 	**Address to Chamber of Commerce and Industry WA** ***How business owners should protect themselves against business scams*** **Dr Michael Schaper** **Deputy Chairman** **21 April 2009, Perth**

1. Introduction

Thank you for the invitation to discuss an issue that should be in the forefront of all business owners' minds.

Many Australians – including some business owners – believe that to become a victim of a scam you have to be gullible, lack commonsense or be plain stupid.

However this is far from the case. Scammers are becoming more sophisticated. They are adapting to the changing circumstances in society and are remarkably persistent.

The lengths that scammers will take to build relationships with their victims sometimes astound me. I'll provide some examples of this shortly.

The ripest time for scammers is during tragedy and economic instability. They seek to prey on the most vulnerable and will continually look for opportunities to take advantage.

For example, at the ACCC we warned Australians to be careful when donating money to aid the victims of the Victorian Bushfires earlier this year. We learnt from the Canberra bushfires in 2003, that fraudsters had no problems stealing money from those who needed it the most.

The current global economic downturn will undoubtedly see an increase in scams and there is anecdotal evidence that this already has occurred.

There was a 60 per cent increase in scams reported to the ACCC in 2008 compared to 2007.

According to an ABS 2007 survey, nearly 6 million Australians were targeted by scammers with about 800,000 falling victim to scams. During the same period, it was reported that Australians lost close to $1 billion to scammers. [1]

According to estimates from the Office of the Victorian Small Business Commissioner, nearly $3 billion each year is lost from small businesses across the nation to scammers.[2]

As you can see, the prevalence of scams is becoming more common and has already drained a substantial amount of money from the Australian economy.

As my fellow Deputy Chair Peter Kell noted earlier this year, a likely explanation for the growth of scams is the internet. Although facilitating international communication and commerce for Australian businesses and consumers, the internet has also been a boon for scammers.

At one level, scammers have a much wider audience than previously before as they are no longer constrained in any one country's borders.

At another level, internationalisation provides scammers with organised criminal networks and allows them to be located in jurisdictions with less rigorous enforcement regimes, particular in poorer countries.

This makes it all the harder to bring scammers to justice and usually once the scams have been successful, it is extremely difficult to recover the money lost. However in saying this, the ACCC will continue to pursue scammers and where possible bring actions against them. But the vigilance of scammers is endless and as soon as one scam is shutdown, a similar one emerges.

As the old adage says, prevention is much better than cure. I'll now outline some of the common business scams, their characteristics and provide you with some real life victim stories.

I'll then provide a checklist to protect your business against scammers.

Let me say at the outset, scam prevention should form part of your business plan and be in the back of your mind at all times. The fight against scammers is a continuous challenge and your business must be prepared.

2. Common business scams

There are four types of scams that commonly target businesses.

These include:

---

[1] Australian Bureau of Statistics, 4528.0 Personal Fraud 2007, http://www.abs.gov.au/AUSSTATS/abs@.nsf/Latestproducts/4528.0Main%20Features12007?opendocument&tabname=Summary&prodno=4528.0&issue=2007&num=&view=

[2] Office of the Victorian Small Business Commissioner, 'Beware of frauds, scams and swindlers – small business warned', 6 March 2009, http://www.sbc.vic.gov.au/press_releases_more.asp?pressReleaseID=9

- overpayment scams;
- false billing scams incorporating directory listing/ advertising and domain name scams;
- phishing and spam scams; and
- questionable franchise scams.

2.1 Overpayment scams

In this type of scam, scammers commonly pose as legitimate buyers replying to online advertisements/classifieds as well as newspaper classifieds. The scammer will then send a cheque/money order or credit card payment for more than the agreed price.

The scammer hopes that the unsuspecting victim will simply 'refund' the excess amount or more commonly pay a freight company linked to the scammer before the scam is discovered. Scammers have also been known to use these tactics in trying to make accommodation or restaurant bookings.

Let me give you a case of an international money transfer scam which targeted Lynne's bed and breakfast, a small business in South Australia:

Lynne was pleased to receive a booking request from Indonesia. The request came via Lynne's website and claimed to be from a travel agency in Kuta, Bali. They wanted to book a two-week stay for two couples, their 'Japanese clients'.

Emails were sent back and forth over some weeks to organise details and costs. The travel agent didn't seem to mind what dates were available and they didn't hesitate to agree to the first price offered by Lynne. The travel agent from Bali even agreed to pay the full amount in advance with their Japanese client's credit card. They asked what there was to see in the area, but didn't appear very interested in any details.

Lynne suggested that the Japanese couples pay via PayPal, but the travel agent claimed they couldn't use it, and instead sent the Japanese couples' credit card details via email. When Lynne tried to process the booking, the credit card transaction was declined by the bank.

Lynne said 'in hindsight, the most suspicious factor was that the supposed travel agent wanted the Japanese clients to pay us the total amount, and then wanted us to pass on the commission to the agent'.

The scammers had used credit card details stolen from Japanese tourists who had been travelling in Bali. They were hoping that Lynne would send the 'commission' to them following their fake booking.

Lynne said: 'It was interesting how elaborate the whole scheme was. Some of the emails from the scammers pretending to be from the Japanese couple were lengthy and spoke more about themselves and their relationship with the travel agent, trying to justify their connection'.

Although, Lynne didn't lose money to this scam, there are plenty of businesses around that may have.

The next scam I'll discuss involves false billing.

2.2 False billing

False billing scams aim to collect money with no return, or strong misleading or deceptive conduct where a product is provided but has little to no value.

The conduct involves tricking businesses into paying for something that they did not want or did not order. Scammers will either use phone, fax, mail, email or a combination of these when targeting small businesses.

False billing scams come in various guises including:

- directory listings/advertising;
- office supplies; and
- domain names.

2.21 Directory listing/advertising

Directory listing/advertising scams stem from requests for payments for advertising in spurious magazines, trade journals or internet directories that sound legitimate or actually exist but are not well renowned. Correspondence from scammers usually is sent via letters often disguised as invoices.

Alternatively, the scam might come as a proposal for a subscription disguised as an invoice for an entry in a bogus international fax, telex or trade directory.

You may also be led to believe that you are responding to an offer for a free entry but in fact, the order is for entries requiring later payment. Another common approach used by scammers is to ring a firm asking to confirm details of an advertisement that they claim has already been booked.

The scammer might quote a genuine entry or advertisement your business has had in a different publication or directory in order to convince you really did use the scammer's product.

If you refuse to pay, the scammers may try to intimidate you by threatening legal action.

Let me highlight a real life directory scam that occurred in South Australia:

A hairdresser in Port Augusta contacted the ACCC about a fake invoice she had received for an advert in a business directory. She initially sought further information about the advertising rates and the distribution of the directory, but was then distressed to learn that her enquiries were assumed by the company to be a confirmation of the placement of an advert.

When she refused to pay for something she had not ordered, she was threatened with legal action seeking payment and legal fees on more than one occasion.

At this point the hairdresser was unsure of how to deal with this intimidating situation. She didn't have the resources to fight a legal battle, and her first impulse was to pay-up to avoid any more confrontation.

Fortunately she had the good sense to contact an officer from the Adelaide office of the ACCC who was able to assure her that it was a breach of section 64 of the Trade Practices Act for businesses to assert a claim for payment for unsolicited goods or services. We advised her it was therefore highly unlikely they would ever be taken to court for the false listing.

The ACCC has taken action against companies engaging in false billing.

In **Australialink Pty Ltd,** it was alleged that misleading or deceptive conduct occurred in the way that directory listings were solicited as well as the use of notices that purported to be official court forms in pursuit of payment for those listings.

The ACCC took action against Australialink and secured court enforceable undertakings constraining them from in engaging in this conduct.

2.22 Office supplies

Like the advertising/directory scam, scammers will send invoices for office supplies that were not ordered. Such examples include paper, printing supplies or maintenance.

You might receive a phone call from someone claiming to be your 'regular supplier', telling you that the offer is a 'special' or available 'for a limited time only'.

If you agree to buy any of these supplies that are offered by you, they will often be overpriced and of bad quality.

2.23 Domain names

Similarly, domain name scams begin with businesses receiving invoices or an unsolicited letter for a domain name that closely resembles that already owned by the business. The business is tricked into paying for a new, unwanted domain name.

It's time for me to explain some examples of phishing and spam scams.

2.3 Phishing and spam scams

Phishing scams can occur via phone or email. Both involve tricking unsuspecting victims into providing important personal information about themselves and their businesses including banking details.

Through the use of copied logos or banners, phishing emails are designed to look as though they have been sent from banking or financial institutions, well-known companies such as employment services or government agencies. The email usually links to a fake webpage where personal details are recorded and then skimmed by the scammer. In some cases the links may lead to an unwanted download onto the computer making it vulnerable to spyware.

Where phones are used, scammers commonly pose as staff from the above mentioned organisations to gain people's trust. Personal information, such as bank account numbers, passwords and credit card numbers, may be used to steal money and identities.

Spam scams are a common feature in today's email inboxes. Particularly vicious are those that are designed to get the recipient to click on a link or an attachment with the intention of loading malware onto that computer.

Recent examples that pose threats to businesses have been emails that purport to have a plane ticket or invoice attached. Once these are opened an unauthorised download attacks your computer. This allows the scammer to remotely log important details or use the computer to participate in furthering the scammer's activities.

The final scam I'll discuss today involves questionable franchises.

2.4 Questionable franchises

Scam franchise opportunities usually offer investors the chance to join a 'proven system' that requires minimum effort, experience or skill. These scams usually promise a risk-free investment with immediate high returns, but then don't deliver.

Unsuspecting franchisees are then invariably left in a position where they cannot succeed, regardless of how much effort they put into the business.

The false promises may be made in advertisements, seminars or workshops where the incentive of a special 'join today' bonus may be offered to induce people to sign up on the spot.

The scammers may misrepresent the franchise earning potential, ease of operation, success of existing franchises, initial outlay and the training and support that will be provided to the franchisee.

Let me highlight the franchise scams of Bon Levi and the devastating effects it had on some small business investors.

Mr Levi sold various distributorships for snack foods, cookies and fruit juices under the 'Little Joe' and 'Joey's' brands. Each was sold for more than $30,000.

Mr Levi made various claims to prospective franchisees in newspaper advertisements and at trade shows, including:

- *that each distributor would receive a guaranteed income week for five years after an initial paid training period;*
- *that Mr Levi would conduct a national TV, radio and magazine campaign promoting the businesses*
- *that the distribution agreement was not a franchise - in an attempt to avoid his obligations under the Franchising Code of Conduct.*

However, Mr Levi failed to disclose to prospective franchisees that he:

- *had carried on business under other names;*
- *had been jailed for three years in the United States for selling fraudulent business licences to distribute snack foods;*
- *had no real experience in, or knowledge of the business he was selling; and*
- *was on bail pending trial for numerous counts involving dishonesty.*

The ACCC successfully took action against Mr Levi for breaches of the Trade Practices Act including breaching the Franchising Code of Conduct pursuant to section 51AD; and engaging in false or misleading and or deceptive conduct as per section 52.

The Federal Court ordered that Mr Levi could not sell a business opportunity unless he either:

- *had run the business successfully for at least six months; or*
- *provided a copy of the court orders and certain information about his business experience and aliases to the purchaser.*

Despite these orders, Mr Levi continued to sell businesses, including snack food distribution, LPG conversions and Bikini Girls Massage businesses.

In return for $36,000 to $66,000, Mr Levi promised to set up the businesses and pay guaranteed weekly incomes. None of these businesses were ever established and, as a result, investors lost all their money.

The ACCC successfully took action against Mr Levi for contempt of court, and he was sentenced to 10 months' imprisonment with 6 months suspended.

Now that you have heard about the various scams, I'll provide you with a checklist to help protect your business from being scammed.

3. How to identify scams – the warning signs

The first line of attack is that you must be on the lookout for scams and be able to identify them.

Although the warning signs depend on the specific scams, here are some general tips for business owners:

- If the offer sounds too good to be true, it probably is;
- You have been asked to 'verify' or 'confirm' personal details - such as account numbers, passwords - via email or on the phone;
- The caller pushes staff to provide personal or corporate information and discourages them from checking if it's a genuine request;
- Your business receives unsolicited invoices for goods/services that you did not order.

Here are some specific warnings for franchises scams:

- claims you can make large amounts of money quickly and with little effort or experience;
- a reluctance from the franchisor to provide sufficient details of existing franchisees;
- franchisors who are reluctant to provide any written information;
- a requirement that payment be made upfront before any information is released;
- inconsistent financial information about the business' profitability; and
- a franchise advertised with only a post office box as identification.

4. What measures can businesses implement to fight scams?

Business owners can take active measures to reduce the risk of being scammed.

The ACCC advises businesses to follow these simple golden rules -

Always:

- read everything carefully. Don't be afraid to ask for an explanation of anything.
- seek professional advice if the request involves significant money, time or commitment;
- check that goods have actually been both ordered and received before paying an invoice;
- check accounts regularly to ensure that transactions are genuine;
- be wary of anyone using multiple credit cards to pay for goods;

- keep a list of all regular providers, including any renewal dates for easy reference;
- ensure that all computers have up to date protection from viruses and other malware A good spam filter will also assist;
- ensure that all business computer hard drives are backed up daily;
- in relation to major business transactions, always carry out due diligence and seek independent advice.

Now I'm going to list some things that business owners and their staff must not do.

Never:

- have a large number of people authorised to pay invoices. Keep a tight control over who pays invoices and ensure proper communication to weed out false invoices;
- accept a payment for goods/services for more than the agreed price. Send it back and ask the buyer to send payment for the agreed amount before delivering goods;
- give out or clarify any information about their business unless you know what that information is being used for;
- agree to anything on the phone – always ask for it in writing;
- click links in unsolicited emails. If asked for personal details or an update for account details, contact the business to confirm. But do not use the contact details in the email, get the information from an independent source, such as the official website or phone listing.

Unfortunately, there will be times when scammers are victorious. I certainly hope this does not happen to you but if it does, please immediately take the following advice.

5. What should businesses do if they have been scammed?

You should report the scam. Although it may be embarrassing, reporting ensures that the relevant authorities are aware of the scam and this could help prevent other businesses from becoming victims.

Contact:

- the appropriate bank/financial institution, if applicable;
- the police; scamming is nothing more than fraud and is a crime;
- the SCAMwatch website – www.scamwatch.gov.au – to report the scam.

Let me now outline the various measures that the ACCC is undertaking to help businesses protect themselves against scams.

6. The ACCC's work in fighting scams

The ACCC implements numerous strategies to educate Australians, including business owners, about common and emerging scams and provides advice on avoiding scams.

SCAMwatch website

The purpose of SCAMwatch is to provide information to consumers about scams that commonly target Australians. Real life scams have been included on the website to assist Australians and businesses in identifying and avoiding scams.

Australasian Consumer Fraud Taskforce

The ACFT consists of 19 government agencies, including the ACCC, with responsibility for consumer protection against scams. Each year, the ACFT runs a campaign to raise awareness about the increasing dangers of scams and the steps consumers can take to protect themselves.

Publications

*T*he ACCC has released 3 scam fact sheets: money transfer scams, lottery, sweepstakes and competition scams and phishing scams. Additionally we publish *The Little black book of scams* which highlights a variety of common scams that regularly target consumers and small businesses.

7. Conclusion

As I have highlighted today, scams are fast becoming a regular occurrence in Australia.

Scammers are now targeting businesses constantly with innovation, persistence and cunning in order to gain trust and manipulate their victims.

It is vital that businesses factor in scam awareness and prevention in their activities and are ever vigilant in the fight against scams.

This is an ongoing battle and if your business has any weaknesses, the scammers won't be far away trying exploit this and steal your details and money.

If you have any questions or require further information about scams, please do not hesitate to call the ACCC on 1300 302 502 or visit the SCAMwatch website – www.scamwatch.gov.au.

Thank you.