13 per cent of retailers were currently trading online (see Table 1). Booksellers had the highest percentage of businesses currently retailing online (17%) followed closely by recorded music retailers (15%). Florists and toy and game retailers had the lowest proportion of retailers currently accepting payments online (11%), although this figure does not include those florists who may use an external web site such as Interflora (43%).

Table 1: Online trading by business type in Australia (row percentages)

Business type	Currently trading	Previously traded	Never traded	Weighted n
Florists (a)	11	1	88	2,766
Booksellers	17	1	82	1,065
Recorded music retailers	15	3	82	502
Toy and game retailers	11	2	87	645
Computer hardware retailers	13	2	85	1,679
Total	13	2	85	6,657

(a) 43 per cent of florists accept payment through an external web site such as Interflora

Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

Online retailing as primary source of business

Online traders are likely to operate in different ways. Some will operate as 'pure clicks' businesses (retailing solely online), while others may prefer the 'clicks and mortar' variety (retailing online while still maintaining a physical presence in the form of a shopfront). The degree to which small businesses focus on online trading can be determined through (a) the percentage of overall turnover attributed to online trading and (b) whether the business simultaneously operates a shopfront while trading online. This study found that 49 per cent of online retailers estimated that online trading accounted for less than five per cent of their overall turnover. Another 21 per cent estimated that the percentage of turnover was between five and 10 per cent. In all, only three per cent of online traders believed more than 80 per cent of overall turnover was attributed to their internet selling. Moreover, only 17 per cent of online retailers were operating without a shopfront, demonstrating that the majority of proprietors are reluctant to invest their entire operations into non-traditional methods of retailing.

How long had businesses in Australia been trading online?

Retailers slowly gravitated toward selling over the internet in the mid to late nineties in Australia, with online trading continuing to increase into the twenty-first century (see Figure 1). In 2002 fewer online traders reported commencing online trading, however preliminary results for 2003 suggest that the 2002 finding is an exception to the trend. Although the study was only able to measure retailers' commencement in the first quarter of 2003, when this finding is projected to the entire year, we can see that the trend from previous years (excluding 2002) looks like continuing. It was also found that male retailers (M=1999.9, SD=2.2) were more likely to have commenced online trading earlier than

females (M=2001.0, SD=1.6) and that florists (M=2001.0, SD=1.5) were likely to have moved into online trading later than the other four business types (M=2000.0, SD=2.1).

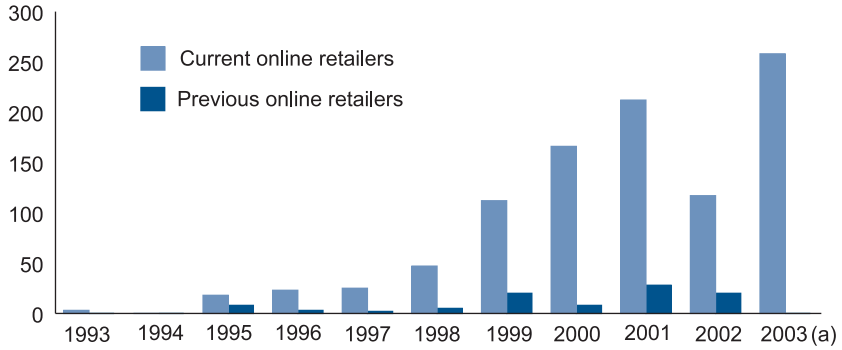
Trading online in the future

Online trading was generally viewed favourably by the majority of retailers, with few differences across business types. When asked how likely it was that their business would stop trading online within the next two years, only five per cent of all online traders indicated this was likely. The vast majority indicated that they were much more likely to continue trading online (93%). To determine potential future activity on the internet, retailers who did not currently accept payments online were asked about the likelihood of their business trading over the internet in the next two years. Overall:

- 39 per cent of retailers stated that it was very likely;
- 38 per cent thought it was somewhat likely;
- 21 per cent thought it unlikely; and
- 2 per cent were unsure.

These findings strongly imply that online trading by these types of business will increase markedly over the next two years. Overall, those who indicated that they were likely to begin retailing on the internet in the following two years were significantly more likely to be

Figure 1: Online trading commencement in Australia



(a) Results projected from 86 retailers who commenced online trading between January and April 2003

Note: Excludes 32 current online traders who could not say when they began trading online

Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

located in a highly accessible or accessible area than a remote area ($p<.05$), were more likely to believe their business was suited to online trading ($p<.001$) and more likely to think customers would use the web site ($p<.001$).

How satisfied are online traders?

In keeping with online traders' likelihood of continuing trading online, the vast majority (89%) were satisfied with accepting payments over the internet. Fewer retailers, however, believed that online trading had significantly increased business sales, with 56 per cent agreeing that their business had increased sales as a result.

Predictors of retailing online

Why is it that two businesses which operate within the same business type may vary in terms of their decision to trade online? Are demographic characteristics such as size or location important? Or are beliefs and perceptions held by the business proprietor about online trading more influential? Those factors which contribute significantly to variability in online trading status were investigated through four logistic regression models, one for each business type aimed at predicting whether or not a business currently traded online.

Predictors varied depending on the type of business. For florists and recorded music retailers, online trading is significantly associated with:

- having more employees; and
- the belief that the costs/time required when trading online are reasonable.

For booksellers, online trading is significantly associated with:

- having more employees;
- being located in highly accessible areas;
- the belief that customers do/would use the web site frequently to place orders;
- the belief that benefits of trading online outweigh the risk of fraud; and
- the belief that the costs/time required when trading online are reasonable.

For toy and game retailers, online trading is significantly associated with:

- the belief that benefits of trading online outweigh the risk of fraud; and
- the belief that the costs/time required when trading online are reasonable.

Finally, for computer hardware retailers, online trading is significantly associated with:

- the belief that the business is suited to selling products over the internet; and
- the belief that the benefits of trading online outweigh the risk of fraud.

These findings indicate that perceptions of and beliefs about online trading are important determinants of whether or not a business chooses to trade online.

Section 4: Fraud prevention

Electronic fraud prevention

The most basic technique of fraud prevention is electronic authorisation. This process involves verifying that the credit card being used to purchase goods is valid and has sufficient funds attached to it. Given that there are significant limitations associated with this process, specifically that it provides no assurance that the person using the card is authorised to make the purchase, technology is rapidly developing to provide retailers with added protection.

For credit card transactions conducted in person, a system involving microchips and personal identification numbers (PINs) is currently being developed in the United Kingdom. This has involved a microchip being added to credit cards to store data securely, and a PIN being used rather than a signature at the point of sale (APACS 2003). This procedure requires traders to install special terminals to accommodate the new chip and PIN. A recent UK trial of the system was successful. Countries around the world are creating chip cards to meet an international specification originally devised by the card issuers Europay, MasterCard and Visa (known collectively as EMV). It is anticipated that all of the UK's credit, debit and charge cards will be reissued with chip and PIN capability by 2005. The potential reduction in over-the-counter credit card fraud should be substantial.

For credit card transactions conducted over the internet, however, the problems of card and cardholder authentication still remain. Chip and PIN cards have the potential at some point in the future to provide more secure transaction technology through the use of chip readers and PIN pads attached to computers, however at this early stage, their application is limited. In the UK and USA, two additional online fraud prevention strategies have been developed in partnership with financial institutions and card issuers:

- an address verification service (AVS); and
- a card verification number (CVN).

The AVS is obtained through the cardholder's issuing financial institution, whereby numerical details of the address provided in the online order are cross-checked. While this service is not foolproof (for example, if the cardholder has moved but the financial institution's records have not been updated), it is nevertheless a tool which traders can use to determine their risks of proceeding with the order. A formalised AVS is not currently available for cards issued within Australia (Turpen 2003).

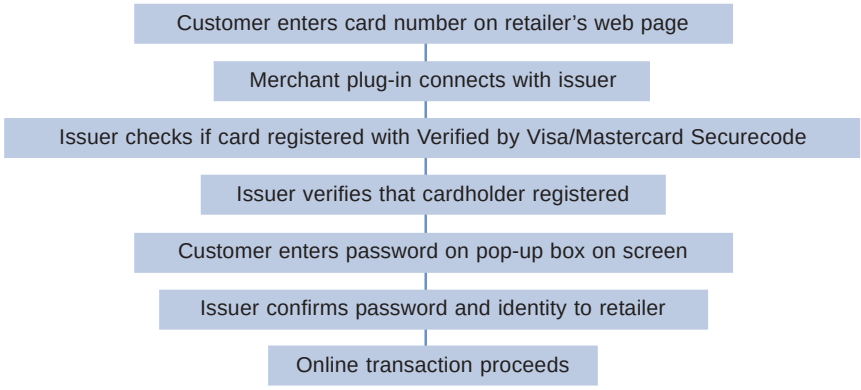
Similarly, online traders can request that the customer enter the CVN, usually a three- or four-digit number printed on the back of most credit cards. Again, while this does not necessarily prevent fraud, it presumably reduces the likelihood of fraud occurring since it

is an additional piece of information which is available only from viewing the card itself and cannot be obtained from items such as discarded receipts. For this reason Australian online traders may ask customers to provide this number (St George Bank 2003), however, the extent to which it is verified with card issuers is unclear. A US survey of online traders found that 75 per cent used the AVS, while 44 per cent used the CVN (Cybersource 2003), however the degree to which these measures prevent fraud has not been assessed.

A third option currently available in Australia is payer authentication offered through both Mastercard ('Mastercard Securecode') and Visa ('Verified by VISA'). These are password-based programs which allow registered cardholders to verify their purchases by entering a password in a pop-up box on the computer screen when an online purchase is being made. Again, however, this requires cardholders to register for the program with participating card issuers and it also requires businesses to be registered and to have a Verified by Visa or Mastercard Securecode merchant plug-in installed on their processor. The procedure of transactions using Verified by Visa or Mastercard Securecode is displayed in Figure 2.

The benefits of Verified by Visa or Mastercard Securecode for online traders are primarily that internet credit card transactions become considerably safer as the credit card purchase will be authorised only if the customer knows the correct password. This makes it much more likely that the person making the purchase is in fact the genuine cardholder.

Figure 2: Procedure of transactions involving Verified by Visa or Mastercard Securecode



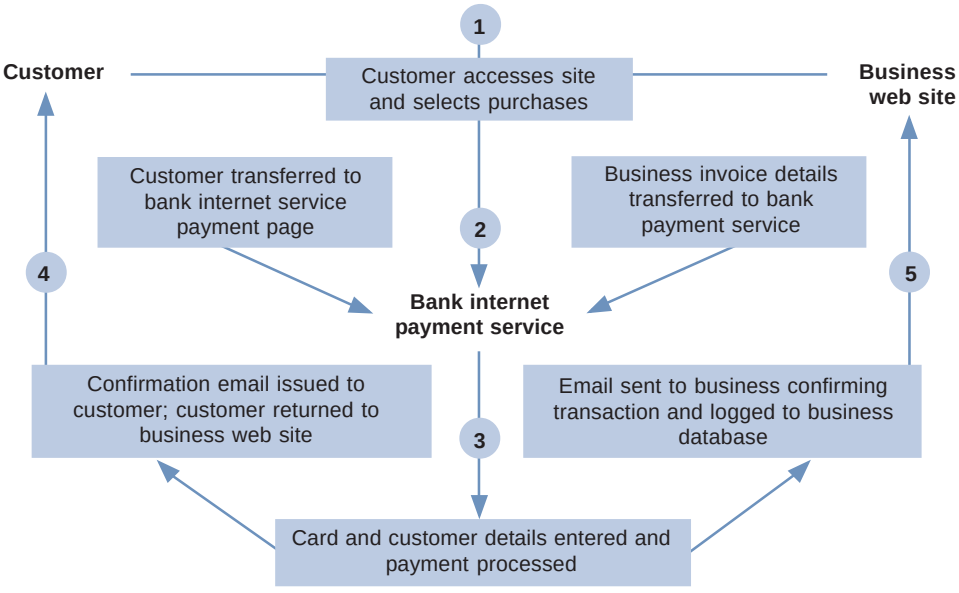
Source: Visa (2004); Westpac (2003)

Further, online traders who participate in these programs are protected to a greater degree against fraudulent chargebacks. Whereas retailers using basic electronic authorisation procedures are liable for the full amount, since April 2003 those using Verified by Visa are no longer liable for chargebacks arising from fraudulent transactions (ANZ Bank 2003). Visa believes that up to 80 per cent of online chargebacks and fraud will be eliminated through this system. Implementation of the system is in its early stages, as it requires participation by both cardholders and businesses, however its future potential if optimised is presumably large.

The use of electronic authorisation

Currently in Australia there are several ways that retailers can authorise a credit card payment for an online purchase. One way is to use a web link to a bank-operated internet payment service (AIIA 1999). This is where credit card details are entered onto the web site of the business and the details of the purchase are automatically submitted for bank authorisation. The authorisation is almost instantaneous and, if approved, the customer receives an approval notice while they are still waiting. Figure 3 illustrates the processes involved in a bank-operated internet payment authorisation service.

Figure 3: Processes involved in bank-operated internet payment authorisation service



Source: Adapted from National Australia Bank (2002a)

Alternative methods of electronic authorisation are where the credit card details are entered onto the retailer's web site and staff later enter them into an EFTPOS terminal, or where the retailer contacts the bank or a merchant authorisation service to obtain authorisation for the credit card purchase. In all three methods (web site link, EFTPOS check and phone call to bank) the electronic authorisation verifies that the card used to make the purchase has sufficient funds and has not been stolen – it does not verify that the customer is the genuine cardholder. All three methods also involve three parties:

- the retailer (who requests the initial authorisation and receives the final approval or decline);
- the retailer's financial institution (the mediator between the retailer and the cardholder's financial institution); and
- the cardholder's financial institution (who provides the authorisation) (Retail Decisions 2001).

However, there are also likely to be instances where some online traders may simply take the credit card details for the purchase at face value and not seek bank authorisation. This latter scenario could clearly put traders at greater risk of fraud and may reflect a lack of knowledge as to the potential risks involved with such a strategy. Identifying the proportion of online traders who fall into this latter category would assist in identifying fraud prevention strategies. This could include developing information kits to make available to all online traders.

Online traders were asked whether they had web-based systems in place which would provide real-time authorisation while the customer waited online and, if not, how often they manually processed electronic authorisations (either by using an EFTPOS terminal or telephoning the relevant authority). It was found that:

- 25 per cent used a system which automatically requested authorisation through the various parties (cardholder's financial institution, credit card company and so on) while the customer waited online;
- 63 per cent always manually processed electronic authorisation prior to dispatching goods;
- 4 per cent manually processed electronic authorisation some or most of the time; and
- 8 per cent never used electronic authorisation.

Manual fraud prevention

In lieu of more technologically advanced prevention techniques, Australian online traders are usually provided with numerous suggestions for fraud prevention strategies by their financial institution, which are intended to reduce the risk of businesses accepting fraudulent online transactions (National Australia Bank 2002b; Westpac 2000). These suggestions usually centre on manually screening orders prior to sending the goods in addition to obtaining electronic authorisation. Retailers are told of possible 'warning signs' which may indicate a customer who is not genuine, such as an overseas mailing address or a postal box address instead of a physical address. Retailers are also warned about:

- orders comprising duplicate items (they may be sold on);
- orders placed on a rush or with immediate delivery (fraudsters are not concerned with delivery costs and want the items quickly);
- cards that have been used previously and found to be fraudulent; and
- customers who provide an email address from a free email service (Tomlinson 2002).

In addition to being wary when these 'warning signs' appear on an order, online traders are advised to:

- verify the order with the customer by telephone or email;
- confirm the address with the financial institution or recent telephone directory;
- establish a database which records good and bad customers (to ensure speedy approval and no unnecessary screening); and
- request information from the customer which only the cardholder would know (address, digits on back of card, bank who offers the card, and so on).

The use of fraud prevention strategies by businesses (prior research)

Although there are clearly numerous methods recommended to Australian traders to prevent online credit card fraud, it is important to know the degree to which they are employed in day-to-day processing. This would help to establish whether additional strategies need to be developed or existing ones implemented. Further, it is important to know *why* businesses do not use particular strategies. This latter point is yet to be investigated.

The Cybersource survey from the United States (2003) found that 65 per cent of online traders manually screened orders, with each retailer reviewing an average 23 per cent of orders placed on their web site. The study reported that the manual review techniques employed (in order of common use) were:

- phoning the customer (78%);
- checking customer records (64%);
- emailing the customer (61%);
- phoning the bank (58%); or
- checking a 'bad customer' database (40%).

In the UK it was similarly reported that 55 per cent of the sample employed manual fraud detection systems and 15 per cent had automated systems for fraud detection (Experian 2001). To date, there have been no surveys published examining the use of these strategies in Australia, hence the importance of probing these issues in the present study.

The use of manual screening

In the current AIC online fraud survey, online traders were asked about the manual techniques they employed to prevent themselves becoming victims of credit card fraud. Specific methods were identified beforehand; often these were recommended in literature provided by financial institutions (National Australia Bank 2002b, Westpac 2000), or in other sources (Internet Scambusters 1998). Some methods were more popular among business proprietors than others (see Table 2), with the most common method used being

Table 2: Use of manual fraud prevention methods by online traders in Australia (row percentages)

Prevention method	Never	Rarely	Sometimes	Mostly	Always	n (a)
Phone/email the customer to confirm order	9	8	22	6	55	838
Check customer details in phone directory	52	17	14	5	12	830
Keep database of good and bad customers	34	13	9	3	41	835
Reject suspicious orders	32	17	16	5	30	806

(a) n varies due to missing cases

Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

to phone or email the customer prior to delivering the goods. While half the traders always undertook to phone or email the customer post-purchase to confirm the order, only 12 per cent consistently checked customer address details in the telephone directory.

Reasons for infrequent manual screening

Why do some online traders never or rarely manually screen orders, particularly as these fraud prevention measures are often advised by financial institutions? For three of the four preventive methods given (all except confirming details in the telephone directory), the most common reason was that they had rarely or never experienced problems with credit card fraud online and therefore felt little need to employ such strategies. This strongly implies that prevention strategies are applied *after* fraud has been experienced, rather than as a pre-emptive measure.

Of those who never or rarely confirmed customer details in the telephone directory, the most common reason was that the international orders which they processed made checking details difficult or impossible. This is important because international orders have been identified as being particularly at risk of involving fraudulent activity (Internet Scambusters 1998; National Australia Bank 2002b). In the Cybersource 2003 survey, for example, less than one per cent of US/Canadian domestic online orders were fraudulent compared with 3.2 per cent of orders emanating from outside the US/Canada.

Predictors of manual screening use

In addition to examining the reasons given above for businesses not employing particular methods, the predictors for whether businesses consistently use fraud prevention measures[1] can also be evaluated more systematically using logistic regression. This model evaluated the importance of both demographic and attitudinal variables and found that:

- experiencing fraud is a significant predictor of phoning/emailing the customer and rejecting suspicious orders, supporting the above implication that traders implement more stringent prevention methods following a fraud episode; and
- male retailers were less likely than females to keep a database of good and bad customers.

1 This was measured by whether the online trader used the particular measure 'most of the time' or 'always' (0=no, 1=yes).

Section 5: Experience of online credit card fraud

Online credit card fraud has previously been estimated at between five and 25 per cent of all internet transactions. This is higher than has been found in the physical domain, where fraudulent transactions normally constitute approximately one per cent of sales (Abru 1999; Attorney-General's Department & OSCA 2000). It has also been argued that businesses have seen credit card fraud occurring 10 times more often online than in the physical environment (Tomlinson 2002). Other reports have suggested a lower level of victimisation overseas. For example, chargebacks (the refund of the amount of goods which retailers have to forfeit in the event of online credit card fraud) have been said to account for approximately three per cent of online purchases in the US (Shankar & Walker 2001).

Other surveys of businesses overseas regarding online credit card fraud have also reported the following findings:

- approximately 70 per cent of businesses in a UK survey reported that less than five per cent of their transactions were fraudulent (Experian 2001); and
- on average, three per cent of US online orders were fraudulent in 2002 (Cybersource 2002) with only one per cent being fraudulent in 2003 (Cybersource 2003).

Unfortunately, the data are patchy and none of these sources report on the percentage of online retailers who have experienced online fraud, either at all or in a given time period.

Fraud victimisation

One of the most important questions included in the AIC online credit card fraud survey referred to the experiences of both current and previous online retailers with respect to online credit card fraud. Of retailers within the five business types currently trading online, the following had experienced at least one incident of online credit card fraud since trading online:

- 28 per cent of florists;
- 43 per cent of booksellers;
- 26 per cent of recorded music retailers;
- 33 per cent of toy and game retailers;
- 30 per cent of computer hardware retailers.

Overall one-third of all retailers who had ever sold products online have been the victim of online fraud at some stage. Table 3 shows the estimated number of online traders across Australia and fraud prevalence rates.

Table 3: Number and percent of victims of online credit card fraud by business type in Australia

Business type	Currently trading online		Previously traded online	
	n	% victims	n	% victims
Florists	296	28	24	0
Book sellers	181	43	15	33
Recorded music retailers	77	26	15	17
Toy and game retailers	72	33	9	100
Computer hardware retailers	215	30	32	50
Total	841	32	95	34

Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

In addition to lifetime prevalence, online traders were also asked whether they had experienced online credit card fraud in 2001 and/or 2002. Prevalence varied by business type as follows:

- 16 per cent of florists experienced fraud in 2001 and 12 per cent in 2002;
- 22 per cent of booksellers in 2001 and 2002;
- 19 per cent of recorded music retailers in 2001 and 13 per cent in 2002;
- 25 per cent of toy and game retailers in 2001 and 17 per cent in 2002; and
- 15 per cent of computer hardware retailers in 2001 and 2002.

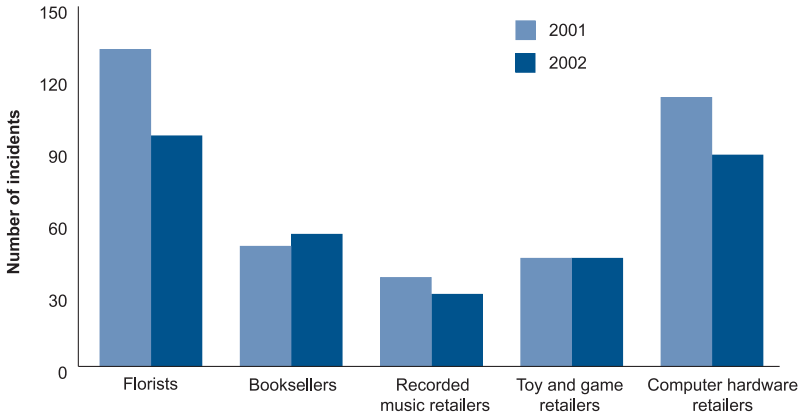
Incidents in 2001 and 2002

The number of incidents estimated to have been experienced by current online traders in 2001 and 2002 in Australia is given in Figure 4. Across Australia, florists and computer hardware retailers show the highest number of incidents (of the five retail categories) in total in both 2001 and 2002. It is also apparent that the total number of incidents reduced slightly in 2002 compared to 2001.

Repeat victimisation

Repeat victimisation is a well-known phenomenon in criminological research; it refers to the hypothesis that those persons who experience one incident of a particular crime are at a greater risk of being victimised again than those who have not been victimised (Farrell 1995; Taylor & Mayhew 2002).

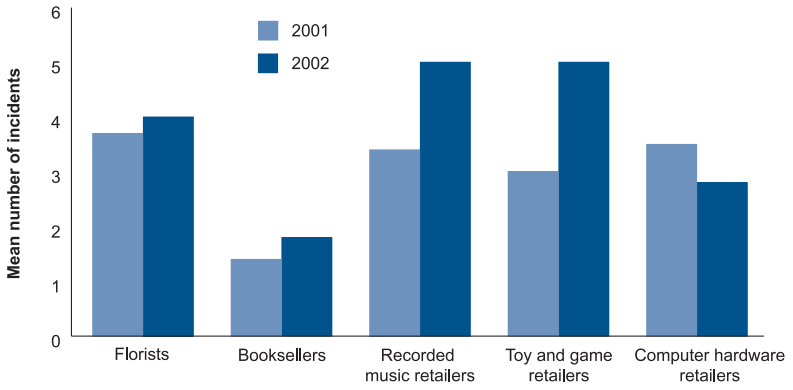
Figure 4: Number of incidents experienced in Australia in 2001 and 2002



Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

The present study found that of all online traders who had ever experienced online credit card fraud, 51 per cent had experienced more than one incident over 2001 and 2002. Overall, 18 per cent of victims accounted for 38 per cent of all incidents. Repeat victimisation also varied across business type, with recorded music retailers and toy and game retailers indicating a higher mean number of incidents per victim in 2002 than the other business types, and booksellers indicating an average of less than two incidents per victim in 2001 and 2002 (see Figure 5).

Figure 5: Mean number of incidents per victim in Australia in 2001 and 2002



Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

Table 4: Logistic regression predicting online credit card fraud risk

Variable	Odds ratio	95% CI (lower)	95% CI (upper)
Demographic variables			
Number of employees	1.01	0.87	1.15
>10% turnover attributed to online trading (0=no, 1=yes) (a)	19.42*	17.93	20.90
Number of locations	1.15	0.42	1.88
Sex (female=0, male=1)	6.34*	5.12	7.56
Months trading online (b)	1.01	0.99	1.03
Florist (versus computer retailers)	7.88*	6.28	9.47
Bookseller (versus computer retailers)	9.77*	8.18	11.37
Recorded music retailer (versus computer retailers)	3.18	1.34	5.02
Toy and game retailer (versus computer retailers)	1.51	–0.42	3.44
Behavioural variable (c)			
Degree to which retailer authorises transactions electronically	1.23	0.74	1.72
Attitudinal variables (d)			
Having staff manually check internet orders for fraud impacts on business productivity.	1.70*	1.22	2.19
Confirming legitimate internet orders hurts customer relations	1.04	0.61	1.46
Nagelkerke R Square	0.42		
N	129		

CI = confidence interval

(a) This variable was originally coded as an ordinal variable with 11 response categories for percentage turnover attributed to online trading; to make the variable conducive to calculating risk, it was recoded as dichotomous

(b) Square root transformation was performed on this variable to normalise the distribution, however this made no difference to the model

(c) Behavioural variable measured on a scale of 1 to 5, 1=never and 5=always

(d) Attitudinal variables measured on a scale of 1 to 5, 1=strongly disagree and 5=strongly agree

* Statistically significant to p<=.05

Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

Predictors of victimisation

Why do some businesses experience fraud and others do not? This question was examined in a logistic regression model (see Table 4). It should be noted that as the experience of fraud predicts the use of fraud prevention measures rather than the other way around (prevention measures tend to be implemented after fraud has occurred), the use of fraud prevention measures are not entered as a predictor in this model.[2]

2 In business surveys which cover a particular time period it is common to find that prevention predicts crime and not vice versa. This does not mean that prevention measures are not useful in preventing crime. Rather, such findings reflect the fact that survey periods do not allow for crime measurement *after* prevention is implemented. Experimental studies are better at evaluating effectiveness of fraud prevention measures than surveys.

Table 5: Coefficients for risk victimisation model

Variable	Coefficient	Standard error	Odds ratio
Sex of retailer (male)	1.85	0.62	6.34
Bookseller	2.28	0.81	9.77
>10% of turnover attributed to online trading	2.97	0.76	19.42
Believes manual checking impacts negatively	0.53	0.25	1.70
Constant	–7.06		

Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

Online credit card fraud was more likely to have ever been experienced by:

- businesses that attributed a higher percentage of annual turnover to online trading – higher online turnover presumably reflects greater opportunity for fraud;
- male proprietors; and
- retailers who believed that staff manually checking orders reduced productivity.

Risk of victimisation for each business type

Levels of risk of fraud for individual retail businesses will vary depending on the individual characteristics of the business. Based on the coefficients provided in Table 5, levels of risk of online credit card fraud can be calculated for retailers depending on their ratings on various risk factors (see Figure 6). Clearly, a combination of factors produces increased risk, with male booksellers at considerably more risk of fraud when combined with other factors such as the belief that manual checking has a negative impact on productivity and the business attributing more than 10 per cent of their turnover to online trading.

Estimating online credit card fraud risk

Estimated probability of online fraud = $1/1 + e^{-(\text{constant} + \text{coefficient} + \text{coefficient})}$

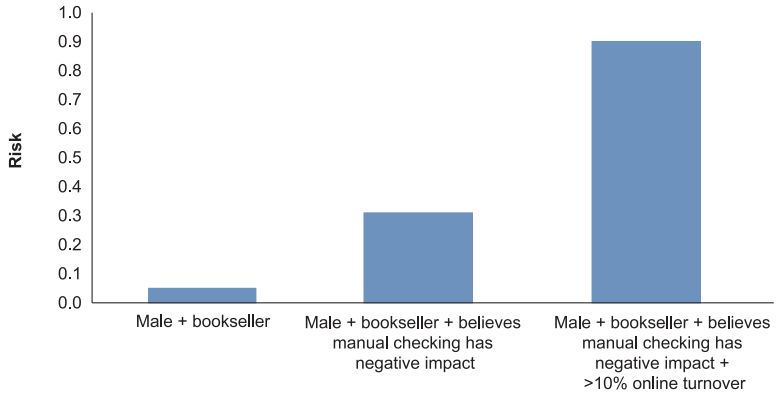
Example

Estimated probability of fraud for male bookseller who believes (rating of 4 on a 1–5 scale) manual checking has a negative impact on business productivity

$= 1/1 + e^{-(-7.06 + 1.85 + 2.28 + 4(0.53))}$

$= 0.31$

Figure 6: Probability of experiencing online credit card fraud



Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

Beliefs about fraud prevalence

Thirty-three per cent of retailers who were currently selling goods online, or had ever done so, had experienced credit card fraud at some stage. Nonetheless, when asked about their perceptions of the extent of online credit card fraud in general, approximately half agreed that it was very common.

Online traders also commented on how their experience of fraud compared with the expectations they had prior to commencing online trading:

- 56 per cent stated that the level of credit card fraud they had experienced since retailing online was lower than they had expected;
- 32 per cent believed that the fraud they had experienced was equal to what they had expected;
- 6 per cent believed the fraud they had experienced was higher than their initial expectations; and
- 6 per cent were unable to comment.

Reporting online credit card fraud to police

The degree of under-reporting of crime to police by small retail businesses has been a focus of research in recent years (Fisher & Looye 2000; Taylor 2003). A senior detective in the area of computer crime was recently quoted as saying that many traders simply

'soak up' the costs of fraud and do not consider it important or useful to report the crime to police (Kennedy 2000). A UK study found that 57 per cent of businesses had reported online credit card fraud incidents to police (Experian 2001).

In the AIC online credit card fraud survey, those retailers who indicated that they had experienced online credit card fraud during either 2001 and/or 2002 were asked how many incidents they had reported to the police. It was found that:

- 35 per cent of incidents were reported to police in Australia in 2001; and
- 21 per cent of incidents were reported in 2002.

These numbers for reporting online credit card fraud appear to be consistent with the low levels of reporting found in previous research. It is clear that retailers are not yet reporting on a regular basis to police and this is of concern, given that police and other authorities will not be made aware of the nature and extent of the problem if incidents are rarely reported officially.

Section 6: Losses associated with online credit card fraud

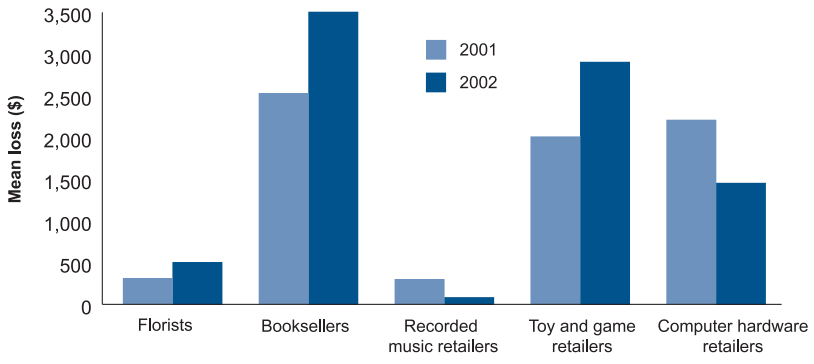
Losses from fraud

Establishing the losses associated specifically with online credit card fraud is difficult. In the UK, losses associated with card-not-present frauds (remembering that these also include telephone, mail and fax orders and other situations in which a fraud may occur in the absence of a card) amounted to £116.4 million in 2003 (APACS 2004), an increase of six per cent on 2002's losses. Cybersource's Online Fraud Report (2002) stated that online credit card fraud amounted to approximately three per cent of overall revenue for businesses in the United States.

It is unclear exactly how much is lost to online credit card fraud each year in Australia (Kennedy 2000). In relation to previously released figures, a 2001 police article quoted the National Australia Bank as reporting its business customers lost $700,000 in the final quarter of 1999 as a result of this crime (Gibbons 2001). The South Australian police have estimated that online credit card fraud cost South Australian businesses as much as $250,000 in a two-month period (SA Police 2000). However, police figures (like that given for SA) include all businesses and not just small retailers, resulting in figures which are likely to be heavily influenced by the high turnover of larger businesses.

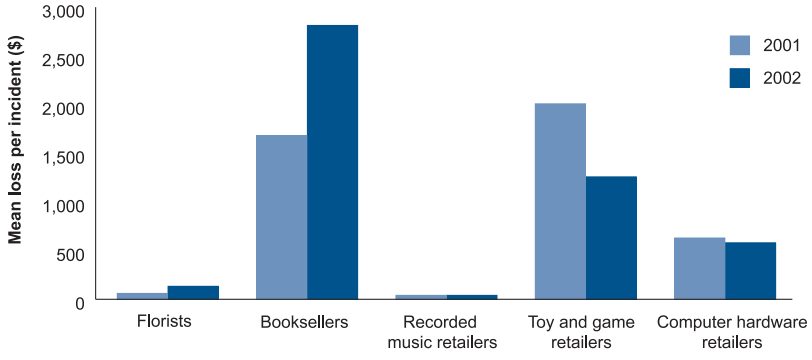
The AIC online fraud survey found that losses varied by business type, and that mean losses for victims who experienced a loss were considerable, particularly for booksellers, toy and game retailers, and computer retailers (see Figure 7). Mean losses per incident were also significant for particular retailers (see Figure 8). Since the annual turnover for

Figure 7: Mean loss (per victim that experienced a financial loss) in Australia in 2001 and 2002



Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

Figure 8: Mean loss per incident in Australia in 2001 and 2002



Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

these small retailers can be relatively small (approximately 60 per cent of online traders reported an annual turnover of less than $500,000), it is likely that these losses impacted considerably on those businesses affected.

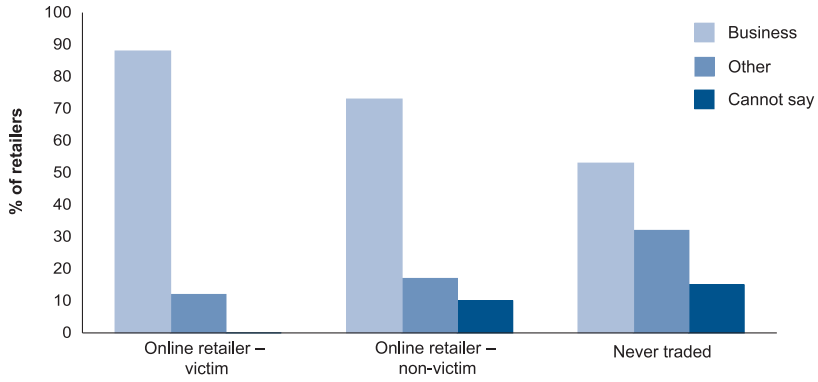
Beliefs about financial liability

In recent times, proprietors have complained that they were not aware of their potential liability for online credit card fraud prior to receiving a chargeback from their financial institution and subsequently being expected to bear the costs associated with the incident (Levy 2002). In order to assess how common this lack of awareness might be among businesses in Australia, all retailers were asked who they believed bore the primary financial responsibility for online credit card fraud (see Figure 9). It can be seen that:

- 88 per cent of online credit card fraud victims were aware that a business bears the primary responsibility for financial costs for online fraud;
- 73 per cent of non-victim online retailers were aware of this liability; and
- only 53 per cent of proprietors who had never sold goods online were aware of this liability.

Although it is clear that the majority of online retailers in Australia (particularly those who have experienced fraud in the past) are aware of their potential liability, some still remain unaware. Also, given that almost half of the sample of non-online traders were unaware of a business's liability with respect to fraud, and given that a large number of these indicated

Figure 9: Perceptions in Australia of liability from online credit card fraud



Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted data]

that it is likely they will soon move to online trading, there is clearly a need to ensure that straightforward information about liability for online credit card fraud is disseminated widely and read by prospective traders.

How did businesses find out about the fraud?

Businesses who provided details of a specific incident of online credit card fraud were asked how they had discovered the fraud; were they advised by their financial institution or another party, or did they discover it themselves? It was found that:

- 91 per cent of businesses were advised of the fraud by their financial institution;
- 6 per cent had discovered the fraud themselves; and
- 3 per cent were advised by another party (for example, the cardholder).

How long did it take for businesses to be notified of the fraud?

The length of time taken to identify that fraud has occurred and, more importantly, the time that has lapsed before the retailer is informed of the chargeback can have important implications for business losses. When the delays are lengthy, the retailer may have processed additional orders on the same card, resulting in a greater number of fraudulent transactions. A recent newspaper article (Kennedy 2000) highlighted this by citing anecdotal accounts of traders who had experienced extensive delays in notification and in some

cases had processed additional orders, resulting in multiple chargebacks. Wales (2003: 10) also indicated a problem with notification delays in the United States, stating 'sometimes chargebacks are not issued for weeks, if not months after the retailer has sent the goods out.'

In the AIC survey, delays in notification were found to be lengthy with:

- 10 per cent of online fraud victims notified within a month of the incident;
- 42 per cent notified between one and two months after the incident; and
- 48 per cent notified two months or more after the incident.

It is understandable that notification can take time, given that in most cases the cardholder is responsible for notifying their financial institution and (especially in the case where a card is not stolen) the cardholder may not become aware of the fraudulent transaction until they receive their monthly statement or check their account through other means. However, this delay can have significant implications for a business victim, given that retailers may continue processing transactions on a card number unless they are advised otherwise. It is not uncommon for retailers to be defrauded more than once using the same card number, which makes delays in notification crucial.

Section 7: Perceptions of financial institutions

If businesses only become aware of their liability for online fraud after experiencing such fraud, and if the delays in notification of the fraud are substantial, how does this affect attitudes of business retailers toward their financial institutions? Perceptions of financial institutions were investigated (see Table 6) and key findings were that:

- approximately half of online retailers (44%) believed their bank to be helpful when they had a query about accepting payments online while 30 per cent did not;
- 56 per cent of online traders felt that the information provided about online trading was easily interpreted while 28 per cent did not;
- in relation to general dealings (not just online trading), 58 per cent of all businesses believed their bank had been helpful and supportive in general while 30 per cent did not; and
- only 13 per cent agreed with the statement, 'Banks care about the losses of small businesses from credit card fraud over the internet.'

The predictors of whether retailers believed their bank was 'supportive and helpful' were found, through a multiple regression analysis, to centre on proprietors' own experience of

Table 6: Retailers' perceptions of banks (row percentages)

Statement (a)	Agree	Neither agree nor disagree	Disagree	Can't say	n
The bank is helpful whenever my business has a query about our internet payment systems (b)	44	18	30	8	144
The information provided by the bank in relation to accepting payments over the internet is easy to understand (b)	56	10	28	6	144
In general we have found our bank to be supportive and helpful in our dealings with them	58	9	30	3	1,078
Banks care about the losses of small businesses from credit card fraud over the internet	13	6	67	14	1,078

(a) Statements were measured using scale 1 to 5, 1=strongly disagree and 5=strongly agree

(b) Only those businesses trading online provided responses to this statement

Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, unweighted data]

online credit card fraud and their understanding of the financial consequences of a fraud incident. In sum, negative attitudes were significantly associated with:

- being male;
- being an online fraud victim; and
- believing that the business victim was responsible for the costs associated with fraud.

Online traders who had not experienced fraud did not differ in terms of their attitudes toward financial institutions from retailers who did not trade online, strongly confirming that it is indeed the experience of fraud which leads to negative attitudes through victims becoming aware of their liability for the fraud. An implication from these findings is that it would benefit financial institutions to clearly convey information to online traders about both their liability in the event of fraud and appropriate fraud prevention measures *before* they commence trading online.

Section 8: Conclusions

This study was the first of its kind in Australia to examine online credit card fraud and online trading in the context of different business types. The research presented here demonstrates that the numbers of small businesses which trade online and the prevalence of online credit card fraud does vary by business type, with:

- 11 per cent of florists trading online (through their own web site);
- 17 per cent of booksellers trading online;
- 15 per cent of recorded music retailers trading online;
- 11 per cent of toy and game retailers trading online;
- 13 per cent of computer hardware small retailers trading online; and
- between 26 and 43 per cent of online businesses having been a victim of fraud.

Regarding the financial consequences of fraud, mean losses per incident and per victim can be substantial. Since businesses may experience more than one incident, it is possible that the losses incurred as a result of particular incidents may add up and impact significantly on a particular business.

It is important that businesses be made aware of the risks of fraud, as well as their liability for incidents of online credit card fraud. This study found that businesses who did not trade online, or had not experienced fraud were often unaware of their liability. While online traders can sometimes recoup the losses associated with fraud through pursuing customers themselves, this can be difficult, expensive and time-consuming. The lack of awareness that online traders are themselves liable for fraud losses is concerning given the large number potentially moving to online trading in the next few years.

While online traders were mostly satisfied with the assistance provided by their financial institutions, the additional finding that fraud impacts negatively on retailers' perceptions of financial institutions suggests that it would be in the interests of financial institutions to actively promote the use of fraud prevention strategies by online traders and to ensure that the information which they provide in relation to online trading is clearly explained to traders.

It was also apparent that there can be significant delays prior to victims becoming aware that a fraud incident has occurred. While some delay in this process is inevitable given that the genuine cardholder in most instances must become aware of the fraud before they can report it to their financial institution, there is a need to try and improve the notification process so that any delay is as minimal as possible. The negative consequences of delays can be substantial as traders may in the interim continue to process multiple purchases on the fraudulently used credit card details if they are unaware of the risk.

However, despite the risk of online credit card fraud and the potential consequences of a fraud incident, overall online traders were largely satisfied with retailing online. Only five per cent indicated that they were likely to discontinue online trading in the future. Half believed that trading online had significantly increased sales in their business. It was also established that approximately 40 per cent of businesses that are currently not online are very likely to commence online trading within the next two years. This represents a potentially large influx of online traders within the next two years and suggests that retailers are steadily increasing their activity on the internet.

This study has presented an empirical investigation of the nature and extent of online credit card fraud within particular types of small business in Australia. It is clear that the nature, extent and risk of fraud varies between business types and that future research into online credit card fraud against business should take such variation into consideration. The findings from this study should be regarded as contributing to the evidence base relating to online credit card fraud against small businesses and a potential platform from which new research directions can be developed.

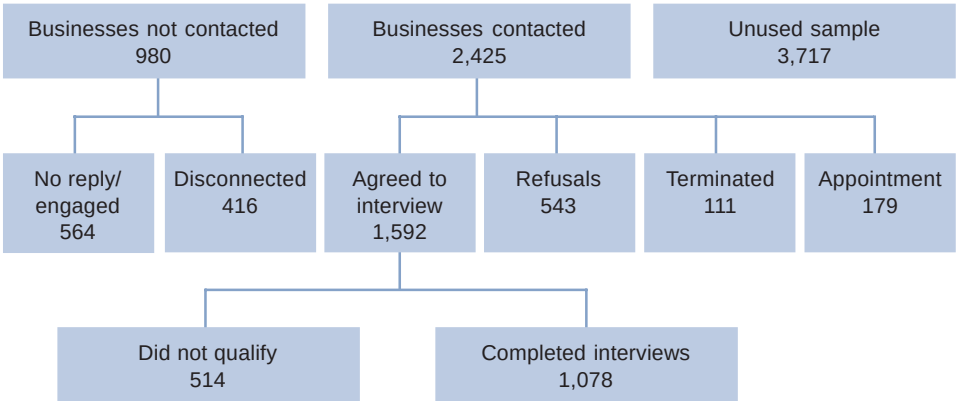
Appendix 1: Methodology

Sampling process

The sampling technique involved a random sampling method, stratified by business type. Five samples (one for each of the five business types) were drawn from Australia On Disc[3] (the electronic version of the Yellow Pages telephone directories), using the appropriate ANZSIC (Australia and New Zealand Standard Industry Classification; see ABS 1993) code or category of retailer. From these five files, retailers were drawn at random until the target quotas of 200 businesses for each business type were met.[4] The total number of completed interviews conducted was 1,078.

The survey was conducted by Roy Morgan Research, using computer-assisted telephone interviewing (CATI). Once businesses had been selected at random and contacted by telephone, they were asked two screening questions to ascertain whether they were 'out-of-scope' for the purposes of this study and should be screened out. These were (a) whether they were a retailer of the given business type, and (b) whether they employed fewer than 20 full-time personnel. The sample needed to include only retailers of the type in question, with fewer than 20 employees. However, only four per cent of businesses contacted were out of scope due to employee size, indicating that most businesses within the five business types are small businesses.

Figure A1-1: Flow chart of sample selection



Source: Roy Morgan Research, Online credit card fraud against small business: technical report (2003), unpublished

3 It is acknowledged that this sampling frame is not necessarily representative of every business that operates in each category, as the sampling frame is unlikely to include businesses which operate solely over the internet and/or are not registered on Australia On Disc. It was not possible to obtain a sampling frame for businesses operating solely on the internet. The findings are generalisable only to those businesses included in the sampling frame.

4 Although quotas of 200 per business type were set, 78 additional random interviews were conducted due to additional time permitting.

It should also be noted that since the survey was interested in online credit card fraud incidents, and it was important that the interviewee was familiar with the business' online trading practices and would know detailed information about each fraud incident, only those businesses which operated their own trading web site were classified in this study as trading online. This meant that some florists which used an external web site operated by an external company (examples include www.interflora.com.au and www.flowers.com.au) but did not operate their own separate trading web site were not classified in this report as being online (but were still interviewed). Forty-three per cent of the florists stated they accepted payments for goods sold through a web site operated by an external business. Figure A1-1 shows the original sample and outcomes to completed interviews.

Instrument

The questionnaire was administered over the telephone by a Roy Morgan trained interviewer, using the CATI technique. This was chosen as it was essential the questionnaire be interviewer-administered (the complexity and various filters and screens required computerised expertise). The telephone is both a convenient and anonymous medium for both the interviewer and interviewee.

The questionnaire incorporated a number of different sections, each of which was answered by retailers depending on whether they:

- currently traded online and had experienced fraud;
- currently traded online and had never experienced fraud;
- previously traded online; and
- never traded online.

The questionnaire is provided for reference in Appendix 2.

Piloting of survey

Prior to the survey going into the field, a pilot survey was undertaken to assess likely response rates, possible incidence rates of online trading and fraud, the utility of the questionnaire (its ability to attain useful responses), and whether retailers would have difficulty with certain questions. The pilot included 104 completed interviews (20 florists, booksellers and computer hardware retailers, 21 recorded music retailers and 23 toy and game retailers). Some minor alterations were made to the questionnaire based on the pilot phase. AIC ethics approval for the full research project was received on 18 March 2003 and the questionnaire was also approved by the Commonwealth Statistical Clearing House on 16 April 2003 after which data collection commenced.

Main data collection and response rates

Roy Morgan Research interviewers, with extensive training in social research surveys and procedures, conducted the interviews. Final data collection began on 15 May 2003 and continued until 6 June 2003. Ten interviewers worked concurrently, during as well as outside business hours (to suit the preferences of interviewees). Response rates varied little across business type, with an overall response rate for the entire sample of 62 per cent (business type response rates varied between 60% and 64%).

Sample demographics

Table A1-1 provides demographic details of the unweighted sample: the sex, size and location of businesses in each of the five types and across the entire sample. Sex varied across business type, with florists more likely to be female and computer retailers more likely to be male. Business size was largely micro, with 86 per cent of the whole sample employing fewer than five full-time staff.

Table A1-1 also provides details relating to the ARIA (accessibility/remoteness index of Australia) classification of the sample. ARIA classification is a measure of remoteness or accessibility which can be acquired from postcodes (University of Adelaide 1999) and indicates the degree to which a retailer is located in a centralised or urban area.

In this survey, remoteness was classified according to the following:

- highly accessible – an area with relatively unrestricted accessibility to a wide range of goods and services and opportunities for social interaction;
- accessible – some restrictions to accessibility of some goods, services and opportunities for social interaction; and
- remote – very restricted accessibility to goods, services and social interaction.

It is clear from the table that the vast majority (82%) of businesses were located in highly accessible areas (major towns or cities).

Weighting of data

Where data are reported in this paper which refer to the whole of Australia (for example, number of fraud incidents), the data have been weighted up to the population for greater representativeness (n=6,657). Weighted data were also used for some regression analyses (again, to ensure that the sample was representative of the distribution of the five business types across Australia), but so as not to inflate statistical significance, an effective sample size weighting was applied.

Table A1-1: Sample demographics (unweighted data)

	Florists		Booksellers		Music retailers		Toy & game		Computer		Total	
	n	%	n	%	n	%	n	%	n	%	n	%
Gender												
Male	40	17.1	94	56.9	151	75.1	131	61.2	185	87.7	601	55.8
Female	194	82.9	124	43.1	50	24.9	83	38.8	26	12.3	477	44.2
(n)	(234)	(100.0)	(218)	(100.0)	(201)	(100.0)	(214)	(100.0)	(211)	(100.0)	(1,078)	(100.0)
Business size												
<5 employees	226	96.6	182	83.5	174	86.6	197	92.1	149	70.6	928	86.1
5 or more employees	8	3.4	36	16.5	27	13.4	17	7.9	62	29.4	150	13.9
(n)	(234)	(100.0)	(218)	(100.0)	(201)	(100.0)	(214)	(100.0)	(211)	(100.0)	(1,078)	(100.0)
Annual turnover												
<$200,000	125	67.6	92	49.7	62	36.0	76	40.6	49	25.4	404	43.8
$200,000 to $499,999	53	28.6	40	21.6	59	34.3	59	31.6	61	31.6	272	29.5
$500,000 to $999,999	6	3.2	32	17.3	33	19.2	33	17.6	35	18.1	139	15.1
$1 million or more	1	0.5	21	11.3	18	10.5	19	10.1	48	24.9	107	11.6
(n)	(185)	(100.0)	(185)	(100.0)	(172)	(100.0)	(187)	(100.0)	(193)	(100.0)	(922)	(100.0)
Remoteness												
Highly accessible	185	80.1	185	85.3	167	83.5	159	74.6	178	85.2	874	81.7
Accessible	35	15.2	24	11.1	19	9.5	35	16.4	21	10.0	134	12.5
Remote	11	4.8	8	3.7	14	7.0	19	8.9	10	4.8	62	5.8
(n)	(231)	(100.0)	(217)	(100.0)	(200)	(100.0)	(213)	(100.0)	(209)	(100.0)	(1,070)	(100.0)

Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, unweighted data]

To weight up to the population, the data were weighted to represent the estimated total number of qualifying businesses nationally. The weighting process involved calculating the proportion of out-of-scope businesses (that is, 20 employees or more; or those not operating in the relevant industry) obtained from the sample contacted and applying this proportion to the number of businesses (post de-duplication) available from the sampling frame (Australia On Disc) for that business type.

Weighting was conducted independently within each business type, and the steps were as follows:

1. Determine the total population of each business type, as available from the sampling frame post de-duplication.
2. Subtract from that total the number of businesses known to be out-of-scope on the basis of their responses to the survey or the pilot.
3. Calculate the proportion of the attempted sample that was identified as being out-of-scope. Apply this proportion to that part of the population that was not attempted. The resulting figure is the estimated out-of-scopes among the unattempted sample.
4. Subtract the Step 3 result from the Step 2 result. The resultant figure is the estimated number of in-scope businesses within that business type.

Table A1-2: Weighting steps by business type

	Florists	Book-sellers	Music retailers	Toy/game retailers	Computer retailers
Starting population (step 1)	2,932	1,228	578	755	2,077
Known out-of-scopes	42	95	76	109	206
Step 2 total	2,890	1,133	502	646	1,871
Total attempted sample	741	715	578	746	1,075
Out-of-scope as percentage of attempted	0.057	0.133	0.131	0.146	0.192
Not attempted	2,191	513	0	9	1,002
Step 3 result: Estimated out of scopes from sample not attempted	124	68	0	1	192
Step 4 result: Estimated in-scope population	2,766	1,065	502	645	1,679
Complete in-scope interviews	234	218	201	214	211
Weight (step 5)	11.82	4.88	2.50	3.01	7.96
Weight for effective sample size	1.91	0.79	0.40	0.49	1.29

Source: Roy Morgan Research, Online credit card fraud against small business: technical report (2003), unpublished

5. The weight for each business interviewed within each business type is the Step 4 figure divided by the number of complete, in-scope interviews for that business type.

Finally, to obtain the effective sample size (for tests of statistical significance) the weights calculated in the five steps above were adjusted according to the formula, 'original weight' x (sample size/population). Table A1-2 summarises the weighting steps for each stratum.

Table A1-3 provides a breakdown of the sample by the state/territory in which they were located at the time of interviewing and by business type. The table provides both weighted and unweighted data and demonstrates the differences between each. It is clear from the table that the location of retailers with respect to state reasonably reflects the populations in each (for example, New South Wales contributed the highest number of respondents, whereas the Northern Territory contributed the fewest). With regards to differences between the weighted and unweighted data, the weighting resulted in a significant increase in florists and computer retailers and a significant decrease in music retailers and toy and game retailers – this distribution more accurately reflects the population.

Table A1-3: Respondents by business type and state – weighted and unweighted (row percentages)

State	Florists		Book-sellers		Music retailers		Toy/game retailers		Computer retailers		(n)	
	UW	W	UW	W	UW	W	UW	W	UW	W	UW	W
NSW	20	39	17	14	21	9	22	11	20	27	380	2,261
Vic.	21	41	23	19	16	7	20	10	19	24	287	1,770
Qld	29	49	17	12	13	5	17	7	25	28	175	1,232
SA	23	44	20	16	22	9	20	10	16	21	101	611
WA	15	33	25	23	28	13	16	9	15	22	67	363
Tas.	24	46	22	17	20	8	17	8	17	22	41	259
ACT	22	40	39	30	13	5	9	4	17	22	23	148
NT	0	0	25	39	50	39	25	23	0	0	4	13
(n)	234	2,766	218	1,065	201	502	214	645	211	1,679	1,078	6,657

UW = unweighted, W = weighted

Note: Percentages may not sum to 100 due to rounding

Source: Australian Institute of Criminology, Online credit card fraud against small business 2003 [computer file, weighted and unweighted data]

Appendix 2: Online credit card fraud questionnaire

Q1a Does the business accept payments made by submitting credit card numbers online through a business web site?

Yes *No* *Can't say*

Q2A When did the business start accepting payments made by submitting credit card numbers through the business web site?

Month ..... Year .....

Q3 What percentage of these TOTAL PAYMENTS were from payments made (by submitting credit card numbers) through the business web site?

Less than 5% *6% – 10%* *11% – 20%*

21 – 30% *31 – 40%* *41 – 50%*

51 – 60% *61 –70%* *71 – 80%*

81 – 90% *91 –100%* *Can't say*

Q4 Is authorisation from the bank AUTOMATICALLY sought without any processing by staff in the business and while the customer is waiting?

Yes *No* *Can't say*

Q5 How often would staff seek authorisation MANUALLY from the bank either by using an EFTPOS terminal, or phoning the bank, prior to sending out goods?

Never *Rarely* *Sometimes*

Most of the time *Always* *Can't say*

Q6a How often does the business phone the customer to confirm the order?

Q6b How often does the business check the customer's address/phone number in the current telephone directory?

Q6d How often does the business record details about good or bad customers in a database for future orders?

Q6e How often does the business reject an order if it appears suspicious?

Never *Rarely* *Sometimes*

Most of the time *Always* *Can't say*

IF NEVER, RARELY ASK:

Q6a1 Why does the business never or rarely phone the customer to confirm the order?

Q6b1 Why does the business never or rarely check the customer's address and phone number?

Q6d1 Why does the business never or rarely record details in a database for future orders?

Q6e1 Why does the business never or rarely reject the order if it appears suspicious?

Excessive cost *Too much time* *Not effective*

Other (specify) *Can't say*

IF MOST OF THE TIME OR ALWAYS, ASK:

Q6a2 Why does the business always or often phone the customer to confirm the order?

Q6b2 Why does the business always or often check the customer's address and phone number?

Q6d2 Why does the business always or often record in a database for future orders?

Q6e2 Why does the business always or often reject the order if it appears suspicious?

Limited cost *Quick* *Very effective*

Other (specify) *Can't say*

Q7 What percentage of orders placed on the business web site were rejected?

Less than 1% *1% – 5%* *6% – 10%*

11% – 20% *21% or greater* *Can't say*

Q8 Has the business been the victim of online credit card fraud since trading online?

Yes *No* *Can't say*

IF YES, ASK

Q9 Did the business suffer any online credit card fraud between 1 January 2002 and 31 December 2002?

Q10 Did the business suffer any online credit card fraud between 1 January 2001 and 31 December 2001?

Q11 Did you report any of these incidents to the police?

Yes *No* *Can't say*

Q12 How many incidents of online credit card fraud did the business experience between 1 January 2002 and 31 December 2002?

Q13 How many incidents of online credit card fraud did the business experience between 1 January 2001 and 31 December 2001?

Q14 How many incidents did you report to the police? .....

Q15 What was the amount of the chargeback for the last incident in 2002? .....

Q16 For the same incident, what was the amount of the chargeback fee? .....

Q17 Was the chargeback recovered by the business fully, partially or not at all?

Q18 Was the chargeback fee recovered by the business fully, partially or not at all?

Not at all/ not yet recovered *Partially recovered* *Entirely recovered* *Can't say*

Q19 For the same incident, were there any other costs associated with the chargeback?

Yes *No* *Can't say*

What were these costs that were incurred for the same incident? .....

What was the amount of the cost? .....

Q20 Was the cost recovered by the business fully, partially or not at all?

Not at all/ not yet recovered *Partially recovered* *Entirely recovered* *Can't say*

Q21 For the same incident, how did you discover the fraud?

Bank discovered *Business discovered* *Other party discovered* *Can't say*

Q22 For the same incident, how long after the purchase did the bank advise of the fraud?

Less than a week *A week or more but less than a month* *One month or more but less than two months* *Two months or more*

Q23 During the period from 1 January 2002 to 31 December 2002, did you suffer a financial loss as a result of chargebacks, chargeback fees, or other costs for online credit card fraud?

Yes *No* *Can't say*

Q24a What was your total loss as a result of online credit card fraud between 1 January 2002 and 31 December 2002? .....

Q24b What was your total loss as a result of online credit card fraud between 1 January 2001 and 31 December 2001? .....

Q25 Has excessive online credit card fraud at your business EVER resulted in your bank charging more than a standard fee because the business is seen to be 'high risk'?

Yes *No* *Can't say*

For each of the following statements, could you please tell me if you agree or disagree.

Q26a The bank is helpful whenever there is a query about a transaction performed on the web site.

Q26b The information provided by the bank in relation to online trading is easy to understand.

Q26c I am satisfied with the business accepting payments online.

Q26d Accepting payments online has significantly increased sales for the business.

Q26e The time staff spend manually checking online orders impacts on business productivity.

Q26f Confirming legitimate online orders hurts customer relations.

Strongly agree *Agree* *Neither agree nor disagree*

Disagree *Strongly disagree* *Can't say*

Q26g Thinking about the level of credit card fraud experienced from accepting payments online. Would you say this is lower than, about equal to, or higher than the expectations you had before you started accepting payments online?

Lower *Equal* *Higher* *Can't say*

Q27 How likely is it that your business will stop accepting payments within the next two years?

Very unlikely *Somewhat unlikely* *Somewhat likely*

Very likely *Can't say*

Q28 Has the business ever accepted payments through a business web site?

Yes *No* *Can't say*

Q29 In what year and month did the business start accepting payments this way?

Month ..... *Year* .....

Q30 And in what year and month did the business STOP accepting payment through a web site?

Month ..... *Year* .....

Q31 Did the bank forcibly remove the business's internet facility because of excessive online credit card fraud?

Yes *No* *Can't say*

Q32 Which of the following descriptions best describes your thoughts with respect to the business accepting payments online through a web site?

Never thought about *Thought about but haven't decided* *Thought about but decided against*

Actively pursuing *Can't say*

Q33 How likely is it that the business will begin accepting online payments in the next two years?

Very unlikely *Somewhat unlikely* *Somewhat likely*

Very likely *Can't say*

For each of the following statements, could you please tell me if you agree or disagree.

Q34a My business sells products which are well-suited to being sold over the internet.

Q34b The time and effort required to develop or maintain internet ordering systems is reasonable.

Q34c The cost of developing or maintaining an internet ordering system is reasonable.

Q34d The risk to online credit card fraud is outweighed by the benefits of selling over the internet.

Q34e Credit card fraud over the internet is very common.

Q34f Our customers did/would use our web site frequently to place orders.

Q35a We have found the bank to be supportive and helpful in dealings with them.

Q35b The costs required to set up/maintain systems online discourage merchants.

Q35c The credit card system is designed to protect customers, not merchants.

Q35d Banks care about small business losses from online credit card fraud.

Q35e Financial losses to credit card fraud online should be accepted as part of accepting payments online.

Q35f The prevention of online credit card fraud should be primarily the business's responsibility.

Strongly agree *Agree* *Neither agree nor disagree*

Disagree *Strongly disagree* *Can't say*

Q36 Who do you believe wears the majority of costs for online credit card fraud?

The business *Business bank* *Cardholder*

Cardholder bank *Other (specify)* *Can't say*

Q37 Does the business have a physical shopfront?

Yes *No* *Can't say*

Q38 Would you indicate the approximate annual turnover between 1 July 2001 and 30 June 2002?

Less than $200,000 *$200,000 to $499,999* *$500,000 to $999,999* *$1 million to $4,999,999*

$5 million or more *Can't say*

Q39 May I have the postcode of the business please? .....

Q40 The total number of full-time, part-time and casual employees?

FT ..... PT ..... Casual .....

Q41 And finally, the number of locations across which this business is spread? .....

References

Abru E 1999. Catching up to cyber crooks. *NSW police news* 79(9): 34–35

——— 2000. Plastic piracy. *NSW police news* 80(6): 38–39

Adey P 1999. Who is buying online? *Communications update* vol 160: 14–16

ANZ Bank 2003. Secure online transactions. http://www.anz.com.au/australia/business/merchant/securetrans.asp (viewed 19 July 2004)

Association for Payment Clearing Services (APACS) 2004. *Card fraud: the facts 2004*. http://www.cardwatch.org.uk/pdf_files/cardfraudfacts2004.pdf (viewed 19 July 2004)

Attorney-General's Department & Office of Strategic Crime Assessments (OSCA) 2000. *The changing nature of fraud in Australia*. Canberra: Attorney-General's Department

Australian Bureau of Statistics (ABS) 1993. *Australian and New Zealand standard industrial classification* cat no 1292. Canberra: Australian Bureau of Statistics

——— 2001. *Small business in Australia* cat. no. 1321. Canberra: Australian Bureau of Statistics

——— 2004. *Internet activity* cat. no. 8153. Canberra: Australian Bureau of Statistics

——— 2003. *Business use of information technology* cat. no. 8129. Canberra: Australian Bureau of Statistics

Australian Centre for Retail Studies (ACRS) 1999. *E-commerce in retailing: a survey of the Australian retail industry*. http://www.ara.com.au/ARA.1179732:LISTRIGHT:363884346:pp=ECREPORT1,pc=ARA_006 (viewed 26 August 2003)

Australian Information Industry Association (AIIA) 1999. *Getting paid on the Internet*. Canberra: Australian Information Industry Association

Australian Payments Clearing Association 2003. *Card transactions.* http://www.apca.com.au/Public/apca01_live.nsf/WebPageDisplay/Stats_CardVolume (viewed 19 July 2004)

Cybersource Corporation 2002. *Online fraud report*. http://www.cybersource.com (viewed 22 January 2003)

——— 2003. *5th annual online fraud report*. http://www.cybersource.com (viewed 15 December 2003)

Experian 2001. *Internet fraud: a growing threat to online retailers*. http://www.experian.co.uk/downloads/business/Internetfraud.pdf (viewed 19 July 2004)

Farrell G 1995. Preventing repeat victimisation. In M Tonry & D Farrington (eds) *Building a safer society: strategic approaches to crime prevention*. Chicago: University of Chicago Press

Fisher B & Looye JW 2000. Crime and small businesses in the Midwest: an examination of overlooked issues in the United States. *Security journal* 13(2): 45–72

Gibbons P 2001. Mouse clicks and dirty tricks. *Platypus magazine* vol 72: 33–34

Internet Scambusters 1998. Eight sure-fire strategies any business owner can use to reduce credit card fraud. *Internet scambusters* http://www.scambusters.org/CreditCardFraud.html (viewed 26 August 2003)

Kennedy D 2000. A web of crime. *Sydney morning herald* 11 July 2000

KPMG 2002. *Fraud survey 2002* http://www.kpmg.com.sg/publications/fraud_survey.pdf (viewed 10 December 2003)

Lang P 1999. How to beat credit card fraud. *Sell it!* http://sellitontheweb.com/ezine/howto004.shtml (viewed 19 July 2004)

Levy W 2002. Online fraud hits ACT business. *Canberra times* 13 May 2002

National Australia Bank 2002a. *Helping your business convert hits to sales.* http://www.national.com.au/downld/nsips.pdf (viewed 19 July 2004)

——— 2002b *Fraud prevention* http://www.national.com.au/Business_Solutions/0,,22354,00.html (viewed 19 July 2004)

National White Collar Crime Center & Federal Bureau of Investigation (FBI) 2003. *IFCC 2002 Internet fraud report*. http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf (viewed 19 July 2004)

Parliament of Victoria 2002. *Inquiry into fraud and electronic commerce: emerging trends and best practice responses*. Drugs and Crime Prevention Committee. Melbourne: Government Printer

Retail Decisions 2001. *ReD's guide to the payment card industry*. http://www.redplc.com/images/uploaded/ReDguidetoPaymentCardIndustry-Jan2001.a08e0d9e-6e53-4aaf-9f86-d0ba18397cf5.pdf (viewed 19 July 2004)

Roy Morgan Research 2003. *Online credit card fraud survey: technical report*. Brisbane: Roy Morgan Research (unpublished)

SA Police 2000. SApol joins the fight against e-crime. *SApol* vol 16: 6–7

Shankar U & Walker M 2001. *A survey of security in online credit card payments*. http://www.cs.berkeley.edu/~ushankar/research/ecommerce/credit.doc (viewed 19 July 2004)

Shimmin I 2000. Retailing in the future and the Internet. *Property investment and finance review* vol 1: 123–132

Smith RG 1999. Internet payment systems and their security risks. *Journal of financial crime* 7(2): 155–160

Smith RG & Urbas G 2001. *Controlling fraud on the Internet: a CAPA perspective. Report for the Confederation of Asian and Pacific Accountants*. Research and public policy series no 39. Canberra: Australian Institute of Criminology and Kuala Lumpur: Confederation of Asian and Pacific Accountants

St George Bank 2003. *Fraud prevention and risk management*. Sydney: St George Bank

Taylor N 2003. Reporting of crime against small retail businesses. *Trends & issues in crime and criminal justice* no 242. Canberra: Australian Institute of Criminology

Taylor N & Mayhew P 2002. Patterns of victimisation among small retail businesses. *Trends and issues in crime and criminal justice* no 221. Canberra: Australian Institute of Criminology

The Investigator 2002. Credit card fraud. *The investigator* [Qld] http://www.theinvestigator.com.au/articles_archives_ccfraud.html (viewed 16 May 2002)

Tomlinson D 2002. Unauthorised signature. *The investigator* [NSW] no 10: 24–26

Turpen A 2003. Preventing fraud on your web site. http://www.ezine-writer.com.au/articles/ic19867.aspx (viewed 19 July 2004)

University of Adelaide 1999. *Measuring remoteness: accessibility/remoteness index of Australia (ARIA)*. Occasional paper: new series no 6. Canberra: Department of Health and Aged Care

US Census Bureau 1999. *1999 annual retail trade survey*. Maryland: United States Department of Commerce

Visa 2004. Verified by Visa. http://usa.visa.com/business/technology_providers/vbv3_howitworks.html (viewed 19 July 2004)

Wales E 2003. E-commerce counts cost of online card fraud. *Computer fraud and security*: 9–11

Westpac 2003. Mastercard SecureCode & Verified by Visa: information pack and enrolment form. Sydney: Westpac Banking Corporation

Westpac 2000. *Merchant operating guide: card acceptance by business*. Sydney: Westpac Banking Corporation

Yellow Pages 2003. *Yellow Pages e-business report: the online experience of small and medium enterprises July 2002*. http://www.sensis.com.au/Internet/static_files/YellowPages_EbusinessReport_July03.pdf (viewed 26 August 2003)

Australian Government
Australian Institute of Criminology

Research and Public Policy Series
No. 60

While the online retailing environment has provided businesses with an unparalleled opportunity to expand and improve their profits, it has also increased the vulnerability of businesses to online credit card fraud. This report presents findings of an empirical study of the risks faced by Australian small businesses when they trade online. As well as examining the prevalence of online credit card fraud, the report considers strategies that businesses can adopt to reduce the risk of online credit card fraud. The findings of the study are intended to be of use to businesses that are currently retailing online, or contemplating online trade, as well as a resource for policy-makers and researchers.

ISBN 064253846-8
9 780642 538468