Australian Securities & Investments Commission

Consumer issues in account aggregation

Account Aggregation Conference
Carlton Crest Hotel, Sydney
18 April 2001

Nicola Howell
Senior Policy Officer, Office of Consumer Protection
Australian Securities and Investments Commission

1. Introduction

My presentation today was originally titled ‘Navigating the account aggregation legal minefield’, but once I started preparing this paper, the title no longer seemed quite right. This is because, in looking at account aggregation issues over the last couple of months, we have found that there are not many specific regulatory requirements governing these services—at least when we are talking about consumer protection.

This afternoon I will give you an overview of the results of our survey of account aggregation websites, and I’ll discuss some of the consumer issues that were raised by this survey and other information that we have received. I will note the relevant regulatory issues as we go along, however, I guess it is fair to say that my presentation today will probably raise more questions than it answers.

This probably reflects the fact that we have not finalised our thinking on these issues. We have identified some areas that we think need attention, but we are still developing our views through further consultation and research. Also, the timing of this conference has meant the results of the website survey are yet to be officially presented to the Commission.

I should also emphasise that I am speaking to you as an officer of ASIC. I will be talking from an officer’s perspective on areas of concern, and not the Commission’s perspective.

2. ASIC’s interest in account aggregation

But to start with, you might be interested to know why ASIC has been looking at account aggregation services.

ASIC’s role extends to facilitating, regulating the Internet and e-commerce where it relates to the financial services sector, we are also providers of e-commerce solutions and services. We have a long history in this area and since 1998 have expanded our watch to include consumer protection issues. Without doubt, the Internet and e-commerce are integral to the markets we regulate, and we need to keep up to date with new developments.

For example, over the last two years, we have chaired the EFT Working Group. A couple of weeks ago, we launched the revised and 'technology neutral' EFT Code that resulted from this Group's work.

Last year, we also hosted two very successful conferences on e-commerce, where we explored some of the issues for regulators, businesses, and consumers in a world when more and more financial services are delivered or transacted electronically.

In general, we think that e-commerce offers both businesses and consumers efficiencies, cost savings, and choices in how they use financial services. Account aggregation services are one of the emerging e-commerce developments that potentially offer great benefits to consumers.

However, the Internet can also create problems and risks for consumers. We believe that the same mischief can occur online as in the offline environment. As a consumer protection regulator, we want to play a role in addressing any potential problems, and through this work, to foster consumer confidence in the e-commerce world.

Its important to do this work at an early stage in the development of these new services—not to hinder development—but because early identification of issues can minimise potential for harm to consumers' interests.

3. Survey of websites and other information

When account aggregators appeared on the marketplace in Australia, we wanted to find out what products were available, how they worked, what technology was used, and whether some basic disclosure standards were met. We thought that a survey of aggregation websites would be a good way to begin looking at these issues.

In addition, at around the time of our survey, each of the main aggregation services in Australia came to talk to us about their products. This gave us the opportunity to ask questions and gain a more detailed understanding of account aggregation.

For the website survey, we looked at the websites of:

- All banks licensed in Australia;

- Approximately half of the credit unions and building societies that are licensed in Australia and have an Internet presence;
- All Australian online brokers;
- All known (third party) aggregation sites in Australia that are not associated with a financial institution

Given the infancy of this market in Australia, we did not anticipate that we would find large numbers of aggregation services. We were focused on finding out what services were available as well as learning:

- whether institutions offered internal aggregation (ie consolidating information from all accounts held within the institution); and
- whether financial institutions provided warnings to their customers about the consequences of disclosing their PIN or password to an aggregator.

Our survey also looked at a number of United States aggregator sites. The North American market is more mature and can provide us with some insight into the potential issues for users, providers and regulators

We surveyed 74 websites—61 in Australia and 13 in the US. The website survey was originally conducted in November and December last year, but we updated the results earlier this month.

4. What did we find?

You probably won't be surprised to hear that we found that there are only a small number of account aggregation services in Australia.

The three main account aggregation providers we found in Australia were:

- AMP's Account Minder;
- Financial Enrichment; and
- E-wise.

Ninemsn are also promoting an aggregation service to be launched this year.

Despite the small number of aggregation services available now, we won't be surprised if more services are launched in the coming months.

We found that aggregation services in Australia use screen-scraping technology—rather than a direct feed arrangement. In terms of functionality, most could aggregate information from a range of financial accounts—eg from deposit accounts, loan accounts, credit cards, to managed funds and broker accounts, as well as non-financial accounts, such as email and frequent flyer accounts. None of the Australian sites surveyed offered the functionality to conduct transactions at this point, although it appears to be a natural progression of any aggregation business model.

In the website survey, we were also interested to see whether consumer protection information was obviously disclosed. The test we used for 'obvious disclosure' was whether the information was within one link (or click of the mouse) away from either the webpage to which it relates or from the site's homepage.

This part of the survey was not an assessment of the quality of the disclosure, or of whether we thought the practices disclosed were appropriate. Rather, we wanted to get a quick picture of whether some of the basic information was provided for consumers.

We found that majority of Australian aggregation sites did obviously disclose basic consumer information such as:

- Terms and Conditions for use of the aggregation facility;
- Fees for use of the aggregation facility (although most did not charge any fees);
- Security standards;
- Who has access to customer information;
- For what purpose customer information is collected;
- Whether information would or could be used for marketing purposes by the aggregator and/or a third party; and
- If marketing might occur, how the consumer could 'opt in' or 'opt out'.

Liability

Most—but not all—also included in their terms and conditions information on customer liability (eg for an unauthorised use of their account) and aggregator liability. The terms and conditions generally sought to avoid liability for consumers' losses in connection with the aggregation service.

Dispute Resolution

Information on complaints or dispute resolution processes for the aggregation facility was not generally provided, and only one site provided information about cancellation of the subscription to the aggregation service.

PIN Disclosure

Although some of the Australian aggregation sites do draw attention to the issue of PIN disclosure, none provided stark warnings on the consequences of disclosure, or on the breach of contract that this causes. In fact, it is feasible that a number of consumers may assume that the aggregation service comes with the approval of their bank. We looked at the websites of the banks to see whether any provided warnings to their customers about the consequences of disclosing their PIN or password to an aggregation service. As far as we could see, none of the financial institutions gave such a warning.

Since conducting the survey, we have gathered more information through talking with aggregation services and consumer groups, and reviewing information available from other jurisdictions. This has helped us to crystallise our thinking on what might be the consumer issues that are likely to arise as these services become more popular.

5. Disclosure

One of the important issues for consumers, using aggregation services, is adequate disclosure. Consumers need to have access to clear, simple and relevant information about aggregation services.

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 or conduct should not be misleading or deceptive. And there are other ASIC Act / TPA requirements that I'm sure you are well versed in.

But 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.

What sort of information might be relevant? If I was thinking of using an aggregation service, these might be some of my questions (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? 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 consumer information will increase further. For example, consumers will probably want to know who would be liable if a transaction was not properly executed.

The Best Practice Model for E-commerce, which was released last year by the Minister for Financial Services and Regulation, includes a section on disclosure. This might be one model for aggregators to follow when preparing and updating the content on their 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 their views on using aggregation services.

In our 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:

> "Regarding Use of Third Party Account Aggregators
> Some of our deposit account and loan customers are using the services of third parties to obtain information on their NetBank

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

> deposit accounts and loans and to conduct transactions on them. This disclosure concerns your use of these third party companies and your liability in connection with their activities on your accounts and loans.
> These companies, often referred to as "account aggregators," are not affiliated with NetBank. 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 (OnMoney.com).

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."

There are currently no positive disclosure obligations on aggregators to provide the type of information that I've talked about. If it is not provided voluntarily, it might be worth considering where there might be a role for some form of guidelines or rules—eg perhaps through an aggregators' code of practice.

It goes without saying that the information 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 to be creative and thoughtful in how they utilise this potential.

6. Liability

The second major issue that we see for consumers using aggregation services is that of liability. What happens if something goes wrong? Who pays if there is an unauthorised transaction, or if aggregation software damages the computer's PC, or if the consumer relies on inaccurate information provided by the aggregation service?

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.

Lets take the question of liability for unauthorised transactions first. 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 disclosure to a third party for the purposes of the EFT Code? My guess is that the answer would be that it probably is, and that the consumer who discloses their password to an aggregation service could be held liable for losses.

The revised EFT Code does modify this rule slightly. It includes the following provision:

"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.

This issue of liability is one reason why clear disclosure—from both financial institutions and aggregators—is important to consumers. Financial institutions can provide information on whether they will view disclosure to an aggregator as a breach of security requirements. And aggregators can advise on the potential risks of disclosing PINs or passwords, and whether there are any steps consumers can take to reduce the risk. Consumers will then be better able to appreciate the consequences of using aggregation services.

Another issue is that the EFT Code does not cover the relationship between an aggregation service and a consumer. This means that, in the absence on 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.

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.

7. 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 proposed Financial Services Reform legislation will include 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 may be, for example, that membership of existing schemes in the financial services sector could be expanded to include aggregators.

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.

8. 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.

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, an approach like this on an industry-wide scale is likely to raise some competition issues.

9. Privacy

The last consumer issue that I wanted to mention briefly this afternoon is that of privacy. I want to assure you that I haven't left it until last because we think that it is of minor importance. Of course, the privacy issues surrounding aggregation services are huge—and I have already talked about some of them in the context of good practice disclosure by aggregators. Our survey showed that all Australian aggregator sites provide information on their privacy policies. The recent extension of the Privacy Act to the private sector will also affect the disclosure obligations.

However, standard disclosure isn't necessarily enough—there is also the question of whether the privacy standards are adequate. Now this isn't really a question that ASIC is well placed to answer—we're not a privacy agency. However, we are getting some advice from the Office of the Federal Privacy Commissioner about these issues, and will be working with them to ensure that a co-ordinated and consistent approach is taken.

In the meantime, I would encourage aggregators to liase closely with the Privacy Commissioner's office and consumer groups when developing their privacy policies.

10. 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.

11. Where to from here?

This afternoon 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
- privacy and security.

We plan to release a report next month that will flesh out these issues in a bit more detail, as well as provide the full results of our survey.

As I mentioned earlier, we are still developing our views. We will be continuing to consult with industry, consumer groups and other regulators. For example, we are regularly liaising with other Commonwealth regulators with an interest in this area—namely APRA, the Reserve Bank, and the Office of the Federal Privacy Commissioner. We have also looked at what regulators in the US have been doing, and will continue to monitor their responses.

We hope that our report will act as a further catalyst for discussions between regulators, aggregators, financial institutions, and consumers about the best way to deal with the challenges for consumers in using these services. And we will be continuing our discussions with interested parties in both bilateral meetings, and multi-lateral forums such as this conference, so that we can better understand the issues and any possible solutions. ■