

Consumer scams in Australia: an overview

Russell G Smith

As part of a global effort to fight mass-marketed consumer frauds and scams, consumer protection agencies in a number of western countries participate in a month of fraud prevention activities each year to raise awareness of the problem and provide advice to consumers on how to avoid being victimised. An initiative of the International Consumer Protection and Enforcement Network in 2000, the campaign is joined by more countries each year, and in March 2006 some 33 countries participated. In Australia and New Zealand, 18 government agencies comprise the Australasian Consumer Fraud Taskforce (ACFT), established in March 2005 to support the network's activities. The key message to consumers in 2006 was 'when a scam comes calling – delete it, hang up, destroy it'. This emphasised the fact that consumers are their own best defence against scams, and should always err on the side of caution when conducting business transactions. This paper presents the results of a pilot study undertaken during March 2006 in which consumers who contacted the Infoline at www.scamwatch.gov.au, agreed to provide information on their experiences of consumer fraud over the preceding year. To date there has been limited statistical data to inform the development of policy in this area.

Toni Makkai
Director

Throughout history, consumers have been targeted by deceptive and misleading practices that have ranged in subtlety and complexity from the barely plausible to the refined and sophisticated. Grabosky, Smith & Dempsey (2001: 105–129) proposed a simple classification of the extensive range of illegal practices perpetrated against consumers, in the traditional marketplace and the electronic environment of the 21st century (Table 1). The fourth category has been refined to accord

Table 1: Classification of consumer fraud

Category	Subcategories
Advanced fee schemes (pretending to sell something you do not have while taking money in advance)	Pyramid schemes, Ponzi schemes, chain letters, 'Nigerian' emails, business opportunities, prizes and lotteries
Non-delivery and defective products and services (supplying goods or services of a lower quality than the goods or services paid for, or failing to supply the goods and services at all)	Online auctions, provision of internet services, cable decryption kits, computer products and services, sexual services, misleading credit and loan facilities, health and remedial products, educational qualifications
Unsolicited and unwanted goods and services (persuading consumers to buy something they do not really want through oppressive or deceptive marketing techniques)	Unsolicited advertising (spam), securities and investment fraud, bait advertising, inertia selling
Identity fraud (gaining money, goods, services, or other benefits, or the avoidance of obligations through the use of a fabricated, manipulated, or stolen/assumed identity)	Phishing, plastic card fraud, card skimming, unauthorised transactions, online banking fraud

Source: Grabosky, Smith & Dempsey 2001: 105–129

ISSN 0817-8542

ISBN 978 1 921185 33 5

GPO Box 2944
Canberra ACT 2601
Australia
Tel: 02 6260 9272
Fax: 02 6260 9293

For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website at: <http://www.aic.gov.au>

Disclaimer:
This research paper does not necessarily reflect the policy position of the Australian Government.

Project no. 0132

**AUSTRALASIAN
CONSUMER FRAUD
TASKFORCE**

AN INITIATIVE OF THE STATE, TERRITORY AND
AUSTRALIAN AND NEW ZEALAND GOVERNMENTS

with current law enforcement usage of identity fraud as outlined by the Australasian Centre for Policing Research (2006).

Such practices can arise out of transactions involving door to door sales, telemarketing, internet sales, and mail orders including email. The subject matter can involve contracts relating to home repairs, buying and servicing motor vehicles, purchasing health care products and services, as well as financial and investment advice. Funds can be obtained from consumers using all payment systems including cash, cheques, electronic funds transfers, and card-based transfers of funds.

Official statistics

At present, official police statistics are not collected in such a way that the consumer status of victims can be identified. Crimes involving deception are simply grouped together and include fraud against consumers, business and government. Police statistics do not show the methodologies used to perpetrate consumer fraud, or the extent to which, for example, email and e-commerce are involved. In its *National information development plan for crime and justice statistics*, the Australian Bureau of Statistics (ABS: 2005) has identified the improvement of fraud and electronic crime data as one of its 12 priority areas. The aim is to compile data to measure the size of the problem, and to obtain offender and victim information including economic impacts. In 2007, as recommended by the ACFT, the ABS will include key questions on consumer fraud in its regular household survey.

Agency administrative data

At present, there is no national uniform data collection scheme in operation for Australian consumer protection agencies. Australian Government agencies record the number and type of inquiries and complaints from consumers for their own internal purposes; hence data are not comparable across agencies. For

example, the Australian Securities and Investments Commission focuses on financial and investment matters, while the Australian Communications and Media Authority deals mainly with scams involving unsolicited email (spam). The Australian Competition and Consumer Commission has jurisdiction over consumer complaints that fall within the provisions of the *Trade Practices Act 1974* (Cth).

At state/territory level, complaints are categorised according to individual agencies' legislative remit, with little uniformity across agencies. In addition, because agencies deal with both inquiries from the public as well as official complaints of fraud and dishonesty, some matters that are recorded fall outside the definition of mass-marketed consumer scams, while other inquiries deal with matters that may, in fact, be legal.

In order to understand the general range of complaints relating to scams, members of the ACFT were asked to provide information on the number of scam complaints they handled between 1 July 2005 and 30 June 2006. Despite considerable variation in definitions and categories adopted, it was apparent from the information provided that the most prevalent types of matters, ranked in order of frequency, were lottery advance fee scams, pyramid/chain letter scams, employment/money mule/work from home scams, other advance fee/Nigerian letter scams and investment/get rich quick scams.

Less frequently reported were banking/phishing scams, online auction complaints, business opportunity scams, investment scams and advertising/merchandising scams.

Of course, these were only those matters reported through existing complaints mechanisms. The majority of matters were not recorded officially. It may be, for example, that most people simply ignore phishing scams without reporting them, despite their being extremely prevalent. At present, it is impossible to ascertain the exact number of

consumer complaints of various types that are recorded officially by agencies, although the ACFT is providing advice on how data collection can be improved.

Survey research

In recent years, a number of surveys have been conducted to obtain information about various dimensions of consumer fraud. Most have been carried out in the United States and Europe, although some Australian data are beginning to emerge. The following discussion focuses on Australian research.

The size of the problem

One of the key questions for policy makers concerns the incidence of consumer fraud in the community. A number of surveys have sought to determine how many consumers have experienced dishonest practices in the preceding 12 months.

In August 2006, Consumer Affairs Victoria published its *Consumer detriment survey* which measured 'the loss in consumer surplus that consumers experienced due to the presence of imperfect information as well as due to a fault or problem encountered with the product or service' (Consumer Affairs Victoria 2006: 1). The survey found that four percent of consumers surveyed had experienced a scam or a get-rich-quick scheme in the preceding 12 months. This was much lower than problems experienced by consumers relating to other categories of concern such as building renovations (22%), utilities (15%), transport (13%) and banking (10%) (Consumer Affairs Victoria 2006: 16).

In May 2006, Sensis carried out its Business Index Survey of Small and Medium Enterprises which examined attitudes and experiences of 1,800 small and medium enterprises from metropolitan and regional areas of Australia. The greatest area of e-commerce concern identified was the possibility of people being able to hack into computer systems, with 49 percent of online businesses

Table 2: Types of fraud relating to other purchases (percent)

Type of fraud	Age group		Total
	16–64 years	65 years and older	
Credit card purchases*	14	0	12
Door to door selling	18	32	20
Fax machine sales	5	0	5
Internet sales*	12	0	10
Items bought over the telephone	15	23	16
Mail order purchases	19	20	19
Telemarketing	9	12	9
Television sales	9	14	9

* Statistically significant at $p < .05$
 Source: Muscat, James & Graycar 2002: 5

indicating that this was a major concern for them (Sensis 2006b). While a large proportion of internet users surveyed expressed concerns about the potential for fraud, breach of privacy and misuse of personal information, only around four percent reported having actually lost money due to fraud, and approximately 13 percent reported experiencing a breach of privacy in online transactions (DCITA 2005: 26).

In December 2006, Sensis published its *Consumer report* (2006a) which examined the views of a sample of 1,500 Australians about consumer behaviour and confidence. It was conducted between 23 October and 21 November 2006. Out of 17 areas of concern in which the drought and the environment were ranked first and second, internet security ranked 15th, scoring 5.78 out of 10 (10 being the highest level of concern). Those in the 50 to 64 year age group rated internet security at 6.16 out of 10, the highest of any age group (Sensis 2006a: 13).

Types of fraud experienced

In the Crime Victims Survey conducted by the Australian Institute of Criminology (AIC) in April 2000, the 3,031 respondents described the most recent incident of fraud they had experienced. Information was classified into eight categories relating to various consumer activities, although the findings did not separately show incidents of mass-marketed scams or online fraud.

Within the category of ‘other purchases’, the highest types of fraud related to door to door sales, mail order purchases, and items bought over the telephone, as shown in Table 2. Credit card purchases and internet sales were less prevalent: note, however, that responses to the survey related to purchases undertaken some time ago, in 1999.

In 2004, the AIC conducted the Australian component of the International Crime Victimisation Survey. The sample consisted of 7,001 Australian households. After advertising and pop-ups (which affected just over 80 percent of households with home internet access), the next most commonly reported problem in Australia concerning internet purchasing was spam, followed by viruses or hacking – both these problems affected more than half of the households with internet access. One in four households with internet access were exposed to internet scams and almost one in five were exposed to false websites and harassing email messages (Krone & Johnson 2006).

Age of victims

The AIC’s Crime Victims Survey of 2000 was undertaken, in part, to examine the extent of consumer fraud victimisation against older Australians and compared their experiences with those of younger persons. It was found that the risk of being a victim of consumer fraud was much lower for older Australians than it was for the population as a whole.

Nine percent of persons aged 16 to 64 reported being the victim of consumer fraud compared with four percent of people aged 65 and over (statistically significant at $p < .01$). Those aged 65 years and over were found to be less than half as likely to be victims of consumer fraud than people aged 16 to 64 (Muscat, James & Graycar 2002).

The findings from this survey indicated that those older people who are at risk of consumer fraud (a minority) are also more likely than other older people to experience personal crime (robbery, assault or theft). The chance of being defrauded was also found to be independently linked to having a more active social life (measured by the frequency of going out in the evening). This was consistent with the idea that being more socially active goes with being more commercially and financially active, and thus more exposed to possible deceitful transactions. In this sense, older Australians are no different from the rest of the population.

Fraud reporting

Those who have experienced consumer fraud can report the problem not only to police, but also to consumer protection agencies, banks and other organisations in the private sector. In the 2000 survey, 35 percent of all victims of fraud reported the last incident either to the police (13%) or another agency (22%: this difference being statistically significant at $p < .01$). Reporting patterns were similar among younger and older persons.

More recently, findings from the Australian component of the International Crime Victimisation Survey (Krone & Johnson 2006) showed that half of all households experiencing difficulties when making an internet purchase reported them to a bank (26%) or some other agency (21%) but rarely to police (3%). Almost five percent did not know whether the incident had been reported at all. Fraud which occurred offline was more likely to be reported than were problems with online incidents. It was found that overall

88 percent of households where credit/bank card misuse had occurred said the matter had been reported – to banks (72%), police (24%) or another agency (8%).

In a survey of consumers in Victoria, Moustakas (2006) found that only six percent of respondents who had experienced problems with an online auction site had contacted police, and only two percent had contacted a consumer protection agency. For 19 percent of respondents, nothing was done in response to the problem.

Consumer perceptions and concerns

A number of surveys have covered concerns about fraud and related issues.

The Australia SCAN conducted annually by Quantum Market Research (2006), found that almost 70 percent of those surveyed used the internet, with almost 20 percent using it every day. Approximately 30 percent of respondents used the internet for banking and travel bookings, although 57 percent were unhappy about using their credit card over the telephone and even more so via the internet (65%).

A global survey for Visa International (2006) in November and December 2005 in 12 countries examined attitudes towards data security and consumer behaviour. Of the more than 6,000 respondents, 64 percent said that loss or theft of personal information was their biggest concern, even above terrorism (58%), job loss (57%), disease epidemics (55%) and natural disasters (48%). Australians felt more secure than respondents from other countries (63% compared with the global average of 57%). In relation to vulnerability and risk that their personal or financial information would be lost or stolen in the near future, only 12 percent of Australians believed this to be very or extremely likely, compared with the global average of 26 percent. Also, less than half (47%) of Australian consumers had heard, read or seen something in the news over

the previous few months regarding personal or financial information being stolen (ranked lowest of all countries participating in the survey). Interestingly, the higher the awareness by consumers the higher their level of concern.

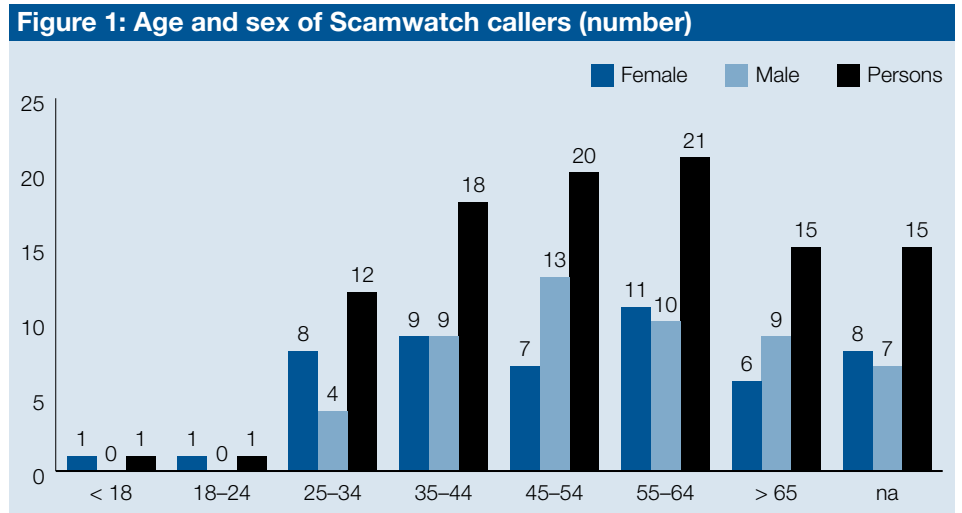
In May 2006, the Unisys Security Survey and Index 2006 was conducted by Newspoll. A representative national sample of 1,200 respondents aged 18 years and over was surveyed for the quarterly report on national security concerns. It showed that 56 percent of the respondents had high levels of concern (very/extremely) about unauthorised access to personal information or its misuse, while 53 percent had high concern about other people obtaining their credit or debit card details. Women were much more likely to be extremely or very concerned about people obtaining these details than men were. These levels of concern were

higher than the perceived threat of war/terrorism (41%) and much higher than concerns about their personal safety over the forthcoming six months (14%: Unisys 2006).

More optimistically, a survey conducted by eBay of Australian internet users in May 2006, found that three out of four regular internet users believed online shopping was becoming safer, a 10 percent increase from 18 months earlier (eBay 2006).

Scamwatch 2006

As part of the ACFT’s March 2006 campaign, 103 of the 121 callers (85%) to the ACCC’s national hotline agreed to complete a questionnaire concerning their experiences of consumer scams over the 12 months from March 2005 to March 2006. Although the results of this pilot study are not indicative of consumer fraud throughout Australia in view of the



Source: Unpublished ACCC data 2006

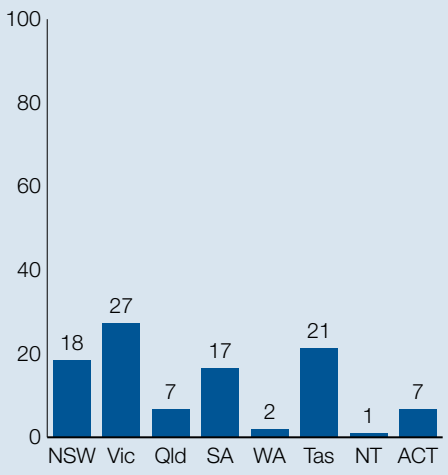
Type of scam	Mode of delivery of scam offer				Total ^a
	Phone	Email	Mail	Other	
Notification of lottery win	9	39	51	2	100
International money transfer	0	69	29	3	100
Phishing	7	86	7	0	100
Supply financial advice	22	48	30	0	100
Other ^b	20	15	5	60	100
Total	10	51	31	8	100

a: May not sum to 100 due to rounding

b: Other includes calls where it was not possible to identify clearly the method used to reach the customer

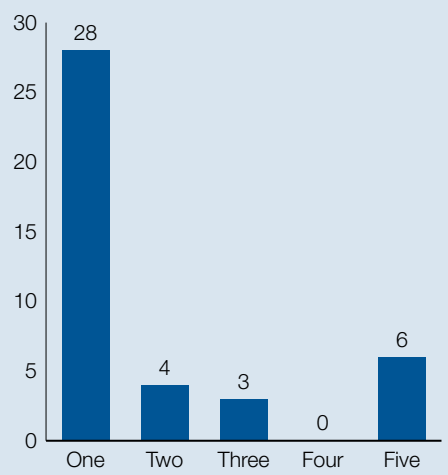
Source: Unpublished ACCC data 2006

Figure 2: Scamwatch callers by jurisdiction (percent)



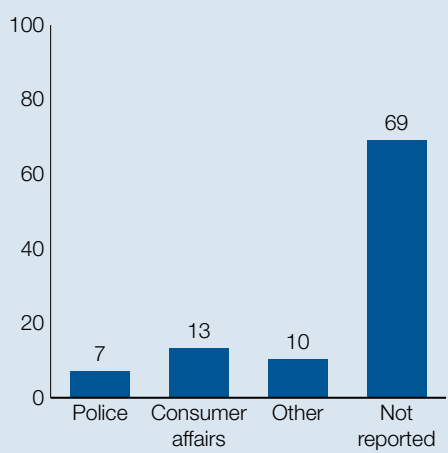
Source: Unpublished ACCC data (2006)

Figure 3: Persons responding multiple times to a scam (number)



Source: Unpublished ACCC data 2006

Figure 4: Reporting behaviour of callers (percent)



Note: Only 97 callers completed this question
Source: Unpublished ACCC data 2006

sample being relatively small, self-selected and focused on the ACCC's campaign activities, some preliminary findings are of interest.

Age

Three items of demographic information were collected from callers – their gender, age, and state or territory of usual residence. Respondents were evenly split by gender, with 50.5 percent of callers being male, and 49.5 percent of callers female. Figure 1 shows data on Scamwatch callers by age and sex.

Although 15 percent of callers refused to state their age, it was found that only two percent of callers were 24 years of age or less, with 29 percent of callers between 25 and 44 years, and 40 percent of callers between 45 and 64 years. With 15 percent of callers being over 65 years of age, this represents a much higher proportion than in the Crime Victims Survey of 2000.

Location

Most calls came from Victoria (28) followed by Tasmania (22), New South Wales (19) and South Australia (17) with other states and territories recording smaller numbers (Figure 2). This distribution follows the impact of the media campaign, rather than population size or incidence of scam victimisation generally.

Type of scam received

Callers were asked whether they had received an unsolicited notification of having won a lottery, request to transfer money, bank request (phishing), offer of financial advice or other scam offer, and the method of contact. Callers were also asked to specify whether they were contacted by mail, email, phone or other means. Multiple responses were allowed to enable a recording of multiple scam types and methods of delivery. The most common offer related to lotteries (67 callers), of which most were received by mail (34) and email (26). Requests to transfer money were received by 32

callers, with 23 of these by email. Some 28 callers received bank request offers (including phishing scams) with all but four of these coming via email. Financial advice offers were received by 23 callers of which 11 were by email and seven by mail (see Table 3).

Of those who had received an offer, the majority had not responded positively. However, 43 callers (44%: five callers did not answer this question) had responded once to one of the scams, and 13 (30%) had responded more than once. As Figure 3 shows, a small proportion of callers responded repeatedly to scams.

Over 80 percent of callers in all categories except 'other scam offers', had not responded at all to scams. Some 13 percent of people who had received lottery offers replied once, with a further eight percent responding on more occasions. Recipients of requests for money transfers, bank requests and financial advice did not respond to the offers at levels of 95 percent, 96 percent and 97 percent respectively. Other scam offers (10), which included competitions, holiday offers, and business opportunities, had a 50 percent non-response rate. Three callers had responded to competitions, and one each to holiday and business offers.

Consumer perceptions

Callers were asked whether they perceived these unsolicited invitations as being criminal, wrong, something that just happens, or if they didn't know whether the acts were criminal. Responses varied across the different scam types. The highest proportion of respondents believed that lottery invitations were criminal (72%), followed by advance fee frauds (65%), financial advice frauds (42%) and phishing scams (44%). Respondents expressed a range of opinions relating to phishing, with it receiving the lowest 'crime' response of all the scams and the highest level of 'wrong' (12%), 'something that happens' (17%), and 'don't know' responses (21%).

Financial loss

Fifteen respondents admitted they had suffered financial losses in the preceding 12 months as a result of responding to a consumer scam (16%). One person refused to answer this question and a further five failed to respond. Reported losses ranged from \$30 to \$100,000. Overall, 82 out of the 97 respondents had not suffered any loss. Of the 15 people who did lose money, seven lost up to \$100, two lost up to \$1000, five lost up to \$6000, and one lost \$100,000.

Reporting

Finally, callers were asked whether they had reported their experiences officially and, if so, to whom. The majority of people had not reported these unsolicited invitations to any authority or regulatory body (69%) (Figure 4).

Of those who had lost money as a result of consumer frauds in the preceding 12 months, some 87 percent had not made any report to any authority. This was a higher non-report rate than for those who had not lost money (66%). None of the individuals who reported that they had lost money through responding to a scam had reported their experiences to state or territory police. One person had reported the incident to a consumer affairs authority (7%), and another to another body (7%). In comparison, seven persons who had not lost money reported unsolicited offers to state or federal police (8%), 12 persons reported scams to a consumer affairs agency or office of fair trading (15%), and nine had reported the scams to another body (11%).

Seven percent of all respondents had reported the incident to police,

13 percent had reported the issue to a consumer affairs agency or office of fair trading (including the ACCC), and 10 percent had reported to some other authority such as banks, legitimate traders, other persons affected by the scam, and consulates.

Conclusion

In Australia at present, only limited data are available on the nature and extent of consumer fraud victimisation. It is known, however, that large numbers of consumers are targeted by fraudsters each year, many operating from overseas. Despite the best endeavours of consumer protection agencies, a small proportion respond to unsolicited invitations and some of these send money, most of which is never recovered. Relatively small proportions of those defrauded report their experiences officially, through fear of appearing foolish, or because they perceive that little can be done.

The ACFT is helping to raise awareness of the problem of consumer fraud in Australia and New Zealand, and the taskforce has facilitated the collection of national prevalence data that will be available in time for the March 2008 campaign. The taskforce is also helping agencies to improve their administrative complaints data holdings to make them of greater use, more timely, complete and comparable with other agencies. Armed with new information, consumers can be alerted to the latest scams as soon as they arise, and provided with information on how to minimise risks and what to do should they be misguided enough to have responded to scams.

Acknowledgments

This paper makes use of information provided by members of the ACFT. Scamwatch 2006 data were provided by Leo Exarhos of the ACCC. Dr Inez Dussuyer assisted with background research. The views expressed are those of the author and do not necessarily represent the views or policies of the agencies represented on the taskforce.

References

- Australasian Centre for Policing Research 2006. *Standardisation of definitions of identity crime terms: a step towards consistency*. Report no. 145.3. Adelaide: ACPR
- Australian Bureau of Statistics 2005. *National information development plan for crime and justice statistics*. Canberra: ABS
- Consumer Affairs Victoria 2006. *Consumer detriment survey*. Melbourne: IPSOS Australia
- Department of Communications, Information Technology & the Arts 2005. *Trust and growth in the online environment*. Canberra: DCITA
- eBay 2006. *Annual report 2005*. <http://investor.ebay.com/annual.cfm>
- Grabosky PN, Smith RG & Dempsey G 2001. *Electronic theft: unlawful acquisition in cyberspace*. Cambridge: Cambridge University Press
- Krone T & Johnson H 2006. Internet purchasing: perceptions and experiences of Australian households. *Trends & issues in crime and criminal justice* no. 330
- Moustakas N 2006. *Going, going, gone: online auctions, consumers and the law*. Melbourne: Communications Law Centre
- Muscat G, James M & Graycar A 2002. Older people and consumer fraud. *Trends & issues in crime and criminal justice* no. 220
- Quantum Market Research 2006. *Australia SCAN 2006: monitoring cultural change*. Melbourne: Quantum Market Research
- Sensis 2006a. *Consumer report 2006*. Melbourne: Sensis
- Sensis 2006b. *e-Business report 2006*. Melbourne: Sensis
- Unisys 2006. *Unisys Security Survey and Index 2006*. Sydney: Unisys
- Visa International 2006. *Consumer attitudes and behaviours toward data security in Asia Pacific*. Hong Kong: Harris Interactive