ASIC

Australian Securities & Investments Commission

Protecting Account Aggregation Consumers

A presentation by Delia Rickard

Deputy Executive Director, Consumer Protection, ASIC

to
Financial Review Conferences: BANKTECH
22nd November 2001

Thanks to Nicola Howell, Francis Ong, Josh Moyes and Jenny Green for the work they have done for ASIC on the issue of account aggregation.

Introduction
Good afternoon.

Its nice to be kicking off the account aggregation session with consumer protection issues. All too often these are left until last if they are considered at all.

My focus this afternoon is on how account aggregation services can be provided in a way that ensures that consumers can access the benefits of them without unknowingly exposing themselves to new risks.

In doing this I want to focus on what the Australian Securities and Investments Commission (ASIC) sees as some of the key consumer protection issues associated with account aggregation. Lest this sounds unduly negative though, I thought I would first spend a quick minute or two discussing ASIC's general approach to e-commerce issues and to account aggregation in particular.

ASIC's role.
As most of you are probably aware, ASIC is Australia's financial services, consumer protection regulator. We have a specific statutory mandate to

> Promote the confident and informed participation of investors and consumers in the financial system.

We have had a particular focus on e-commerce in recent years believing that it has the potential to offer both businesses and consumers greater efficiencies, cost savings and choices in how they undertake their financial services dealings. We have also developed a set of principles for how we will approach e-commerce. In brief,

- we will seek to achieve regulatory objectives rather then develop technological solutions (that is, we won't tell you how to do something, just the outcome we expect);
- we aim to make ASIC's policies technologically neutral:
- we want to ensure the regulatory requirements for electronic commerce are no more onerous than those applying to traditional ways of doing business to the extent that this is consistent with good policy; and
- we want to make sure that consumers using electronic commerce have at least the same levels of protection as they get from the laws and practices that apply to existing forms of commerce.

You will notice that I haven't said identical protections and this is because e-commerce (and account aggregation is no exception) frequently raises a range of new consumer issues which have not previously had to be grappled with. Of course, just as often, many of these new issues are simply different manifestations of problems that we have traditionally seen in the off line world.

We are not new to having to grapple with the issues thrown up by emerging technologies. Amongst our experience has been chairing the working party with

revised the EFT code to apply to all forms of electronic funds transfers and policy statements on a range of issues such as chat rooms and online purchases of life insurance policies.

The Business Case for Getting Consumer Protection Right
Before talking about ASIC's specific areas of concern, I want to stress that we believe that getting consumer protection right will be critical to developing consumer confidence and trust in account aggregation services which in turn will have a key impact on influencing take up rates.

We have all seen the stats about the small percentage of early adopters of new technologies and the small percentage who will take years to use the technologies or never do so and that big group in the middle who will wait until they are confident about the technology, price etc before using them. I expect that this will also be the scenario for account aggregation.

Overview of ASIC's concerns.
The key areas of account aggregation services that ASIC is interested in should not come as a surprise to anyone familiar with consumer protection issues. We are concerned to ensure:

- That consumers are adequately educated about account aggregation services so that they know the benefits and risks associated with the product and the questions to ask when deciding whether or not to use aggregation services and, if so, which one.

- That consumers have access to adequate disclosures to make informed choices. (And with account aggregation this means not only disclosures by the aggregator but also by the consumer's financial institution about their attitude towards PIN disclosure).

- That there is a fair allocation of liability when things go wrong.

- That suitable privacy policies are in place;

- That the aggregation services marketed to Australians have appropriate security standards and there is no scope for disreputable or unsafe services to appear; and

- That should anything go wrong, that there are appropriate complaint handling processes in place.

We have formed our views about these issues as a result of:

- undertaking surveys of websites both here and overseas in 2000 and again more recently;

- talking with the providers of all the aggregation services currently available in Australia and some planning on introducing services as well as many of those

involved with the provision of the relevant technologies; and

- through keeping up to date with the views of overseas regulators, consumer groups and commentators on this issue – in particular those coming from the US where account aggregation services have a slightly longer history than they do here.

For those of you who are interested, we issued a detailed issues paper on this topic in May 2001 entitled "Account Aggregation in the Financial Services Sector". It is available off ASIC's website which is located at www.asic.gov.au. I will cover some of what we said in that paper and will add to it given that in this rapidly moving industry newer issues are emerging and practices are already changing.

So, lets look at each of these areas in a little more detail.

Disclosure by account aggregators.
I will start with disclosure since in this country much of our consumer protection regime is based upon the provision of adequate disclosure as opposed to legislation which prescribes what can and can't be done.

The rationale behind disclosure is that consumers should have the information necessary to enable them to make informed choices. In part this means that they need access to clear, simple and relevant information about aggregation services that allows them to weigh the benefits and risks, be confident about processes and to compare between service providers.

There are, of course, legal requirements that govern the information provided by aggregation services. In particular, the consumer protection provisions of the ASIC Act and/or the Trade Practices Act are likely to apply to aggregation services provided by corporations. These provide some basic disclosure standards, including the general rule that information, representations and conduct should not be misleading or deceptive, and the idea that you can be misleading or deceptive by omission (i.e what is not said as well as what is). In other words, there must be adequate and accurate disclosure in the context in which the service is offered.

In ASIC's opinion, however, aggregation services that want to build consumer understanding of, and trust and confidence in, aggregation services, should aim to do more with disclosure than simply complying with the legislative requirements. Taking positive steps to disclose relevant information in an accessible way is a start.

So, the obvious next question is what sort of information is relevant. If I was thinking about using an aggregation service, some of the questions I might want answered include (in no particular order):

- How much does the service cost? And if there is a charge, what happens if I don't pay? Can the aggregator automatically deduct money from one of my accounts using the password I have provided?

- How secure is this service? (in simple terms!) and what sercurity guarantees are offered? Is there anything to stop hackers or others from accessing my

account details and withdrawing money?

- How current and reliable is the information provided through the aggregation service? What guarantees are provided? Who will pay if I suffer loss because the information provided was out of date?

- What is the aggregation services going to do with all of this financial information about me? Will it use my information for marketing purposes? If so, will it be an opt-in or opt-out service? Or will my information be sold to third parties for marketing? [The new amendments to the Privacy Act will obviously have some impact here.] What happens to my information if I decide to cancel my registration? Will it be deleted from the aggregator's systems?

- What are the risks of using the aggregation service? Does my financial institution mind if I disclose my password to an aggregator? If I do disclose my password, will I have to pay for any unauthorised transaction that occurs?

- What's the relationship between the aggregation service and the financial institution? Has my bank given the aggregator permission to 'scrape' my information?

- Where is the aggregation service located? If the aggregator is based overseas, will it be more risky to use the service?

- What are the terms and conditions for using the service? What obligations do I have (eg for password security)? And what happens if I don't comply with them?

- What happens if I have a complaint that relates to using the aggregation service? Should I go to my financial institution or the aggregator? Is there an independent dispute resolution scheme that I can access if I'm not happy with the result of my complaint? What if the aggregator is based outside Australia?

- Am I protected by the same consumer protection, privacy and other regulations as I am when conducting Internet banking? (In the US, one survey showed that more than two-thirds (71%) of respondents believed that aggregation services provided by financial institutions have to comply with federal banking regulations. In addition, 51% thought that aggregation services provided by third-party Internet companies have to comply with federal banking regulations.[1])

- Who is this aggregation company? Can they be trusted?

These are just some of the questions that consumers might be asking when thinking about using an aggregation service. And if the functionality of these services increases further – for example, to include transaction capabilities, the need for clear

[1] Star Systems Inc, *Web aggregation: a snapshot*, August 2000, p. 49-50.

consumer information will increase further. For example, consumers will probably want to know who would be liable if a transaction was not properly executed.

In our May Issues paper on Account Aggregation we included a draft good disclosure template for account aggregation services. It has been pleasing to see that some institutions are already paying attention to it when drafting terms and conditions for their services. I would strongly encourage any of you presently involved in establishing an aggregation services or reviewing the terms and conditions for existing services to refer to the template.

Disclosure by Financial Institutions.
The need for improved disclosure isn't confined to account aggregation sites. There are also some important disclosure questions for financial institutions to think about. A key example is whether financial institutions should tell their customers the institution's views about using aggregation services generally and PIN disclosure in particular.

In our original website survey, we found three different approaches to disclosure on this issue by financial institutions.

The first approach is to say nothing on this topic on the institution's website. This is the approach that seems to have been adopted by almost all of the sites that we surveyed.

A second approach is to, in effect, advise that consumers use aggregation services at their own risk. One American institution, Netbank, included the following in its terms and conditions:

> "If you choose to use the services of an account aggregator, you assume all risks inherent in disclosing your passwords or personal identification numbers (PINS) to a third party. NetBank has no responsibility for any use or misuse of your account data by any third party to whom you have provided your account information, passwords or PINS. This means, among other things, that you are liable for all transactions conducted by the account aggregator on your behalf or with the use of your personal passwords or PINS ….
>
> If you experience any problems with a third party account aggregator to whom you provided your account information, you will have to resolve the problem directly with that third party. NetBank cannot accept responsibility for any loses, damages, or fees assessed by another company or institution caused by the involvement of a third party account aggregator."

The interesting thing with this disclosure is that Netbank also offer an aggregation service (Online Account Consolidation Service).

In contrast, one of the UK Banks – Egg – takes a different approach. It tells its customers that disclosure to approved aggregators is permitted. It has this to say about its customers using account aggregation services:

> "If you want a third party to collect information about your Egg accounts from us so that it can be aggregated with information about accounts you have, you may be asked to give your security details and passwords which have been set up to access the Secure Area ("Passcodes") to that third party. Before doing so you must check that the third party is approved by us. We will not treat the disclosure of your Passcodes to such a third party whom we have approved as a breach by you of the provisions of this condition."

Since our original survey it is pleasing to see that at least 1 Australian institution that we are aware of has started publicising the approach they will take to account aggregation. Colonial First State provides its consumers with a range of information about account aggregation services including the warning that:

> It is important that you realise that by providing an account aggregator with your login information you are in breach of the FirstNet terms and conditions of use. This means that we will not accept liability for any loss or damage suffered by you in connection with your use of FirstNet.

There are currently no obligations on financial institutions expressly requiring them to provide the type of information that I've talked about. ASIC is firmly of the view, however, that such disclosure should be provided to consumers. We would suggest that institution's should be clearly informing their customers, and in particular their online customers, what their views are on the use of account aggregation services generally and, more specifically, their views about disclosure of PINs to aggregators.

When providing such disclosure to customers institutions should also make clear whether their views vary at all depending upon who the provider is or the technology used. (For example do their views vary depending upon whether it is a user driven or third party aggregator?) Where financial institutions believe that disclosure of a PIN to an aggregator is a breach of the EFT Code's security requirements they should not only inform consumers of this fact but also of the potential consequences of undertaking such a breach.

If this information is not provided voluntarily, it might be worth considering whether there might be a role for some form of guidelines or rules such as an amendment to the EFT Code of conduct.

Finally, in respect of both disclosure by aggregators and financial institutions, it goes without saying that the information we are suggesting be provided should be designed in such a way that it is clear and accessible. Consumers are not always going to know what information they should be looking for, or what questions they should be asking. Burying important information in fine print of the terms and conditions is not usually conducive to consumer understanding. Among other things, we suspect that many people don't read terms and conditions documents.

However, the Internet has the potential to improve the way in which information is provided to consumers. We'd encourage aggregators and financial institutions to be creative and thoughtful in how they utilise this potential.

Liability

The next issue I want to discuss is one of the most important consumer issues associated with the use of account aggregators – namely the allocation of liability when things go wrong. That is, who pays when something goes wrong?

There is now a fairly clear historical trend when new technologies appear. Namely, that at least some institutions will attempt to use the occasion as an opportunity to transfer liability for problems from themselves to consumers. For example, there are long established common law rules that when your signature on a cheque is forged

the financial institution is responsible for the loss. When ATMs first appeared there was an attempt to pass all liability for unauthorised transactions onto consumers. Not surprisingly, this was one of a number of factors inhibiting the take-up rates for ATMs initially and eventually the EFT Code was established to create a fairer regime for allocating liability between institutions and consumers.

We have seen a similar move by account aggregators, although the more the issue is publicly debated the better things are getting. Of the services available in Australia today we run the gamut from those attempting to deny all liability on the aggregator's part for anything other than undisclosed statutory warranties, to those who accept a capped liability in certain limited circumstances to those who accept unlimited liability in limited circumstances (eg where fraud their employees is involved).

No aggregation service that we are aware of has systematically gone through the circumstances where liability could arise and dealt bit by bit with their approach to liability on each of the issues. And it should be noted here that there are three, not two, parties to consider in this context. Namely, we need to look at when the consumer should be liable, when the aggregator should be liable and when the financial institutions should be liable.

Of course, we hope that the incidence of problems will be low. We expect that reputable operators will have installed security systems of the highest standards.

That said, there is a need for a debate on the appropriate allocation of liability in the range of circumstances where things can go wrong. ASIC does not yet have set views on what the appropriate allocation of liability should be in each instance. We are, however, clear on the fact that disclaiming all liability in circumstances where employee fraud results in unauthorised transactions or attempting to cap liability for such employee fraud is not a fair allocation of liability.

To make this issue a little more concrete, lets examine the question of liability for an unauthorised transaction. If such a transaction occurs on a bank, building society, or credit union account, it is likely that the revised EFT Code would apply. Under clause 5.6 of this Code, consumers can be held liable for an unauthorised transaction if they have contributed to the loss by disclosing their PIN or password to a third party.

The question then becomes - is disclosure to an aggregation service provider a disclosure to a third party for the purposes of the EFT Code? My guess is that many financial institutions will argue that the answer is yes and that the consumer who discloses their password to an aggregation service could be held liable for losses. The issue is then about the allocation of liability between the consumer and the aggregator.

The revised EFT Code does modify this rule slightly. It basically says that consumers won't be in breach of the code's security requirements if they give their PIN to an aggregator in two circumstances – namely where their financial institution has specifically given them permission to do so and, secondly, where their institution impliedly promotes, endorses or authorises the services say, by hosting it on their site.

The actual provisions state:

"5.7 (a) Where an account institution expressly authorises particular conduct by a user (either generally or subject to conditions), the engaging in that conduct by the user (within any applicable conditions) is not a contravention of the requirements of sub clause 5.6.

(b) Where an account institution expressly or impliedly promotes, endorses or authorises the use of an account access service by a user (including by hosting an account access service at the account institution's electronic address), no disclosure, recording or storage of a code by a user that is required or recommended for the purposes of using that account access service is a contravention of the requirements of sub clause 5.6."

This will provide some protection for consumers using aggregation services, but it does not cover all circumstances. For example, it won't protect consumers if their institution does not "promote, endorse, or authorise an aggregation service" and is silent on the question of whether its customers have permission to disclose their PIN or password to an aggregator.

Whilst on the issue of liability for unauthorised use following PIN disclosure, I have been disturbed to hear or read of some account aggregation providers claiming definitively that the use of their system does not result in disclosure to a third party. This may well turn out to be the accepted view but until either other financial institutions have expressed their own views on this issue or some type of standard or code has been developed this cannot be stated with 100% confidence.

Other liability issues not covered by the EFT code include the relationship between an aggregation service provider and a consumer. This means that, in the absence of any other regulation, the terms and conditions can set the liability allocation rules if loss occurs.

In our survey, we found that it was not uncommon for aggregators to disclaim liability for consumer losses suffered because of:

- unauthorised use of the service;
- misrepresentations;
- timeliness, completeness and accuracy of the information provided;
- omissions, errors or delays in the service;
- non-performance or interruption of the service; and
- quality of the service;

even if the aggregation service might have contributed to or caused the loss.

The question for aggregators is then whether this is a fair allocation of liability – especially in circumstances where they are trying to build consumer trust and confidence in their services.

I should just note before moving on that, in practice, implied statutory warranties, such as those in s. 12ED of the *ASIC Act*, might reduce the effect of these very broad disclaimers. However, this relies on individual consumers having the knowledge and resources to pursue a dispute. This is even less likely if there is no external dispute resolution service available – and I will talk about this next.

Over the coming months, we will be talking with industry and consumers about the liability issues involved in aggregation services, and the best way to ensure that consumers are adequately protected. A range of possibilities present themselves for what the standards may be. For example, in our issues paper we raised two possible approaches:

- a provision along the lines that disclosure of a PIN to an account aggregator will not contravene clause 5.6 unless the account institution specifically, prominently and clearly warns consumers that such disclosure is not permitted either in general, or to one or more particular aggregators.

  or alternatively:

- a provision that restricts aggregators to accessing data only from sites which have authorised their consumers to hand over access codes to the aggregation services.

I'm sure that a number of other options for dealing with liability issues will also be put forward for consideration. When looking at each of the options, one of the things we will need to keep in mind will, of course, be the competition law implications of the proposals)

Complaints and disputes resolution
Ensuring that consumers have access to appropriate processes for complaints and dispute resolution can help to build trust and confidence. Conversely, if consumers believe that there is some risk involved in using aggregation services, and they cannot see evidence of some process that can be used if something goes wrong, they may be reluctant to try out a new service.

Financial institutions that offer aggregation services and are members of the Banking Code or a similar code already have to provide their customers with access to internal and external dispute handling procedures. And the soon to commence Financial Services Reform legislation includes similar obligations.

However, the situation is a bit different where an aggregation service is not provided by a financial institution. Currently the Banking Code and other codes do not apply. And it is possible that, unless the aggregation service also offers transaction capabilities or financial advice, the proposed FSRB requirements may not apply.

As an initial step, aggregators should make sure that they provide accessible contact details for queries and complaints. This should include an email address. However, consumers should also be able to contact aggregators by telephone, fax, mail, or perhaps even in person.

In addition, we'd strongly encourage aggregation services to develop, document and implement internal complaints handling processes that are easily accessible.

And, as the industry matures, we'd like to see consideration given to the best way to offer users of aggregation services access to an independent dispute resolution

scheme or schemes. It seems likely that for financial institutions offering aggregations services existing schemes will be used and at least one aggregator already acknowledges the ABIO's jurisdiction in respect of it.. Ideally, one scheme, such as the Banking Industry Ombudsman, would handle all account aggregation complaints, thus ensuring consistent treatment of like issues.

And once developed, these complaints and disputes processes must be adequately promoted – they will be of little use is consumers don't know about them.

There are a couple of other issues to think about in the context of complaint handling:

- How can we reduce the risk that consumers will be shunted between the aggregator and their financial institution – with neither accepting responsibility for resolving the dispute?

- In the absence of formal agreements between aggregators and financial institutions, how can we ensure that an aggregator can seek from an institution, information that might assist in resolving a complaint, and vice versa?

- How can information about unauthorised transactions and other losses be collated to identify a significant breach of security? If, for example, the security of an aggregator's password vault is compromised, there could be unauthorised transactions made on accounts with a number of different institutions, and owned by more than one consumer. Without some way of collating information about losses, it might be difficult to quickly identify that the only link between the unauthorised transactions is the aggregation service.

We don't yet have all the answers to these questions, and we are interested to hear what others think.

And that leads nicely to my next issue: security.

Security

Given what I have just talked about – it is clear that aggregation services need to have adequate security standards. It's fairly obvious that a password vault is going to be very attractive to hackers and others. The possibility of a large scale systemic problems if a vault were breached once these services take off is a very sobering thought in deed.

Each of the aggregation services that we looked at provided a security statement that outlined the measures taken to ensure that information provided to the service was not compromised. However, most consumers would find it difficult to assess whether the security standards are adequate.

There are no common security standards for aggregators. Of course, legitimate operators have fairly significant incentives to get security right. Any security breach is likely to send consumers rushing away in droves.

However, it is possible that less reputable businesses could establish an aggregation service with inadequate security standards – or even with the intent of using the

account information itself to defraud users. Consumers may not necessarily be able to distinguish such a service from a more reputable operator.

In these circumstances – is there a need for common security standards? If so, who should set those standards? Should they be voluntary or mandatory standards?

Or, should it be left to financial institutions to warn consumers to use only certain aggregators, or only aggregators meeting specified standards? The Egg Bank example I referred to earlier suggests that the institution would be making its own assessment of suitable aggregators. However, as noted, an approach like this on an industry-wide scale is likely to raise some competition issues.

All of these issues were discussed at ASIC's recent round table on account aggregation. APRA, the regulator with the greatest interest in security issues, also participated in the round table. Amongst the options canvassed on the day was the possibility of asking Standards Australia to look at the issue of standards in this area.

On a related issue, I will include the plea of the head of our e-enforcement unit that aggregators and financial institutions keep their logs on and keep their records so that if there is a security breach, electronic footsteps remain and can be traced.

Privacy`

The last really big consumer issue associated with account aggregation is privacy. The privacy issues here are huge. And, while all the Australian institutions we have surveyed have had a disclosed privacy policy, the critical issue is whether or not the standards contained in those policies are adequate.

Certainly most aggregators will be required to comply with the National Privacy Principles under the new legislation once it comes into being later this year. There is a debate, however, about whether further clarification is needed about its application to aggregators. There is also some concern that small aggregators may fall within its small business exception although as privacy is not within our jurisdiction, I haven't looked closely enough at that issue to know how valid such concerns are.

Some other consumer issues

There are also some other important consumer issues – including consumer education, and whether aggregators should be regulated, however, I will leave them for discussions on another day.

Where to from here?

This morning I have tried to give you a good idea of some of the issues that we are currently focusing on in relation to aggregation services. In summary, these include:

- disclosure generally, and in particular, disclosure by financial institutions and aggregators about the consequences of disclosing PINs and passwords;
- appropriate liability allocation if loss occurs;
- complaints resolution processes; and
- security and privacy.

On the 31st of October ASIC convened a round table conference of industry, consumer and government stakeholders in this issue. At the round table, there was general agreement that these are legitimate issues of concern. There was also general agreement to ASIC convening a consultative process with a view to developing an account aggregators chapter of the EFT code. We are currently in middle of designing the most appropriate process for doing this.

Any such process will inevitably take some time, however, so we would urge those involved in aggregation issues to start addressing the problems I have raised today now, rather than waiting for the completion of any future aggregators chapter to the EFT code.

Thank you