Taking Charge of Your Money

Scams: recognising and avoiding them

An address by Professor Berna Collier

Commissioner

Australian Securities and Investments Commission

The Australian Investors' Association and

The Courier-Mail Seminar

Saturday 19 November 2005

Brisbane Convention & Exhibition Centre

Thank you for inviting me along to speak with you today.

Before launching into my presentation for tonight I thought I might say a few quick words about ASIC. I hope that you will feel free to get in contact with us if there are issues you want to discuss or you see things happening in the marketplace which cause you concern and which you believe ASIC ought to be aware of.

- ASIC, as I'm sure you know is the companies regulator and the consumer protection regulator for financial services.
- We provide consumer protection regulation in relation to superannuation, life and general insurance, banking products and shares and managed investments.
- We don't have responsibility for regulating property advice (although this is an issue governments are currently looking at) nor, on the whole, do we regulate credit beyond our general consumer protection powers.
- Finally, we use a variety of tools to do our job, including enforcing the law, giving guidance on compliance, promoting law reform and educating consumers so they can make informed decisions that are in their best interests. Today's talk falls squarely under that education role.

Scams and how to avoid them

No matter how experienced an investor you are – we all share a common goal.

Aim of every investor

Not to lose all (or any) of our money in a scam

At ASIC we see an almost never-ending range of scams from the outright illegal and fraudulent to those that skate on the edge of the law and seek to appeal to the gambling/dreaming nature of so many Australians. We have one clear consumer message that covers them all:

The Golden Rule

If it looks too good to be true then it is probably a lie.

Unfortunately though – our actions as consumers don't always follow our brains. In the ANZ survey of financial literacy in Australia it was found that:

Actions don't follow knowledge

- While 85% of people knew that high returns equal high risk, 47% of respondents still said that they would be prepared to invest in a product that was advertised as being "well above market rates at no risk".

We conservatively estimate that over the last financial year, more than 2,150 investors invested a total of around $220 million. That is a lot of money. We closed down 76 of them and obtained protective court orders in many other matters pending further action. A further five promoters of illegal investments are in jail serving sentences imposed in the 2004-05 financial year for dishonesty associated with the investments they offered.

Here in Queensland, there were 480 investors who invested $56 million.

ASIC is therefore putting a lot of effort into educating people how to avoid such scams.

Beyond the golden rule that **if it looks too good to be true then its probably a lie,** there are some common hallmarks to today's scams:

Scam indicators

- They often look real
    - They print attractive documents and set up business like web sites
    - They choose names that sound like reputable companies
    - They tell persuasive stories using the right jargon
    - They drop names of people you know to build trust
    - They may belong to a group you are involved with ie affinity fraud – for example a church or sporting group. This is becoming more common in Queensland. The Wattle scam was spread by social groups and networks (including the AFP!)

- Other common clues include:
    - They offer bigger faster profits than other investments. Some offer 20% per year – others go to 300%. It's too good to be true. By comparison, Australian shares are some of the most successful investments and their value has grown about 7 – 9 % over the long term.
    - Scams are also often sold as involving less risk and less effort than real investments. Eg insider information, new techniques such as new share trading software.
    - Scams are also often offered by strangers - whether cold calling you from overseas or promoting seminars. While people can sound genuine, they rarely have real credentials such as an AFS license to give advice or sell financial products. Often these calls discuss shares in companies that have familiar sounding names.
    - Scams are also usually more urgent than the real thing. "Don't miss out", 'act quickly', 'this week only'. They want your money before you have a chance to change your mind or do some proper thinking. And this leads to our second golden rule –never sign anything on the night.

How to protect yourself

Obviously it's easy to be fooled. So, how can you protect yourself:

- Always use Australian businesses that have an AFS licence to sell financial products or give financial advice. Check if they do for free on our consumer web site - FIDO or by calling our Infoline on 1300 300 630.
- Take your time before investing your money.
- Research all investments and only get involved if you understand the offer.
- Make sure you are comfortable with the risks, especially if you are borrowing to invest. REMEMBER – the higher the return, potentially the riskier the investment.
- Get information or advice only from reputable people – use licensed financial advisers or genuine educational organisations such as the ASX, Securities Institute or Centrelink's Financial Information Service.

- Remember the basics of investing:
    - Align your investments with your investment objectives
    - Improve your financial skills and knowledge
    - Surround yourself with a team of excellent advisers
    - Diversify your investments; and
    - If something sounds to good too be true it's probably a lie.

But onto the scams themselves. We find that there are trends in scams. Some that we have been seeing a lot of over the last few years are:

- Cold calling
- Wealth creation seminars, including those run by property spruikers;
- Share trading software;
- Unsolicited offers to buy your shares
- Phishing
- Nigerian Scams

Cold Calling

Cold calling as I'm sure most of you know is when overseas cold calling operators make unsolicited phone calls, falsely claiming to be large international brokers offering shares in overseas companies to Australian consumers. Although typically based in Asia, most operators are not Asian nationals. They make false promises about the investments and use fake 'props' such as expensive documentation, websites and couriers to convince investors of their legitimacy. Their tactics are relatively sophisticated compared to things like the Nigerian letters scam but they are just as fraudulent and just as illegal and, unfortunately, people seem just as likely to fall for them.

Investors receive near worthless and/or restricted shares, or no shares at all. Once investors' money leaves Australia, it is almost impossible to recover. The operators are elusive, using 'virtual offices' to mask their true size, purpose and location. That said, with cooperation from overseas regulators we have managed to shut down some.

ASIC is still getting a steady stream of complaints about cold calling. We believe that well over $400 million has been lost by investors.

A large percentage of those who lost money were experienced share traders who thought they knew what they were doing. And worse still, we know that lots of people are too embarrassed about being duped to tell anyone so we suspect real losses are much higher.

Phone scams checklist

So, our tips if you are cold called:

- Ask the right questions ie name, address, telephone number and whether the caller holds an AFSL licence
- Just hang up if you are suspicious
- Don't make decisions over the phone – you should always take time to check; and
- Check ASIC's list of known cold callers on our consumer website – www.fido.gov.au We update it regularly. But, remember, just because your caller isn't listed doesn't mean they are legitimate.

Wealth creation seminars

You have probably all seen ads for investment seminars that claim:

- You can be a millionaire in three years
- Traditional investments are too slow and lack excitement
- Turn your financial dreams into reality
- Amazing, fabulous, unbelievable strategies for building massive wealth

As I'm sure you know – you need to be very careful about these sorts of seminars. Our concerns about them include:

- They are overpriced and poor value for money – we have seen seminars that charge $10,000 plus, and worse still, people are borrowing to attend or putting them on their credit card
- They may make misleading and deceptive claims
- They push strategies that can be financially dangerous; or
- They promote outright scams.

ASIC can take action against misleading and deceptive claims and ensure that unlicensed financial advice isn't given at these seminars but we will never stop them all. Our most effective regulatory tool is to educate consumers not to attend.

Some of the things to look for in a seminar before attending and some of the things to watch out for including:

- Secret techniques
- Rags to riches stories; and
- 'free' seminars designed to sell expensive follow on seminars (and I should tell you, we have heard some horror stories about the psychological strategies they use in these free seminars to ensure success. Things like having the whole group chant at the non-registers – loser, loser).

Consider obtaining an investment plan from a qualified person instead!

Share trading software

Sales of sharetrading software appear to be on the rise. ASIC is concerned that as real estate prices steady or decline, trading software is becoming the new area where consumers are sold a promise that is too good to be true. Increasingly, these software products are being marketed through direct mail, the internet and get rich quick seminars.

Our experience is that these products are rarely, if ever, able to fulfil the extravagant claims made for them. The claims are that very large returns, in both dollar and percentage terms, can be achieved for minimum effort. The software is generally of a

black box nature such that it is difficult for consumers to assess what value it might have and what service it can provide.

Many providers don't have a license which means they can't lawfully provide advice. This means that *buy sell* recommendations can't be made. This leaves relatively little scope for software to provide a useful service to consumers wishing to trade in the market. This limited service, however, is not reflected in the price, which can be as high as $15,000.

ASIC has taken successful enforcement action against providers either for providing financial products without a license or being misleading in claims made. However such litigation is costly, technically difficult and time consuming. One of our focuses going forward is to try and increase consumers' understanding of these products and reduce their vulnerability to extravagant claims.

So our tips to you on share trading software:

- Ask yourself if you really need a computer trading program?
- Learn the basics of investing before buying. Consider enrolling in an ASX or Securities Institute course
- If you still want a program, find out what it does before purchase; and
- Shop around for reputable providers who are licensed by ASIC

Unsolicited offers to buy your shares

Since late 2003 there has been a wave of unsolicited offers to buy shares at well below their market rate. In mid 2003 the Government moved to prevent this type of behaviour by requiring a person who makes an unsolicited offer to buy your shares off market for a certain price to give you:

- A written statement setting out the market value of those shares on the day the offer is made; and
- A minimum of one month to accept the offer.

Unfortunately, despite the new law, we are still seeing unsolicited offers being made at well below market rates.

When assessing an off market offer to buy your shares its worth making a few safety checks:

- First, who is making the offer. The offer may not come with the normal investor protection you get when you sell through a licensed broker or authorised exchange.
- Check the up to date market price for your shares. While any offer you receive must quote the current market value, it may be out of date.
- Ask yourself why the offer is being made. Naturally the person making the offer wants to make money. For shares traded on the Australian Stock exchange, check the exchange for announcements or talk to a stockbroker in case you have lost touch with important news.
- Also think about whether you really want to sell. Unless you really need the money now you may do better by holding on.
- Compare the cost of selling on the market and be careful to read the offer to see if you must pay any fees or charges.
- If you hold unquoted shares you will need to make a personal judgement about what they are worth. As a shareholder, you are entitled to talk to the company you own the shares in about its plans, including possible listing on an exchange. Also, consider seeing a licensed adviser who knows about valuing unquoted company shares.
- If you are still tempted by a below market offer, remember there are really only a few cases where accepting the offer makes sense:
    - You have compared all costs carefully and you will end up with more cash if you accept the offer;
    - You need to sell now and your quoted shares have been suspended from trading or you hold unquoted shares that no other shareholder wants to buy.

Phishing

An all too common scam is Phishing. I'm sure most of you are aware of it. It's where you receive emails which use a range of pretexts such as 'security and maintenance upgrades', 'investigation of irregularities', or 'bills and charges due' to get you to email your private details such as your access code for internet banking.

These scams are inevitably linked to fake websites that look like the real thing, especially bank sites with the right logos and branding and copies of genuine pages but with slightly different addresses. Most banks have now experienced such frauds and are taking action to warn consumers about them. You will see these warnings on the bank web-sites and on the ABA home page.

For customers who do get caught up by such scams there are protections in place through the EFT Code and banks have been reimbursing all money. That said, here are 6 rules for safer internet use:

- Use your pin only through the official log in site. Keep your site in your favourites folder and log on that way.
- Check official websites for announcements.
- Use only secure sites for keying in financial or personal information – look for a padlock icon at the bottom of your web browser.
- For Australian sites, look for the '.au' domain such as 'com.au' or 'net.au'. Anyone registering an .au domain must first show a link between their proposed URL and an Australian trading identity.
- Take a few privacy precautions – where possible avoid banking or shopping at internet cafes and other public facilities and keep private information out of chat rooms or email.
- Finally, act quickly if you have been conned – if you are worried that you have sent details through a suspect email or website, contact the bank, credit card company or business straight away.

Wrong number messages on your answering machine

The scenario is this. You come home from work and check your answering machine and there's a message waiting for you. It's from someone you don't know, obviously a wrong number, but in the message the caller tells her friend about a hot investment tips she's received.

Would you buy some stock in a company on the basis of a call like this, from someone you don't know?

Seems unlikely doesn't it, but that's exactly what's happening in the US right now, and if past experiences are repeated, it could happen here too.

What the US authorities have been saying is that if you get a call like this, its most likely not a wrong number at all, but part of what is known as a 'pump and dump' scam. In the US, people are employed to leave messages like this on thousands of answering machines across the country. What the scammers behind this scam are trying to do is to influence people to buy stock in a company that they invest in, causing its share price to rise. The scammers then sell their shares at a profit and, once they stop promoting the stock, its price falls and many investors lose their money. Scammers choose stock that is only thinly traded and little is known about, so its share price is easily manipulated.

ASIC's advice — never put your money into shares on tips from people you don't know.

Nigerian Scam

This venerable old scam is over 50 years old and has proliferated further than ever by the use of e-mails.

Even as I read this, the world famous Nigerian Scam (also known as a "4-1-9" or "Advance Fee Fraud" scheme) is parting yet more of the 'something for nothing' crowd from their money.

Here's how it works: Letters (or, nowadays, e-mail messages) postmarked from Nigeria (or Sierra Leone, or the Ivory Coast, or almost any other foreign nation) are sent to addresses taken from large mailing lists. The letters promise rich rewards for helping officials of that government (or bank, or quasi-government agency or sometimes just members of a particular family) out of an embarrassment or a legal problem. Typically, the pitch includes mention of multi-million dollar sums, with the open promise that you will be permitted to keep a startling percentage of the funds you're going to aid in squirreling away for these disadvantaged foreigners.

If you're not saying "scam" by now, you should be. Should you agree to participate in this international bail-out, something will go wrong. Paperwork will be delayed. Questions will be asked. Officials will need to be bribed. Money from you — an insignificant sum, really, in light of the windfall about to land in your lap — will be required to get things back on track. You pay, you wait for the transfer . . . and all you'll get in return are more excuses about why the funds are being held up and assurances that everything can be straightened out if you'll just send a bit more cash to help the process along. Once your bank account has been sucked dry or you start making threats, you'll never hear from these Nigerians again. As for the money you've thrown at this, it's gone forever.

FIDO (www.fido.gov.au)

Finally today, I want to give a plug for our consumer website – FIDO (and there are some postcards with its address on it down the back). If you haven't discovered it you should, as it really is an invaluable resource. Just some of the things you can find on it include:

- An unclaimed monies directory where people can find money they have forgotten about in old bank accounts, shares and matured life insurance policies. FIDO also includes a link to the ATO's lost members super register where there are billions of unclaimed dollars in millions of lost–member accounts.
- As I mentioned earlier, it contains lists of known cold callers who try to con people into buying worthless shares

- Warnings about scams and swindles
- Our superannuation fee calculator that helps you work out and compare the long term impact of fees
- A budget calculator/planner and budgeting tips
- A managed funds fee calculator to help you work out the true cost of an investment
- A credit card calculator
- A DIY Statement of financial position
- Advice about a myriad of topics including all types of financial products from selecting a credit card to purchasing shares and selecting a financial adviser
- Our Super Choices Booklet and information
- Consumer Publications

Conclusion

Thank you for listening today and remember – if is sounds too good to be true then its probably a lie and – don't sign anything on the night.

Also, please remember, if you are concerned about practices you are seeing in the market place, please don't hesitate to get in contact with us

Thank you.