Australian Competition & Consumer Commission

ACCC Submission

House of Representatives
Standing Committee on Communications
Inquiry into cyber crime

July 2009

Summary

Cyber crime in its broadest application covers a range of conduct some of which is associated with social harm and other conduct that causes economic harm. The Australian Competition and Consumer Commission (ACCC) is focussed on economic harm to consumers and on competitive markets. This includes conduct that is fraudulent and has the purpose of misleading consumers for financial gain.

The *Trade Practices Act 1974* (the Act) applies to misleading or deceptive conduct and other fraudulent activity. The ACCC enforces the Act and also has a role in educating the community on how to recognise and deal with fraudulent conduct and avoid becoming a victim of such conduct.

This submission outlines how the ACCC manages its role through its educative function, disruption activities and where appropriate, enforcement action. The submission also outlines the leadership role that the ACCC has taken in relation to cross-agency work on cyber crime both within Australia and internationally, particularly in the area of online consumer scams. The ACCC has taken on this role because we recognise the increasing importance of inter-agency cooperation as well as working with other organisations in the private sector to achieve positive outcomes in the area of cyber crime.

The challenges of cyber crime

Where the internet appeared to offer seemingly endless opportunities for e-commerce, it now also offers anonymity and innovative tools for criminals, unscrupulous traders and scammers.

The result of their activities in the area of fraud is one of significant personal loss[1] to consumers, as well as losses to business and the economy. Cyber crime is also likely to be hindering strong growth in e-commerce by undermining consumer confidence in the reliability and safety of transacting online.

Apart from the ACCC, a number of state and federal law enforcement agencies have responsibilities that relate to cyber crime. Many may face similar challenges when dealing with issues that arise from dealing with such conduct including the difficulties in effectively and swiftly removing offending websites, locating scammers, securing evidence and dealing with cross border and jurisdictional issues.

---

[1] In 2007, the Australian Bureau of Statistics published a report on personal fraud. The report showed that of the victims surveyed, 453,000 incurred a financial loss totalling one billion dollars. This included losses from online conduct such as phishing and advance fee fraud. – see *ABS Personal Fraud 4528.0 2007*.

The ACCC and the Trade Practices Act

The ACCC is an independent statutory authority that promotes competition and fair trade in the market place to benefit consumers, business and the community. It also regulates national infrastructure industries. Its primary responsibility is to ensure that individuals and businesses comply with the Commonwealth's competition, fair trading and consumer protection laws.

As part of its consumer protection provisions, the Act prohibits conduct that is misleading or deceptive or likely to mislead or deceive.

The Act also provides for the dissemination of information.

What is 'Cyber crime'?

Cyber crimes are generally technology enabled and can involve significant potential social harm such as child pornography and cyber stalking or economic harm including frauds, scams, spam, phishing and identity theft. The conduct may involve a number of perpetrators and in some cases, the perpetrator may not be aware of their involvement in the conduct.

There are a number of laws in Australia that specifically deal with such conduct including the *Cybercrime Act 2001*, the *Spam Act 2003* and various provisions in the *Criminal Code Act 1995*.

General laws also apply. In the case of conduct that amounts to fraud or misleading or deceptive conduct, the Act applies as do general criminal offences that relate to obtaining advantage in the marketplace by deception. This could include price fixing and other collusive behaviour where technology was being used to not only facilitate but also to attempt to obfuscate the steps being taken to perpetrate the conduct.

Cyber crime vs misleading or deceptive conduct

The ACCC receives many complaints each year that relate to scams. In the last financial year, over 18,000 such complaints were recorded out of a total of approximately 77,000 recorded on the ACCC's complaints database. Of these, around 12,000 complaints related to online scams. Of course, the ACCC is only one of the agencies that receive complaints about such activities.

Losses for all types of scams reported during that period, totalled over $50 million. The biggest losses were to advance fee fraud (eg Nigerian or 419 scam), which netted around $30 million. These frauds are often perpetrated via spam and unsolicited mailouts, where the trader is difficult to trace or identify.

Complainants have also reported fraudulent conduct that can involve the proliferation of malware, such as via phishing emails.

A multi-pronged approach has been adopted to address consumer concerns regarding this conduct. The main focus is on the use of education, complemented by disruption activities and working with other agencies, both international and domestic.

Where the conduct involves representations made in trade or commerce by an identifiable trader whose main aim is to relieve consumers of their money, the ACCC may take an active enforcement role.

Educative and outreach activities

SCAMwatch

The main platform for providing information about scams is the ACCC's SCAMwatch website.

SCAMwatch seeks to inform consumers and small business about how to recognise, avoid and report scams. The ACCC considers that SCAMwatch is a powerful and effective tool in its endeavours to raise scam awareness and combat scams.

The site was devolved to the ACCC from the Treasury, where originally it housed the *Little Black Book of Scams.* SCAMwatch was revamped and relaunched in 2006.

The current site provides information on a range of scams, including those that are perpetrated online and related activity such as phishing. There are also regular postings on current scams, mock scams to show the tricks of the trade, a downloadable version of the *Little Black Book of Scams* plus a complaints portal that lists where to complain for common scams.

SCAMwatch also provides a free subscription alert service. There are currently over 11,000 subscribers.

For the March Quarter 2009, the SCAMwatch site received 105,440 unique visitors and 1,009,792 hits. One of the most visited areas of the site is the 'victim stories'. These clearly show that scams can affect people from all walks of life

The most recent alerts related to online conduct have been on a number of phishing emails featuring the logos/crests for well-known agencies or businesses including the ATO, the Commonwealth Bank and McDonalds.

Others have issued warnings against online overpayment scams, scareware or fake virus protection, and scams targeting social networking sites.

Alerts and postings form part of the ACCC's disruption activities. Consumers who are forewarned are less likely to become victims and the fewer consumers who actively refuse to deal with scammers, the sooner the conduct will cease.

As well as the revised *Little Black Book of Scams*, a series of fact sheets are being released. These include the fact sheets *Phishing* and *Money transfer scams*.

Australasian Consumer Fraud Taskforce

The SCAMwatch website also provides a portal for the work of the Australasian Consumer Fraud Taskforce (**ACFT**). The ACCC chairs the ACFT which was formed in 2005. It comprises 19 government regulatory agencies and departments with responsibility for consumer protection regarding frauds and scams.

The ACFT works to enhance the efforts and impact of Australian and New Zealand regulatory and enforcement agencies in their fight against consumer frauds and scams. This is undertaken through sharing information on enforcement activities as well as educative and information campaigns. The ACFT is also involved in research on consumer fraud,

The ACFT actively involves the private sector and community groups in its information campaigns and encourages them to share information they may have on scams and fraud.

Each year, the ACFT holds its outreach campaign timed to coincide with Global Consumer Fraud Prevention Month in an effort to inform consumers how best to avoid being scammed. In 2009, as well as its annual campaign the ACFT hosted the Consumer Fraud Forum that provided an opportunity for information sharing and discussion on strategies for dealing with scams. The introductory address to the Forum given by Mr Peter Kell, ACCC Deputy Chair and also Chair of the ACFT can be found at Attachment #A.

Outreach to business and consumers

The ACCC continues to have a strong role in outreach work, in particular in regional areas. Part of this work includes educating both businesses and consumers to the dangers of online scams and related fraudulent conduct. This also includes strong messages about the importance of effective computer security.

Outreach work includes presentations by the ACCC's Regional Outreach Managers to business groups (for example, industry associations) and community organisations such as Probus, Rotary and senior citizens groups. Commissioners and staff also use appropriate speaking opportunities to educate business and consumer groups and organisations about the importance of being vigilant against scams and assist in halting the progress of scam activity.

The ACCC also produces two publications on scams that target small business – a DVD entitled *Scams, frauds and your business*, which looks at e-commerce scams, business start-up scams and directory listing scams, and *News for business – Scams, protect your business from them*, which offers information to businesses on ways to avoid falling victim to scams that most commonly target their activities.

International and domestic liaison

The ACCC participates in the work of multi-agency initiatives and working groups that focus on combating scams and mass marketed fraud. The aim of these initiatives ranges from coordinated educative strategies to intelligence sharing protocols that may assist in locating scammers or disrupting their activities.

The ACCC has also participated on number of occasions in the US Federal Trade Commission initiative known at one stage as the 'Open Relay' campaign. Through this campaign, letters were sent to administrators of servers that had been identified as having open ports that could be used to relay spam, recommending that these ports be closed.

The ACCC is a member of the International Consumer Protection and Enforcement Network (**ICPEN**) and in August 2009 will be taking on the role as President of ICPEN. ICPEN is a network of national fair trading law enforcement agencies from over 30 countries, most of which are members of the Organisation for Economic Cooperation and Development (OECD).

ICPEN's mandate is to share information about cross-border commercial activities that may affect consumer interests, and to encourage international cooperation among law enforcement agencies.

ICPEN conducts regular International Internet Sweep Days, which is coordinated by the ACCC, to generate important information for enforcement agencies in targeting unscrupulous internet traders, and serves as a reminder that the internet is not an unpoliced forum for trading.

ICPEN agencies have assisted the ACCC in a number of successful investigations, as can be seen from the case studies below.

Enforcement action – selected case studies

Since the early 2000s, the ACCC has taken up the challenge of testing the reach of the Act across the internet space. A number of positive outcomes have resulted from investigations into online conduct including those involving get rich quick schemes, exaggerated claims for questionable products, domain name resellers and online directories that failed to deliver a decent service.

Success in this arena has also highlighted the integral role that international and domestic cooperation plays in achieving this success. The ACCC continues to build on this strategy. The following selected case study summaries particularly illustrate the importance of cooperation.

Designer Brand Outlet

Late 2008, the activities of the Designer Brand Outlet website were brought to the ACCC's attention by the US Federal Trade Commission, after reviewing complaints made by a number of overseas consumers to the eConsumer.gov website.

eConsumer.gov is an ICPEN initiative. The site provides information on international fair trading issues as well as a complaints portal where consumers from across the globe can complain about online traders that appear to be operating out of member countries.

Consumers reported that they had lost their money to a website that they had trusted as it gave the impression that it was Australian. In fact the site was being operated out of China. Consumers either did not receive anything for their money or poor quality merchandise instead of the designer brand clothing advertised.

In dealing with such online conduct which can reach consumers anywhere in the world at any time of the day, it was important to act quickly to prevent other consumers from getting caught. Assistance was obtained from a number of parties once informed of the ACCC's concerns. The domain name registrar disabled the website and the bank where the website's merchant facility was held, suspended the service after conducting its own inquiries.

The ACCC was also able to have the assets of the company frozen to ensure some return for consumers who lost money.

The matter was concluded in April this year after those responsible for the site offered compensation for consumers that had been misled.

Sydney Opera House

In 2002, Mr Richard Chen operated a fraudulent website that purported to be the official booking site for the Sydney Opera House. Consumers in both the UK and in Europe had been caught by Chen's fraudulent site.

The website was both hosted and administered from overseas, thus posing particular difficulties. The matter highlighted the valuable cooperation from the ACCC's counterpart ICPEN agencies, in particular the US Federal Trade Commission.

In August 2003, the Federal Court declared that the site was illegal. In his summary, Justice Sackville said that 'While domestic courts can, to a limited extent, adapt their procedures and remedies to meet the challenges posed by cross-border transactions in the internet age, an effective response requires international cooperation of a high order'.

Worldplay Services

Similar cooperation was also called upon during the investigation into a Gold Coast company, Worldplay Services Pty Ltd. In 2004, the Federal Court found that Worldplay Services had participated in an international pyramid scheme. Consumers recruited into the scheme came from a number of countries, including Canada, the UK and Norway. The matter involved the cooperation of a number of overseas regulatory bodies. In parallel proceedings, the Royal Canadian Mounted Police took successful criminal proceedings against Canadian participants.

Cash for Organs

In securing the prompt removal of the Cash for Organs website in June 2008, the ACCC was able to provide assistance to domestic agencies. The site had claimed that it could link transplant donors and recipients. It was also intimated that organs could be sold through the site, however there are legislative restrictions that prohibit the sale of organs.

Strategic disruption

The investigations listed above highlight the importance of swift action and cooperation with a number of parties, including overseas agencies to achieve a positive outcome for consumers. This is particularly important when it comes to online conduct as the internet can be a very effective hiding place.

Where the perpetrator is unidentified such as those behind scams promoted via spam or those that target online classifieds, as mentioned previously the ACCC's main focus is on education and outreach activities. However, more recently a strategic approach to disruption has also been used to complement the ACCC's educative work. In a practical way this has been through intelligence sharing such as providing IP addresses, bank account and other relevant details derived from preliminary investigations to appropriate agencies.

The ACCC also works actively with providers of online content such as online classifieds, social networking and employment sites to have identified scams removed. In the March Quarter 2009 over 500 fraudulent online classified ads were removed with the assistance of the website administrators.

Disruption case study - A proactive approach to significant events

In some instances, rather than wait for scams to be reported a proactive approach has been devised for dealing with identified significant events.

Natural disasters such as floods, fire and tsunamis as well as celebrity deaths and sporting events will often attract scammers, including those that operate online. As an example during the recent Victorian bushfires, the ACCC took a proactive approach, beginning with a number of warnings about potential charity scams, issued via SCAMwatch and media releases.

Lists were made of possible domain names that could be used by scammers wanting to catch anyone looking for a website where donations could be made online. These domain names were monitored on a daily basis, with staff actively scrutinising any websites found.

Complaints to SCAMwatch and the ACCC's Infocentre were also carefully monitored. Two websites of concern were located. One site was disabled through the assistance of other agencies and another modified voluntarily by the site's owner. It transpired that neither site was intent on actually scamming the public and where monies were collected these were provided to the charity leading the appeal.

Trap email accounts were also monitored for any phishing emails. To date none were found. However, the unfortunate event could be used as part of an inheritance scam at a later date. Where appropriate, a similar strategy will be adopted at times of high profile events.

Future opportunities for criminal activity

The internet has provided an opportunity for ever developing areas of commerce. However, where there is an opportunity for commercial activity there is also the likelihood that this opportunity will attract fraudsters of every kind. Online forums and complaints to regulators such as the ACCC have shown that the internet space has delivered both positive and negative results for consumers, with the negatives including products paid for never being delivered, online dating scams and bogus business opportunities. No doubt these tried and true scams will continue while there are ready victims.

There is also concern that future developments of the internet and related technology such as advanced internet and mobile telephony will assist in facilitating anti-competitive conduct that will impact on other businesses, for example the collusive activities of price fixing and market sharing. Recent changes to the Act have now opened the way for this conduct to be considered criminal where appropriate. However, new or developing technologies will call for vigilance and using the correct tools for tracking electronic footprints.

Recent developments have also shown fraudulent conduct and scams being pushed through mobile phones and the mobile internet. This platform for the proliferation of malware and scams is still in its infancy but is expected to rise.

The ACCC has received a number of complaints from concerned consumers regarding suspicious messages being sent to their phones. A recent 'death threat' SMS was

particularly nasty. The text message was followed by an extortion email to anyone who cared to respond.

For now, these scams have been fairly basic in their execution, involving follow-up phone calls or email contact. After that they appear to adopt the operating method of the well-known email lottery scam or advance fee fraud. However, it is not expected that this will last. More sinister approaches are bound to surface given the number of mobile phones in the community coupled with their broader use in accessing emails and social networking sites.

The impact of changes to the internet space such as the dynamic and interactive Web 2.0 and beyond will also offer further opportunities for cyber criminals. This is an internet space that caters for user-centred activities and peer-to-peer communication, allowing perpetrators easy access as was seen in recent attacks on popular social networking sites.

Attachment A

Consumer Fraud Forum

2 March 2009

Introduction – Combating Consumer Fraud

Peter Kell

Chair, Australasian Consumer Fraud Taskforce

Deputy Chair, Australian Competition and Consumer Commission

Welcome to the inaugural Consumer Fraud Forum. This Forum kick-starts our 2009 National Consumer Fraud Week, which is the major annual education and awareness campaign run by the Australian Consumer Fraud Taskforce.

Consumer fraud is as old as consumer markets. But there's no doubt that the opportunities for scam operators have expanded dramatically in more recent times. The Australian Bureau of Statistics recently found that around 1 in 20 Australians fall victim to some sort of consumer fraud each year, with a direct cost to the community of around a billion dollars. At the Australian Competition and Consumer Commission we have seen a significant increase of more than 60% in scams reported in 2008 compared to 2007, and this accelerated towards the latter part of the year. Given this context, given how high the stakes have become, it's vital that we ask how we can best combat consumer frauds and scams. That's what today's forum is about.

This is the first time we have run a Fraud Forum in conjunction with Consumer Fraud Week. We have a great mix of speakers, including expert academics from the UK and Australia We'll also hear from some private sector firms about their experience in combating consumer scams. And you'll hear from representatives from some of the Australian government agencies that are members of the Australasian Consumer Fraud Taskforce - practitioners in the field so to speak who can speak with experience about dealing with consumer scams.

The Australasian Consumer Fraud Taskforce

And as the Forum is hosted by the Australasian Consumer Fraud Taskforce and I'd like to say a few words about this group before looking at trends in consumer scams.

The Taskforce was established in 2005. The ACFT has 19 government members - 18 from around Australia, with agencies from the Commonwealth, States, and Territories represented, as well as a representative from New Zealand. In effect the establishment of this group is a clear indication of the increasing importance of coordinated efforts in combating consumer fraud.

I am pleased to be able to welcome representatives here today from many of the agencies involved in the Taskforce.

The purpose of the Taskforce is:

- To ensure that government agencies in Australia and New Zealand work together more effectively in the fields of consumer education and enforcement against frauds and scams

- To share information and generate research in the area of consumer scams and frauds. A major example of this was the recent ABS Survey on personal fraud, which I know other speakers will discuss today.

- To undertake an annual Consumer Fraud Week - a co-ordinated information campaign for consumers about consumer fraud.

Consumer frauds and scams are typically classified into two types:

- Technical scams. These target a consumer's computer - in many cases the consumers may be unaware of such attacks.
- Deception Scams. These are the more familiar scams, and of course have a long history. They rely on the consumer to respond in some way to the offer, whether it's easy money or a free holiday.

The Taskforce is interested in combating both types of scam, and different agencies bring different expertise to this task. Having said this, in the areas of both consumer education and enforcement activities to address the second type of scam – deception scams - are a particular focus of the Taskforce.

The ACCC's SCAMwatch website acts as the portal during the Scam Week campaign to carry key messages, with each agency promoting their own messages depending on their target audience and jurisdiction. Of course, Scamwatch.gov.au also provides a service to consumer all year round, with:

- an extensive set of tips about how to identify scams and how to avoid scams;
- updates on the latest scams that are currently 'doing the rounds'; and
- facilities to report scams.

The Taskforce is also linked to the Mass Market Global Fraud Project of the International Consumer Protection Enforcement Network (ICPEN). At this time each year over 30 consumer protection agencies from around the world participate in campaigns to warn consumers against scams and frauds.

As well as government members, the work of the Taskforce is greatly assisted by private sector business and community group partners. Taskforce partners all recognise the seriousness of consumer fraud in Australia and are committed to disseminating the Taskforce's message to consumers during the Consumer Fraud Week and more generally throughout the year.

Private sector partners also promote the major messages of Consumer Fraud Week in two ways – externally to their customers and other stakeholders, and internally to their staff. The involvement of businesses and other non-government organisations is a valued aspect of Consumer Fraud Week and an indication of the impact of fraud on many sectors of the community.

Consumer Scams – Some Recent Developments

One of the aims of today's Forum is to gain some insight from experts and practitioners about recent trends around the spread and impact of consumer fraud. By their very nature it is difficult to obtain a clear picture of consumer scams and frauds, not the least because many consumers feel embarrassed if they fall for such scams and therefore fail to report them.

But while it is challenging to get a full picture of consumer frauds, there are some developments in consumer markets that have clearly facilitated the growth of scam offerings. The most obvious is the growth in online communication and online commerce.

- For a start this has dramatically expanded the potential audience for consumer scams. Even while the 'hit rate' of many online scams is low, the ability to reach a vastly expanded audience opens up massive new 'markets' for scams.
- It's not only a mass market that has been been created for scam operators in this way. The internet has also opened up greater opportunities for targeted and specialised commerce – this is the underlying idea of the 'The Long Tail'. This has created new opportunities for scams in areas that would simply not have seen such activity in the past. For example, prior to the rise of the internet the hobby of genealogy (detailed research into one's family history), would hardly have opened up opportunities for widespread fraud. Now with genealogical websites we have seen fraudsters move into this area, trading on people's understandable curiosity and emotional attachment to their family history. This is catching consumers unawares, so their defences are down.
- The web has, of course, facilitated much greater international communication and commerce for consumers. This has been a wonderful boon in many ways, but it has also facilitated the growing internationalisation of consumer scams. At one level this provides the wider audience that I've mentioned above. Importantly this internationalisation also facilitates the interconnection of organised criminal networks and consumer scams, as it allows such networks to base themselves in jurisdictions with less rigorous policing regimes, often in poorer countries, while targeting consumers across borders.

- It's worth noting that while the web has proven to be a remarkable device for spreading information and knowledge this unfortunately also applies to information about criminal activities. Scam operators can learn very quickly about scams in other jurisdictions, they can see what is and isn't working. I am constantly impressed, if that is the right word, at the speed with which scams emerge and spread and then transform to take into account local conditions.
- Finally, as in many walks of life the web has not simply replaced previous technologies but allowed additions and enhancements to many of our day to day activities. This also applies to scams. Telephone and face-to-face contact are still particularly effective ways of carrying out consumer fraud. What has changed is that online material is increasingly combined with other technologies to facilitate the ability of scamsters to create a multi-layered 'story' to trap the consumer.

Some of the key speakers today will be providing more insights into developments and trends with consumer scams. If we're going to protect consumers from scam operators then it certainly helps to understand more about their operations and development.

Global Financial Crisis

I'll turn now briefly to the issue of the financial downturn. This appears to be creating some new opportunities for scams. These opportunities fall into two categories.

1. Scams directly related to the global financial crisis.

For example, both the US and Australia have seen scams emerging that seek to take advantage of government stimulus or support payments. Bogus emails have been sent asking for personal information such as name, date of birth, address and bank details. These have been disguised in the Australian examples as official communication from the Australian Tax Office or Centrelink.

2. An environment conducive to scams

In uncertain economic times, offers of cheap or free holidays, or cheap rental accommodation, may have more resonance with consumers. Small businesses that are facing economic difficulties can also be more aggressively targeted.

The speed with which scam operators can adjust to changing conditions means that we now see scams emerging as a matter of course in response to exceptional circumstances – the scam charity collectors in the face of the recent bushfires have been an unfortunate example of this phenomenon. So we expect to see more scams in the face of exceptional events or circumstances, and the global financial crisis is obviously a very significant economic event in all our lives.

What can we do in response?

As my comments indicate, consumer frauds and scams are constantly evolving the face of new technologies and economic circumstances. How can best combat these consumer frauds and scams?

This will be one of the key themes of today's Forum, so I'll simply make a few brief comments.

One major point is that combating the operators of consumer frauds and scams is a task that requires *cooperation* across agencies and in many cases across countries. Disrupting the activities of scam operators will be more effective if it is a multi-pronged attack. In many cases it also desirably involves cooperation with non-government partners such as companies in the finance, online and communication sectors.

As the establishment of the ACFT indicates, regulatory agencies are benefiting from cooperative approaches to consumer education and enforcement. Many of the agencies here participate in the Global internet Sweep-day, in which regulators from around the world "sweep" websites to check for illegal or misleading sites.

Recently the ACCC took action against a misleading website selling high-fashion clothes based on information and advice from our counterparts at the US Federal Trade Commission.

There is no doubt that this cross-agency and cross-border cooperation complicates efforts to combat scams. This is what scam operators explicitly rely on – the challenges of working across jurisdictions and in environments where multiple agencies are involved. But that is also why efforts such as the ACFT are important.

Combating scams also, I believe, requires us to refresh and revamp our approach to consumer education and awareness. And that leads me to this year's Consumer Fraud Week.

Consumer Fraud Week

Our Consumer Fraud Week campaign seeks to increase public awareness of scams and to educate consumers about scams generally and the steps they can take to recognise them and protect themselves from scammers. The campaign will highlight the significant costs to consumers and businesses that arise from the activities of scam operators, and the need for a broad-based approach to combat these scams.

There are two related themes for the 2009 Consumer Fraud Week

- Scams target you
- Protect yourself from scams

Let me say a few words about the first theme, which has been a message for some time from the Taskforce. It's a strong message to consumers that *anybody* can become the victim of a scam, including online.

I am constantly surprised at the ingenuity and sophistication of scam operators. However, I find that often in interviews with media or in talking to consumers in the wider community, there is still the view that all scam operators are dodgy looking guys in dirty jackets, 'amateurish' and easy to spot, or else the authors of the world's worst emails. In this light, too many consumers believe that the only people who fall for scams are the gullible or the careless.

What speakers today will highlight, however, is that scams can hit anyone, from any walk of life, any age and any educational attainment. New technologies and ways of doing business have given scam operators greater scope to create a strong impression of legitimacy and trust around their offerings. Scam operators are in many cases part of highly organised criminal networks.

As I've noted the ABS found that around 1 in 20 adult Australians will be hit by some sort of consumer scam each year. This figure is broadly consistent with findings from overseas. For example the UK Office of Fair Trading found that around 1 in 15 people had responded to a scam. The US Federal Trade Commission found that more than 10% of the adult population had lost money to a scam in a single year. Anyone can and does fall.

This of course does not mean that we should stop engaging in online commerce or ignore the 'phone when it rings. Rather, it's a signal to the community that a vital step to avoid falling for scams is to recognise that it could happen to you.

Conclusion

In conclusion, we all know that combating consumer frauds and scams is a permanent feature of the regulatory agenda. They have always been with us, and always will be into the future. But the scope of consumer fraud and scams in the age of modern communications technology poses new challenges. As the opportunities and choices of consumers have expanded in recent times, so have the opportunities for scamsters.

It is therefore more important that we educate consumers about the risks of scams and provide them with practical advice about how to avoid the traps while going about their daily business. It is important that we work with the media to ensure that we get the message across. It is important we take a cooperative approach involving government agencies, community organisations, academic researchers and businesses to minimise the prevalence and impact of scams. And it is important that we work with our overseas counterparts as the international dimension of scam activity continues to expand.