National Consumer Fraud Week

Opening address

Rod Sims, Chairman

19 March 2012, Sydney

Welcome to National Consumer Fraud Week.

The theme this year is *Slam Scams!,* which is our straightforward advice for consumers who want to ensure they don't get taken in. More on this crucial theme in a moment.

First – why are we all here?

This is the Australasian Consumer Fraud Taskforce's major annual public awareness campaign, and it's a key initiative in helping to fight consumer fraud in Australia, in New Zealand and internationally.

The week is intended as another means for us to get the word out to Australians: protect yourself against scams and slam them! at the point of contact.

So, welcome to everyone: to our 22 Taskforce government member agencies, who come from the fields of consumer protection, law enforcement and research; and to the many Taskforce partners, who come from the public, private and community sectors.

Key events this week – ACCC reports

As part of National Consumer Fraud Week 2012, I am pleased to launch two important publications on scams.

These are intended to inform the public about scams targeting Australians, and the need to be vigilant against scam activity.

One publication is our annual report entitled *Targeting Scams,* which is the ACCC's detailed account of 2011 scam activity and trends. The report draws heavily on information and data gathered when members of the public contacted us to report a scam throughout the year.

The other publication is the ACCC's pocket-sized edition of *The Little Black Book of Scams,* for consumers and businesses. It's the ACCC's most popular publication and exposes scammers' top tactics and how to avoid them.

Our latest *Targeting Scams* report reveals some interesting trends in scams activity targeting Australians.

It shows that in 2011, the ACCC received more than 83,000 reports of scams from consumers and small businesses. That is almost double the 42,000 plus reports we received in 2010, which is extremely troubling.

And, sadly, the total of all financial losses reported to us in 2011 was more than $85.6 million, up 35 per cent from 2010.

These are stark figures, both due to the significant increases, and the fact that the numbers represent ordinary people who have been approached by scammers.

The stories in this report are likely to resonate with many of you because some of these scams start off with what seems like a plausible approach which could catch any of us off-guard.

So this is the backdrop against which we meet today – scams targeting Australians continue to evolve and increase.

I should quickly say, however, that the news in *Targeting Scams* is not all bad.

Of the scams reported to the ACCC, almost 88 per cent of the people and businesses who contacted the ACCC last year, regarding scams, reported no financial loss at all.

That means around nine out of 10 people realised the risk and slammed the scam – they hung up the phone, shut the door, threw out the letter or clicked delete.

It also means that many consumers know they can and should report scams to the ACCC. Whether or not they have suffered financial loss, their reports help the ACCC to identify emerging scams so that we can alert the public.

The ACCC's SCAMwatch website, which last year had a 400 per cent increase in hits, does just this by issuing public alerts on emerging scam threats. In 2011, over 5000 people signed up to receive these alerts directly to their inbox.

Education and enforcement results

Notwithstanding the levels of consumer awareness, as regulators and enforcement agencies, we are bolstering our collective efforts. The events this week are testimony to that.

But there are more recent examples.

- Last year the ACCC successfully prosecuted two companies targeting small businesses with false billing scams. One of these scams falsely led businesses into believing that they were dealing with Yellow Pages, and we achieved a penalty in the courts of $2.7m.
- In another case, last year a group of itinerant workers was scamming home owners on the east coast, undertaking to do building and maintenance work that they never completed, or which they did badly. There were many complaints about the group. The combined efforts of police forces, fair trading agencies, and Customs and Immigration, saw 20 of them prosecuted. This was a particularly good example of the state and territory agencies lead by NSW and Victoria working together to disrupt fraudulent activity. I understand that with the cooperation of Immigration, 18 of these traders have now departed Australia.

- And in online romance and dating – a fast-growing business sector, but one which has been troubled by scams – the ACCC, in collaboration with many of the dating and romance website operators, has provided website guidelines for the industry to protect their consumers from scammers. Michael Schaper, my deputy at the ACCC, launched these guidelines – not surprisingly – last month on Valentine's Day.
- Elsewhere, the Australian Crime Commission, who you will hear from later this afternoon, is leading Taskforce Galilee. It brings together 19 agencies, including the ACCC, to target 'boiler room' fraud. Those are frauds that solicit investments in firms or other schemes that either don't exist or are worthless.

This is all good work in raising public awareness and enforcing the law. We must keep it up.

But we must also ensure we keep pace with both the number and type of scam activity. Where with fast changing technology and new applications vigilance is more important than ever.

I will briefly underline one of the trends we are seeing in scams, to which we must remain alert.

Specifically, this is the scam that seeks to exploit the name of a recognised company or government agency, which is perpetrated over the phone, and which easily operates internationally. It goes something like this.

Out of the blue, someone calls you at home, or at your small business. They say they are from one of the big computer firms or telecommunications service providers; it's a company name that you are sure to recognise.

Already you relax your guard a little.

It's a very personal approach and one I have experienced myself. They talk you into providing remote access to your computer, because they say it is experiencing technical problems, is infected with a virus, or is sending error messages. They convince you that they need to run a scan to diagnose the problem.

They might convince you that you need some type of security software and will direct you to a website where you are asked to enter your credit card details and other sensitive personal information in order to get the software.

But – and here's the scam – they are actually hacking into your computer, stealing information, and possibly stealing directly from your credit card account.

I should note that Taskforce partners Microsoft and Telstra, which are two companies that have been exploited in this scam, have been active in warning people of this scam.

But, of course, the scammers can morph their identity quickly, using another company or government organisation's name in a few days time.

Consumer message for National Consumer Fraud Week

Our message for consumers this week – in National Consumer Fraud Week – is very simple: if you suspect something is up, the best technique is not to engage.

Our slogan is this:

- If you receive a scam, slam it! Press delete, throw it out, shut the door or just hang up.

Your chances of becoming a victim fall steeply if you don't open the email, don't take the call, or don't respond to the letter.

Conclusion

So, once again – thank you for coming. It's pleasing to see so many people here, and to be able to report on examples of outcomes that protect consumers, and on enforcement efforts that have led to prosecutions or other outcomes before the courts.

Now I'd like to introduce my colleague, Dr Michael Schaper, the Deputy Chairman of the ACCC and Chairman of the Australasian Consumer Fraud Taskforce.

Michael will lead a storytelling session where some key representatives will speak about their experiences and responses to scams.