

SWINDLES, SCAMS AND STINGS PANEL DISCUSSION

Louise Sylvan, Deputy Chair of the Australian Competition and Consumer Commission.

Col Fry, Australian High Tech Crime Centre – Col.

Russell Smith, Principal Criminologist, Australian Institute of Criminology.

Delia Rickard, Director, Office of Consumer Protection, ASIC

Louise Sylvan:

We're going to be talking about scams and frauds and what is called global low value high volume economic crime. This kind of set of scams and the global nature of them and so on kind of happened to us if I can put it that way. It came in under the horizon of a lot of the regulators who were watching this sort of stuff. Now we decided to all get together the lot of us into a task force, the Australasian Consumer Fraud Task Force, I'm really actually wearing the hat this morning of chair of that. And three members of the task force today are going to try to paint a picture of where we are in Australia with these frauds and scams.

The task force consists of and I think that the Parliamentary Secretary mentioned a bit about it this morning, it consists of the eighteen regulators and policy departments in Australia and New Zealand that have remit for consumer protection in one way or another and they're joined by the nineteenth member which is the representative of the States and Territory Police Commissioners. The group, there's a number of them conducting research through the Australia Bureau of statistics, it's got a prevention group looking at how this stuff can be stopped. The main thing that you'll probably see is the campaign that we do each year. It's a four week campaign. It's happening at the moment, so lots of media is talking about it and this year the four weeks of the campaign are targeted at protecting your money which was last week, protecting your phone which is on at the moment, protecting your computer which is next week and protecting your identity which is the fourth week of the campaign.

And the point is to have not only government saying the same thing but we're joined by forty private sector partners who are also saying the same messages and also another forty community and consumer groups saying the same thing. The point is to get millions and millions of messages out there that are identical, happening at the same time from a whole variety of trusted sources in the hope that we can get through because enforcing against this global fraud is actually quite difficult. So today three of the task force members are going to try to paint the picture for you in Australia and our first speaker is going to be Russell Smith, the Principal Criminologist from the Australian Institute of Criminology.

Russell Smith:

Thanks Louise, and unlike Bernard I'm not going to tell you about all the other Russell Smith's that there are other than just to say one I think is a rugby coach, there's a bass baritone opera singer in Tasmania and 1 guy from customs that I keep bumping into at fraud conferences. Sorry fraud is this one. There we go, more statistics. I thought I'd start by telling you what we don't know about scams, swindles and stings.

This is a chart of recorded fraud offences that the police collect over my lifetime since the 50s. You can see that there's been a gradual progression over many years with interesting developments in the mid-80s which I'm going to analyze at some point when I get a minute to

see why that happened. But unfortunately we don't have a similar chart which shows us consumer fraud incidents. This is all fraud in Australia and we really don't know what's happening with mass marketed scams and scams that target individuals. Transitions a bit slow here. Strange. There we go, that's it.

A quick snap shot of different types of swindles, scams and stings. As we heard there are many different types in fact as many as you can imagine I guess. This is four fraud categories that we devised some time ago. Advance Fee Schemes I guess is the largest category that includes such things as pyramid schemes, Nigerian emails, business opportunities. They're all trying to extract an upfront payment from you so that you'll hopefully get a larger payment in the future which of course never arrives. Non-delivery and defective products and services, buying something that isn't really what you anticipated, there's some defect or in fact the goods and services don't arrive at all.

Online you see lots of examples of these such as health scams, online auctions is a particular area of concern in recent times. Unsolicited, unwanted goods and services - I suppose most come in the form of spam email. A lot of securities and investment fraud fits into that category. And most recently the worrying category of identity related crime and this is people manipulating individual identifying information so that they can perpetrate a wide range of other scams and in fact some of the proceeding categories are carried out using aspects of identity fraud. Phishing where people devise phony websites to trick you into disclosing your personal information is a recent form of that. If we look at some statistics from the ACFT agencies these are the sorts of scams that are most prevalent at the moment.

Lottery advanced fee scams are probably leading the pack at the moment followed by pyramid and chain letter scams. These are traditional ones which have been around for a very long time and are now being adapted to the electronic age. Very recent increase and worrying from many perspectives is the use of scams which are trying to get you to loan your money. They say that they are work from home schemes but in fact they're really just trying to get you to use other people's money and disguise the money trail.

There is Nigerian scams of course most of which are probably not coming from Nigeria, they can come from all around the world and in fact there is a number of enterprising Australians who have been using the exact same strategies where they pretend to have received an inheritance and try and get an upfront payment. And finally and Delia is going to talk about this in more detail – investment and get rich quick scams.

In the future the developing areas that I think we need to watch out for relate to Phishing scams and these are going to become much more sophisticated, Col will tell you a bit more about those from the technical perspective in a minute, but they're becoming much more difficult to identify as a scam and they do very nasty things to your computer at the same time.

Online auction scams – not to say all online auctions are fraudulent and in fact some of the large online auction companies have got very sophisticated schemes to help consumers but it is possible to get defrauded using those activities. The development of mobile nolis(?) creates many risks in terms of the technical security that is available on mobile phones and wireless laptops but also just the fact that there's this desire to engage in transactions very quickly if you've got a mobile phone and somebody's trying to sell you something on that. The possibility for contemplative thought about what's going on is reduced.

And finally and worrying is the use of email and other scams to extract money using threats of extortion or violence. No longer do sophisticated fraudsters try and trick you out of giving money in advance. They'll say if you don't give us money we'll come over and murder you or beat you up. Okay, now some very brief views about what we know about these sorts of scams. This is just a quick snap shot and something that social scientists should never do which is give you a percentage from a whole survey without going into the underpinnings of that.

If you want to read more about it you can download a paper we've just done on consumer scams which is available from the [AIC's website](#). I guess the transition is with survey research to look at the experience of people, people who have said to experience scams and that's sometimes not a very helpful concept because we don't know what experience means in some of the surveys. People responding to scams, so you get an email and you actually do something. Then other surveys talk about being victimized and finally some surveys actually ask people about how much money you've lost and that's probably the best indication of the extent of the problem. Various percentages there but you can see that there's fairly high proportions of people who are experiencing scams and that might simply be receipt of a scam email or letter or invitation by the telephone.

In terms of responding to scams, we've got some reasonably detailed statistics from New Zealand on different types of scams and there's fortunately relatively low proportions of people who are responding. Although if you look at 1% of the whole population that's many 100s of 1000s of people so I think it's still a concern that this number of people are willing to part with their personal information, and then 8% of Americans who respond to Phishing emails is very frightening. Being victimized and this is again not a very precise concept that a lot of surveys have used, we are talking about maybe people who have experienced a problem, maybe people who have lost money. Its sort of all grouped in together so that's not very clear.

From the very large surveys such as the UK one I found that 6.5% of the whole British population had been victimized by scams in this way and again that's a very large number of individuals. And finally people who lose money to scams, Australian Scam Watch callers, these are people who have called into the Scam Watch line during March 2006, the campaign of activities then. 16% of the people who called in had said they had lost money to a scam. Of course those people who called in were self selected as people who had a problem with consumer fraud. 17% of those in Hong Kong in a recent international survey claim to have lost money as well. Okay, there we go. I'll go back one.

Now there's a whole range of different places that you can go to if you experience a scam. This chart sets out mostly federal agencies on the left and the state and territory agencies on the right. You can see that it can be a bit of a problem for individuals who have experienced consumer fraud to know who to go to. Do you go the High Tech Crime Centre? Do you go the ACCC, Consumer Affairs Victoria or perhaps Births, Deaths and Marriages if you have experienced identity fraud? Knowing where to go is a key problem.

The survey research that has been done has found a whole range of different statistics about what people actually do in terms of reporting consumer fraud and you can see the figures there of reporting to police which varies according to the type of activity. A survey that the AIC did a couple of years ago shows that there was a very considerable difference in the way in which people responded to online scams and offline scams – ones that didn't involve the internet.

Online scams were very rarely reported to police – only 3% whereas the offline ordinary door-to-door sales and telephone scams were reported to police much more frequently. Identity fraud in the U.S. seems to be reported much more often than other types and online auctions didn't seem to be reported very much. I guess understanding those sorts of figures you have to think about what people hope to get out of reporting. If you've got an insurance policy that you want to claim on then maybe there's an obligation that you have to report the case to the police in order to make an insurance claim. Reporting to banks - again quite a difference between online and offline scams in the survey that we did. In the offline world a much higher proportion of people reported to banks and card issuers than in respect of online scams.

In Canada marketing fraud generally was only 6% reported to banks. Reporting to other agencies and this includes the regulators, Consumer Affairs in Victoria for example had a pretty wide variation in the sorts of proportions of people who report to those agencies. And finally and I think the most worrying is the very large numbers of people who don't do anything. In sociological terms that is called 'exiting a situation' where you just give up. "I've had enough, I don't want to lose any more money, I don't want to waste any more time on this." But very large proportions of people don't want to report these cases officially. That of course creates problems for us in a lot of ways. We don't know what's going on out there, we don't know which parts of scams are the worst and we can't gather proper statistics.

So the solutions, and this is where the Australasian Consumer Fraud Taskforce has done a lot of work over the last couple of years, is to try and improve our knowledge base about what is really happening with consumer fraud and particularly mass marketed scams. At the moment as we speak and those of you who have got wireless laptops will be able to do it as I'm talking, you can go to our website and fill out the online survey which we're conducting at that URL there and this is to try and get a handle on what people in Australia at the moment think about consumer fraud and how victimized they have been. This is just a very brief snapshot for this month's awareness campaign and we'll probably only get 400 or 500 responses over the month. A much larger survey is being conducted by the Australian Bureau of Statistics and that's going to be rolled out in July this year.

There will be a household survey sent out to 13,000 households in Australia and there will be about some 10,000 or 11,000 responses which they'll analyze in time for next year's fraud awareness campaign. So by March 2008 we should have some really hard data on the extent of victimization, how much money is involved and what people are doing about it.

The other activity that needs to take place is to try and improve the data collection activities of regulators and consumer affairs agencies around the country. We need to have uniform sets of categories, data collection instruments so that when people ring up consumer affairs agencies they can report their experiences in a coordinated and uniform way. We can then try and get some information on which agencies are dealing with which types of matters, which get more and which get fewer. So to try and establish some consultation between agencies and improve their reporting activities I think would be an important outcome of what the task force has been doing over the last year.

And finally and by no means least is to try and persuade people to report their experiences officially. Not to just say "I've been scammed, I feel foolish, I don't want to do anything more about it," but to notify Police or the appropriate regulator to let them know what has happened. We will then be able to find out which are the most prevalent and changing types of scams, how much money is involved and hopefully give some feedback to people about

how any claims that they want to make are progressing. So I'll leave it there thank you and hand over to Delia.

Delia Rickard:

Thanks. Hi. Now there is a whole range unfortunately of financial scams I could talk to you about this morning but I want to narrow myself to these four here. I think they provide quite nice examples of the different challenges some of these scams throw up for a regulator in terms of detection, in terms of eradication, in terms of enforcement and in terms of effectively educating consumers on how they can try to avoid them.

I want to start first of all by talking about illegal investment schemes because Australians have lost many hundreds of millions of dollars to these schemes over the last decade. The victims come from right across the spectrum. There are nurses, there are retirees, there are professionals, there are members of church groups. The list is pretty much endless and illegal managed investment funds are actually a particular focus for our sector, we try to look at new and smarter ways in which we can start to combat these.

Just by way of a bit of background, these schemes are usually structured as I said as managed investments and they tend to fall into two main categories. You've got those schemes that are inadvertently illegal in which case you go and you either shut them down or you do the things that are needed to make them legal, and then there are the ones that are deliberately illegal, the ones that involve fraud. And it has to be said from the outset about all those obvious questions to have a quick look as to whether a scheme is legal or not and if it is illegal which of those categories it falls into. So some of the things we are doing at the moment just to try and be more proactive to spot these as soon as they appear to put them out of business before they can get too many victims, one of the main things we are doing is much more proactive advertising monitoring.

We have employed a commercial monitoring service to provide us with all copies of investment ads that appear in the print media, television, radio, in both metropolitan and rural and regional areas and we have got people who are going through each of those ads trying to identify which are the suspect ones. And as I said it usually won't be obvious so it involves a little bit of sort of staff shadow shopping, calling up pretending you want to invest, going down a few steps before you can really get a bit of a feel for what the product is that you have seen the ad for. Some of these prove to be legitimate if high-risk investment opportunities, others prove to be inadvertently illegal schemes which as I said we fix up. Some are illegal and we go about shutting them down and some are nothing like what we thought they were.

We had an example of this the other day when two of our staff went off to a seminar expecting to find an illegal managed investment scheme which we would set out to shut down, instead they found diet gel cream so they passed it onto the ACCC. So this work has only been going for a short period of time but so far it's proven to be quite active in terms of finding things when they first emerge. We have got a number of cases currently under surveillance that are heading for enforcement. Because the illegal nature of this scheme isn't always that obvious and they are not easy to spot, the other side of the role as an educator one part is the enforcement the other is really the consumer information/consumer empowerment side.

Educating consumers about how to identify these schemes and how to avoid them is a lot more difficult than some of the other scams we are talking about today. Yes there are simple messages that we all cut out you know that look too good to be true and it probably isn't true

but the reality is a) most people don't know what constitutes too good to be true and secondly we are seeing scams these days which are promising basically market returns. So that alone is not a fore mark of it.

So at the end of the day one of the set motives for things we think we can do as a regulator is to try and provide consumers with tools and skills with which they can go about making some sort of initial assessment about whether or not this is something that is worth pursuing. Interestingly we have been doing some research of late around this area that suggests this is what consumers want. The message we have had back is consumers don't want to be educated as such, they want information and they want practical tools that allow them to do it themselves and DIY was really a very strong message we got back in relation to all of this.

So in addition to the sorts of searches you can already do to check whether or not someone is licensed to check to whether or not they have been banned, whether they are on the list of illegal investment schemes we have up on our website one of the more important things we have done for a long time. We have put a risk return calculator so that when people see an ad, something they find interesting, they can actually type in what sort of investment category it is, what the promised rate of return is, the average length of the investment and then we have got a really strong warning – “That's really high risk, stay away” or “That's within the normal bounds.” We will also tell people what its reasonable to expect in terms of returns over the long(?) terms of that investment class. So hopefully in that way we can start to give people the skills to have some sort of filter to get rid of the worst of the things out there.

The other thing we are doing in this area is trying to be more proactive in helping people on a one-on-one basis. As well as...(inaudible – muted recording)...which we are redesigning and hopefully making it a bit easier for people to find things, we are trying to run more interactive phone conversations so that when people call up while we can't say “don't invest in that, that's a scam,” but we can say “well look, these are the risks, this is what we would usually say about an investment that has that kind of return,” and give all the right warning signals and take people through the safety check that needs to be done, a kind of dial before you dig thing if you've lived in Melbourne. And one of the benefits that we hope to get from that is in terms of our early notification about what sorts of scams are circulated out there in the community.

Because not all scams do advertise but a lot the illegal managed investment schemes out there don't advertise at all and they are sold through affinity group and these are some of the hardest ones as a regulator for us to find out about. We have seen these sold through church groups, we have seen them sold through schooling groups and police forces have even been victims to some of these so we are hoping that by promoting that kind of a telephone service that we will get more early signals about what's there and we can sort of be more active in terms of shutting things down.

Now one of the schemes I wanted to quickly talk about this morning was the early release of superannuation funds because this too is where we are seeing huge consumer damage and every increasing numbers of scamsters. Now as most of you probably know it's really very hard to get early access to your super, you don't get it before preservation age except for very, very limited circumstances involving financial hardship and compassionate grounds and there are some quite strict tests involved. Now the early release schemes that I'm talking about specifically target people on low incomes and those in real financial difficulty and the promoters also target in on retrenched workers and those living in rural and remote communities, particularly farmers and indigenous people.

And when you think about it given the amount of money we've got in super these days which I think the figure has just reach one trillion dollars and the number of people at this point of time that are suffering financial hardship, there is going to be no end of people who are trying to perpetrate this scam and that's certainly what we are seeing and what the ATO is seeing. What they are trying to do is that they falsely claim that they can help you withdraw your super or that they can put it into a self managed super fund that you can access and do whatever you want – pay off the car, get a new home.

In the worst case what happens is they just straight out steal your money, you don't see it any more and we've goaled a number of people for that in recent times. In other cases they do put it into a self managed super fund, they tell the client that they can use it as they wish and then they cream off 20+% of the assets of the funds in terms of fees for themselves, quite often a lot higher than 20%. They take off, the ATO catches that you are now in a non-complying fund, you get hit with a huge whopping tax bill and really most of the super savings that you had have been eradicated through the whole process. So this is another example of regulators, registered agencies working together and the ATO and ASIC are doing a lot of work together at the moment to try to find those scams and close them down.

I would say to people here who are financial counselors and have clients who are maybe vulnerable to this, it is a message that is worth getting out that there is only very strict limited ways of getting it and you won't get early access to your super through any of these schemes. Next cold calling scam, I'm only going to touch on these briefly here. Now these should be very easy to combat, there is a very simple consumer education message. If you get a call out of the blue from somebody offering to sell you shares, just hang up. Should be the end of the story, but like the Nigerian letter scams we continue to see these and we continue to see people falling victim to them. They continue to be our number one type of financial scam and the number of complaints we receive continues to increase unfortunately.

We conservatively estimate that in the six years from 1999 Australians lost well over \$400 million to these scams, that's a lot of money. And this money isn't just lost to the individuals, most of its lost to the economy as a whole because most of it ends up overseas. The reason I said I would talk about them very quickly this morning is a bit of a lead on to Col's talk which is a nice example about how these scams really are run on an international scale these days and some of the challenges that that throws up for regulators.

One example from last month, three people who ripped off Australian investors through a cold calling scam were arrested in Malaysia and this was done as part of an international investigation that was led by the Dubai Financial Services Authority which ASIC and a number of other regulators cooperated in. Now this particular scam, excuse me reading here but I always sort of lose track of the details here, involved call calling by recks(?) of a fictitious London firm to get consumers to invest in off-shore options trading. The fraudster had set up a website for the Dubai Options Exchange, they had set up a fake regulator called the United Arab Emirates Commodities Futures Board and they set up the company Cambridge Capital Trading which claimed to offer financial services within the Dubai International Financial Centre.

To further disguise the scam they had electronic answering services/devices, phony faxes and false billing addresses for websites in Dubai, the UK and the USA. Now its just a very small part of the story but when you start to look into these its not unusual to find three or four continents covered with those who are involved in the whole scam which makes it very, very hard for a local based enforcement agency to actually get in there and close it down.

We have all heard about Phishing these days, most of us when we boot up our computer in the morning we find two or three you know security alerts from a range of banks etc. They are all too familiar. My reason now for mentioning it quickly this morning is to give flag(?) the fact that the Electronic Funds Transfer Code is presently being reviewed and a discussion paper to kick off that review was put out in January. For those of you who aren't familiar with the Code, that's the Code that sets out all the rules for how liability is allocated where there is an authorized transaction including where there is internet fraud, including where people fall victim to a Phishing scam. I would urge people who have an interest in this area to get a hold of the paper and to get involved in the review and to make submissions because obviously the rules around liability allocation in these areas have consumer protection implications and its important that we get the broader community not just the industry side of things engaging with this whole issue.

Now to finish off, because it is scam week and this week's theme is how to protect your phone I thought I'd finish with a telephone scam. Now as a regulator of course you are meant to condemn and hate and horrified by all scams but every once in a while you see a new one where the imagination behind it is so extraordinary that you do have to sort of stop back and have a begrudging admiration for the scamsters out there. The one that recently caught my attention was the wrong number scam which emanated from the US and this is the scam, you get home from work, you check your answering machine or maybe it's on your mobile and there'll be a message from someone whose voice you don't recognize and they have obviously got your phone number confused with someone else and they have left you a message that has got a stock tip on it and the idea is that you will then go off, buy this stock as many people in fact did, and its your classic pump and dub(?) and you lose your money.

There are a million permutations of these scams out there and I just think the message is to keep your guard up the entire time when you are being invited to any kind of investment opportunity. Finally since there is a bit of a theme this morning about plugging your own thing, likewise I would encourage people who are interested in this to go to the scam watch website and also if you are interested in keeping up to date with the financial scams that are out there go to ASIC FIDO site, www.fido.gov.au and there is a free electronic newsletter there which because we get so many scams reported to us one of our ways of letting the community know is through that and that will help keep you up to date with what is happening. Thanks.

Col Fry:

Thank you Louise and thank you everyone. Very quickly I'm going to run through if I may the role of the Australian High Tech Crimes Centre, our partnership, the tools, the limitations and lastly just close with how effective we are actually being.

The role of centre, we started operation in July 2003, I think it was an old experiment to get government agencies and private sector agencies to work together in this space. To be quite honest I think it has been partially successfully. Working together collaboratively is a difficult path as some of you no doubt know.

Today I'm going to focus specifically on Phishing, or internet banking fraud and on that point we have two bank fraud investigators and two police officers and a contractor, so that is five people in a team of twenty that their sole job is internet banking fraud. As most of you might appreciate that is a big ask for five people. That is just to give you an overview of some of the tools, but just on this sub-point we have come to realize that probably the single most powerful weapon in this fight against internet banking fraud or Phishing or nil recruitment as

we say in the business is probably education of the consumers, the clients and if I may share with you a short story.

We met an absolutely lovely lady, middle aged in Sydney about six months ago. We were undertaking some enquiries up there and whilst we were talking to her we had a look at her computer and she was telling us that the last three months this computer would come on in the dead of night, it used to wake her up and it was so bad that she had to go to see a doctor for some sleeping tablets. She never ever actually turned her mind to actually turning the machine off or anything like that but the reality was that some criminals, some bad guys had gotten control of her computer and were using it for criminal things.

So I think if we can do more work to educate consumers, the people in the community to take steps, proactive steps to protect themselves, protect their computers I think that will go a long way. What we have found is that most of these crooks, the organizers, the people responsible for this criminal activity are located offshore. Working with law enforcement and other agencies off shore is very difficult. Partly because of the different legislations the thing that comes to notice quite frequently is privacy issues. Everybody wants to talk to us about privacy and exchanging information to investigate criminal matters.

In terms of our effectiveness, I've been with the centre since October 2004 and I would have to say I think a lot more can be done, I wouldn't say we've been completely effective. Working collaboratively with other organizations is a hard task. Some of the things that we do or measure against is IP blocking and because of our relationships with the major internet service providers we are able to put in place through legislation facilities to actually block Australians from connecting to offshore Phishing or nil recruitment sites. That is a short term measure and there are other long term measures that other organizations affected by those schemes can put in place in partnership with organizations like volsurt(?) up in Queensland.

What we are finding is the deregistration of illegitimate sites is fairly good, usually within one week depending on the registrars that actually registered those websites. I've got question marks there beside the site removal from the internet. The internet is a very flexible and dynamic place and as quickly as sites are removed other sites are put up to replace them. So having sort of really whipped through that to get us closer back on time, that is it for me and I'll pass back to Louise.

Nigel Walters:

Nigel Walters from the Privacy Foundation of the Consumers Federation. A two-part question, both about privacy; can't let Col get away with the sort of generic side-swipe of privacy there, because, as you know, I mean all the privacy laws basically allow for disclosure in relation to investigation of criminal activity. So, you know, I'd ask Col to elaborate on what he was saying there. I mean, why do you see privacy as being an issue? But equally, a question to I guess all of you; it strikes me that the Privacy Commissioner is a sort of glaring omission from the list of agencies involved in your project. There are major privacy principles dealing with security and why isn't the Privacy Commissioner a player in your group? Thanks.

Louise Sylvan:

I might start without him and pass to Col. The Privacy Commissioner's office is a partner of the Tax Force, as opposed to a member, so we work with them and they partner in terms of the work that we're doing. So we are pretty actively aware of those issues and do involve her.

Col:

Nigel, just in relation to that question, what we are finding is that a lot of organisations or people, I think, do not really understand the privacy legislation. What we find repeatedly is that we end up with their lawyers talking to our lawyers, and that's quite protracted and while that's happening, the criminals are getting away or moving on. So, I think that's the confusion over the legislation.

Jan Whittaker:

My name's Jan Whittaker, I'll just put a consumer hat on at the moment to distinguish the privacy relationship. I had an experience where I wanted to report something and tried to do that and ended up falling into that 69%. I am wondering about what the Tax Force is doing to reduce the complexity of that slide and, to test the idea to see if anything had gone any further since I had this experience last year, I actually went to the High Tech website to see if anything had changed. Essentially, I was referred to every other law enforcement that was on that list so I still had no way to know how to jump into the system to report the problem. So, in a position of enabling consumers to actually participate, to report, what are you doing to reduce that complexity, rather than sending us back to our local Police stations who couldn't care less?

Louise Sylvan:

This is the time for me to pass to my colleague, isn't it? Look, I'll tackle that a little bit and then we'll invite other people. One of the difficulties that we know is out there and is hard to address is that everybody's got a little piece of this puzzle in different ways. The High Tech Crime Centre, in a sense, can't do a great deal for the consumer who just sends \$30 away to a scam by mistake. Police forces don't want to know about that and it's quite clear that their responses to this sort of thing aren't sort of encouraging.

One of the things that we do want to do, but we've got a Federation to deal with – there's a question about how we do it – Scam Watch, during the month of the campaign, acted as a repository where all of the information is coming in and then, with the permission of course of the consumer, can go back out to the various agencies that are concerned with this problem. Whether we can, without having a sole agency, if you like, responsible within our Federation, whether we can get to the point with the 16 agencies in Australia, or less than that taking complaints, but still a great number; get to the point where everybody's happy to say, yes, they can come in or we will show them, which is really what we are working towards at the moment, so that everybody's got the same data that we are working from. I'm not sure, but that's the goal.

So we are not working towards – there will be one thing where you go – but working towards if you go to any of these places, it will essentially become one collected area of information. It's hard to do and for good reasons it's hard to do. The States and Territories need a sense of what's happening in their areas and regionally and so on, the National regulators need to know nationally; so everybody wants a full part of this action and we're just going to have to find a way to share that in such a way that it makes sense to the consumer trying to deal with all of the agencies who have a concern. That's my initial answer, others may have a different view.

Delia Rickard:

If it's a financial services scam, you can call ASIC and register a complaint with us. Sometimes we will be able to do something, sometimes we won't, but we like to have the information because it helps us know what's happening out there.

Unknown Male:

There probably is a more centralised reporting scheme in the UK with the Office of Fair Trading and that's a model that would be nice to try and apply in Australia if we had enough money, but it's incredibly expensive to run an organisation like that because you need to have quite a large staff to receive complaints from different types of media and then to communicate them to all the other interested agencies who've got specific jurisdiction to deal with them and then to receive feedback from those agencies, so that they can report back to the consumer. I think the worst thing that can happen, is for people to report complaints and then not have any feedback about what's happened to them. Providing feedback of course requires someone sitting at the end of the phone or a computer to give that information.

Louise Sylvan:

I don't know if David Cousins is in the audience, but these are all Federal agencies, but if he is or one of his staff might like to address that question from a State perspective. Anybody from CAV who wants to take that on?

Unknown Male:

With ASIC, I suppose, we are coming to understand what's happening out there and encourage consumers to reply and register complaints with us through the Task Force, there's a sharing of that information through OzShare(?), but I think the first step there is to understand what the issues are and to try to pick up emerging issues that occur in every week of the month and act quickly through that coordinated mechanism to be able to explain.

George Negus:

I knew I was the devil's advocate. You said something before that caught my attention, when you said that the States and Territories need to know what's going on their area. That bothers me enormously; trying to share your problem. Why do they need to know particularly what's going on in their area? Isn't this an Australia-wide problem and aren't there patterns and trends and indicators that suggest that the 16 different agencies are probably unnecessary? Why do they need to know what's going on in their area? I would have thought that scamming and swindling and stinging and sharking is a National problem.

Louise Sylvan:

It is a National problem. The National regulators by and large though, like ACCC and ASIC, are there to deal with the broad problem, if you like; something which is enforceable that we can deal with at a National level. It's the State and Territory Consumer Affairs agencies that actually handle the individual complaints directly and go back to consumers. So, they are much closer, I think, to the individual consumer than the National agencies are and are designed to be, but it's kind of the complimentary way the system is organised. I do think it is important for them to know. They can take enforcement activity in their own right, so can the National regulators and if there is a local problem from a scamster, for example who is operating just within a single jurisdiction, they can take action on that as well.

National Consumer Congress

George Negus:

Are the regulations and the laws similar, or different?

Louise Sylvan:

The laws are very similar in this area.