ASIC

Australian Securities & Investments Commission

CONSULTATION PAPER 20

Account aggregation in the financial services sector

May 2001

Your comments

We invite your comments on the *issues* in this paper. All submissions will be treated as public documents unless you specifically request that we treat the whole or part of your submission as confidential.

Comments are due by 13 July 2001 and should be sent to:

Nicola Howell
Senior Policy Officer, Office of Consumer Protection
Australian Securities & Investments Commission
Tel: (02) 9911 2410
Fax: (02) 9911 2642
Email: nicola.howell@asic.gov.au
Address: GPO Box 4866, SYDNEY NSW 1042

You can also contact the ASIC Infoline on 1300 300 630 for information and assistance.

Executive summary

Background

Account aggregation services allow consumers to view, on a single web page, information from their online accounts with a range of institutions. This allows the consumer to get a picture of their financial position as a whole, without having to log in separately to the websites of all of their financial institutions. Most aggregation services can also aggregate non-financial accounts, such as email and frequent flyer accounts, as well as news and information services.

Account aggregators gather a consumer's account and other information through direct feed arrangements or through screen-scraping technology.[1] In Australia, screen-scraping technology is used for two distinct aggregation models – the third party model, and the user-driven model.

To use a third party aggregation service, the consumer provides the aggregator with the account details (including username and password) for each of their nominated accounts. These details are stored on the server of the aggregation service provider or the aggregation technology supplier and the service provider uses these details to retrieve balance and other information from the nominated sites. This information is then collated onto a single page for presentation to the consumer.

To use a user driver aggregation service, the consumer stores their account details in a digital safe on their PC. The user activates the aggregation application on their PC, and the application uses the account details to retrieve balance and other information from the nominated sites. This information is collated onto a single page for presentation to the user.

Account aggregation services were first offered in the United States in 1999. Since then, a number of US financial institutions, portals, and other businesses have either begun offering aggregation services, or have announced plans to offer aggregation services.

Aggregation services are now also appearing in Australia.

As part of its consumer protection responsibilities, ASIC conducted a website survey of financial institutions and other organisations to determine the availability and functionality of aggregation services in Australia, and to identify issues for consumers. This paper presents the results of this research and describes the consumer issues. It is intended to facilitate discussion on possible solutions.

[1] See page 15 for a description of "screen scraping" and "direct feed".

Availability and functionality of aggregation services

In our survey, we found that:

- there are currently only 3 main account aggregation service providers in Australia (AMP Limited, eWise.com.au Pty Ltd, and Financial Enrichment Pty Ltd), although from our discussions with industry, it is clear that other services will emerge in near future;
- the aggregators in Australia generally use screen scraping technology to collect information, and do not have direct feed arrangements with financial institutions;
- each of the main aggregation providers can aggregate information from a range of financial and other accounts, but do not offer transactional capabilities;
- most of the aggregation providers in Australia included information on their website on terms and conditions, privacy, security, fees, direct marketing intentions, customer liability, and institution liability.

Consumer and regulatory issues identified

The main consumer and regulatory issues generated by account aggregation services include:

- **disclosure** – including disclosure about the risk of using an aggregation service;
- **liability for unauthorised transactions** – it is important to determine for losses caused by unauthorised transactions. For example, under the current regime, a consumer who discloses their password or PIN to an aggregation service may lose the protection offered by the EFT Code if an unauthorised transaction occurs;
- **liability for other losses** – for example, losses caused by misrepresentations, inaccurate information, poor quality of the service, downloading software, interruption of the service, etc;
- **privacy** – eg who has access to personal information, and what will the information be used for;
- **security** – especially the security of any location where account information is stored by the aggregator;
- **consumer education**;
- **complaints and dispute resolution** – most aggregation services surveyed do not appear to provide internal or external complaints resolution processes;
- **cost of aggregation services**, and debt recovery;
- **cross-jurisdictional issues** – for example, what are the implications if the aggregator is based in another jurisdiction;

- **regulation of aggregators** – should they be subject to the same prudential supervision framework and other regulations that apply to deposit-taking institutions and/or other financial institutions?;
- **the implications of the Financial Transaction Reports Act**, which is designed to deter money laundering and tax evasion.

Responses by regulators and industry groups

In Australia and most other countries, the market for account aggregation services is relatively immature, and there have been few, if any, regulatory or industry responses to the consumer issues raised by account aggregators. However, in the US, there have been some regulatory and other developments.

These include:

- a ruling from the US Federal Trade Commission that the term "financial institution" includes account aggregators for the purposes of privacy regulation;
- the possibility that the US Federal Reserve will issue guidance on whether the Electronic Funds Transfer Act applies to aggregation or screen scraping services;
- the release of guidance from the US Office of the Comptroller of the Currency to banks on the risks of offering aggregation services, and the management controls that are needed to minimise those risks; and
- the release of voluntary guidelines for aggregation services, developed by the Banking Industry Technology Secretariat, an industry group in the US.

Possible responses in the Australian context

Further discussion between consumers, industry and regulators on the issues raised by aggregation services would assist in developing appropriate solutions.

Some possible solutions for further discussion include:

Disclosure – ASIC could develop and promote a good disclosure template for aggregators and/or promote the inclusion of disclosure obligations in relevant self-regulatory forums.

Liability – a set of rules for allocating liability in the event of losses caused by unauthorised transactions or other circumstances could be developed, perhaps for inclusion in an aggregator module of the EFT Code or a separate aggregator code.

Complaints handling – ASIC and consumer organisations could encourage aggregators to join an existing external process for resolving disputes, or, if no appropriate process exists, to establish one.

Consumer education – ASIC and others could develop and distribute material that will enable consumers to make an informed decision about using aggregation services.

Where to from here?

ASIC believes that the consumer issues raised in this paper need to be addressed, although some are more urgent than others. Appropriate rules or practices need to be developed, published and implemented by aggregators and financial institutions. However, we are open to the views of others as to whether this should be through an aggregators' module in the EFT Code, a separate aggregators' code, or an ASIC guide on good practices. In addition, it is worth considering whether there should be a role for regulation or legislation.

We plan to hold a roundtable meeting with interested stakeholders later in the year. Among other things, such a meeting would provide an opportunity to:

- confirm the scope and nature of the consumer issues;
- identify any priority issues;
- seek consensus on the most appropriate solution(s), including what format any agreed rules or practices should take;
- seek consensus on the most appropriate way to progress the development of solutions; and
- facilitate communication between aggregators and financial institutions, which in turn could lead to the development of industry solutions on issues such as identification and audit trails.

Table of contents

Section 1

Introduction

Account aggregation services allow consumers to view account information from different institutions on the one webpage. Aggregation services collate information from a consumer's deposit accounts, credit accounts, managed funds accounts, and/or brokerage accounts, thus giving an overall picture of the consumer's finances. Often, they also collate non-financial information, such as information from email accounts and frequent flyer accounts.

Account aggregation is a service that is becoming increasingly prevalent in the United States, although there are different views on the size of the consumer uptake. One source estimated that there were 1 million users of aggregation services in the United States in April 2000.[2] Another estimated that use of aggregation services expanded from 10,000 in January 2000 to 700,000 in December 2000,[3] while a third estimated that use would expand from 1 million users in 2001 to 22 million users by 2003.[4]

Aggregation services are now also appearing in Australia. By the end of 2000, there were a small number of account aggregation services available to consumers. We understand that other organisations, including financial institutions, are looking closely at providing such services.

Aggregating financial account information raises significant consumer issues, including issues of liability, disclosure, privacy and security.

ASIC is responsible for consumer protection regulation in the financial services sector. We are keen to ensure that the consumer issues associated with account aggregation are adequately addressed while the products are being developed and established. Early discussion of the consumer issues will encourage solutions that can be incorporated into business plans and product characteristics.

To facilitate discussion, we have surveyed and reviewed information about current and proposed account aggregation services in Australia, including their terms and conditions and other documentation.[5] We have also examined some of the

---

[2] US Bancorp Piper Jaffray study, quoted at http://www.ira.com/ref/general/news-981062601.632.html. (viewed 1/5/01).

[3] Altman L et al, "Run for the money: The battle for online aggregation business", *enews – Developments in strategy and business*, 2001, available at http://www.strategy-business.com/enews/011501/enews011501.html.

[4] Morgan Stanley Dean Witter study, cited in Altman, L op.cit.

[5] One aggregator released revised terms and conditions shortly before this paper was released. Due to time constraints, these new terms and conditions were not fully reviewed. However, where relevant to the text, the discussion refers to the provisions of the revised terms and conditions.

aggregation services offered in the United States for comparison. To complement this information, we have reviewed additional information and views from aggregation suppliers, industry organisations, consumer organisations, and regulators, both here and in other jurisdictions (primarily the United States). We have also received information and assistance from Australian regulators, including the Office of the Federal Privacy Commissioner (OFPC), the Australian Prudential Regulation Authority (APRA), the Reserve Bank of Australia (RBA), the Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Australian Competition and Consumer Commission (ACCC).

This paper presents the results of the survey, undertaken in November and December 2000, and updated in April 2001. It summarises the major consumer protection issues, and makes some suggestions for addressing these issues.

Section 2

Background

What is account aggregation?

Account aggregators use a type of software that retrieves specified information from accessible web pages. They then collate and display that information onto a single page.

Aggregators can be financial institutions, extensions of existing portals, or third-party Internet companies.

In theory, there is no limit to the type of information that can be collated by an account aggregation service. However, the information accessed generally falls into two types:

- information that can only viewed by entering a username and password (eg financial account balances, frequent flyer point balances, personal email accounts, etc); and
- information that is publicly available (eg lifestyle information such as news, weather, travel specials, stock quotes, store specials, etc).

To register with and use an aggregation service, a consumer needs to:

- nominate a username and password to access the service;
- nominate websites and the information to be collected from those websites; and
- enter the consumer's username and password for each website where the consumer must be identified before the personal information can be retrieved.

Once registered with an aggregation service, the consumer can access all of their nominated financial and other information simply by logging onto the aggregation service. Thus, the consumer needs to remember only one username and password.

Account aggregation services can, and do, provide user-nominated non-financial information. However, most promote their service as being of greatest value for managing a consumer's financial information.

For example, here is how one aggregation service to be offered in Australia promotes itself:

"This revolutionary service:

- *Consolidates all your account information onto the one page.*
- *Provides you with a quick, easy snapshot of your finances.*
- *Provides easy and secure access to banks, credit cards, investments, email and brokerage accounts.*
- *Makes life simpler – you only need to remember one password."*[6]

At this point in time, account aggregators do not generally provide consumers with the ability to make transactions on their online accounts through the aggregation service. We found only one service (in the United States) that offered transaction capabilities, although it was not clear whether this functionality arose out of the aggregation technology or a separate product.

However, it is expected that in the future, transaction functionalities will be incorporated into aggregation services.

What are the consumer benefits from account aggregation?

Promoters of account aggregation assert that these services provide great benefits to consumers – in convenience, flexibility, and more efficient personal financial management.

For example, one study in the US has suggested that average households could save almost $1700 a year by aggregating consumer financial services, with savings generated by managing saving and borrowing more skilfully, purchasing from the most competitive provider, and paying bills when they are due (i.e. not unnecessarily early or late). The study also suggested that more affluent households could save much more.[7] Account aggregation services can provide consumers with an overall picture of their financial affairs, thus creating an environment that makes better management, and these sorts of savings, easier.

By viewing all of their accounts and other information at one place, consumers can save time. In addition, as only one password is needed to access the aggregation service, consumers do not need to remember or record the various passwords and usernames that are needed for each of the relevant websites. We understand that most aggregation services can pre-load a consumer's password and username into a financial institution's login page so that the consumer can directly access the site and make transactions.

---

[6] Promotion for Account Master, offered by ninemsn, http://finance.ninemsn.com.au/money/accountmaster/introduction.asp (viewed 3/05/01).

[7] Singer M, Stephenson J and Waitman, R, 'Click and save', *MaKinsey Quarterly*, 2000, available from www.mckinseyquarterly.com/electron/clsa00.asp.

Services offered in the foreseeable future through aggregation providers might include:

- online, real-time transaction capabilities;
- electronic bill notification and payment; and
- ability to purchase products.[8]

It is also possible that aggregators could ultimately provide:

- cash management and financial planning services;
- tailored financial advice;
- intelligent agents that can complete tax forms, loan applications, and other documents;[9] and
- automatic financial analysis and decision making, eg automatically analysing aggregated information and – based on a customer's financial goals and risk tolerance – reallocating assets as needed to maximise value and return.[10]

Consumer attitudes to aggregation services

Consumer attitudes to account aggregation services have been surveyed by a number of organisations in the United States. These include a Star Systems Inc survey of 705 consumers who had previously expressed an interest in online banking (August 2000),[11] and a BoozAllen Hamilton survey of 1001 users of aggregation services, and 1900 general Internet users (January 2001).[12]

The Star Systems survey confirms that the use of aggregation services is still fairly low (7% of those surveyed),[13] although more than one-third of those surveyed were very familiar or somewhat familiar with the services.[14] Almost one-third of respondents who did not use an aggregation service said that they were very likely or somewhat likely to use an aggregation service in the future.[15]

The most common reason for using an aggregation service offered by potential users was "easy/one stop access to financial information" (46%). Other reasons

[8] Star Systems Inc, *Web aggregation:* a snapshot, August 2000, p. 7. Available from www.star-system.com.

[9] "Yodlee unveils next generation of online aggregation; debuts powerful advice, analysis and transactional capabilities", Yodlee media release 11/12/00, available from www.yodlee.com.

[10] Star Systems Inc, op.cit., p. 7.

[11] Star Systems Inc, op.cit.

[12] Altman, L et al, op.cit.

[13] Star Systems Inc, op.cit. p30.

[14] Star Systems Inc, op.cit. p 29

[15] Star Systems Inc, op.cit. p. 32.

were convenience (23%), saving time (10%), less hassle (10%) and because they preferred to do things online (9%).[16]

Of those already using an aggregation service, the two main reasons for using it were "easy/one stop access to financial information" (38%) and convenience (35%).[17]

In contrast, the main reasons for consumers not using an aggregation service were concerns about security (33%), concerns about privacy (16%), a lack of trust in general (14%), and a preference for going directly to a financial institution's website (13%).[18]

Many current (41%) and potential (55%) users preferred to use an aggregation service provided by a financial institution.[19]

In the Star System survey, the main reasons for preferring a financial institution aggregation service were "the financial institution is more responsible/more trust in them" (52%), and "security of financial information" (22%).[20]

In the BoozAllen Hamilton survey, those respondents who used an aggregation service tied to a financial institution cited their existing relationship with the financial institution (68%) or the degree of trust (25%) as the reason for using that service.[21]

However, the surveys did not show an overwhelming preference for aggregation services provided by financial institutions:

- In the Star System survey, one third of respondents said that it would make no difference whether the service was provided by a financial institution or by a third party internet company;[22]
- In the BoozAllen Hamilton study, one-third of those using aggregation services used a service that was not tied to a major financial institution.[23]

In the BoozAllen Hamilton study, users of aggregation services provided by portals or non-financial businesses based their decision on the fact that it was the first aggregation site they had found (26%), or on their level of trust in the company or site (24%).[24]

---

[16] Star Systems Inc, op.cit. p. 33.

[17] Star Systems Inc, op.cit. p. 34.

[18] Star Systems Inc, op.cit. p. 36

[19] Altman et al, op.cit; Star Systems Inc, op.cit. p. 37.

[20] Star Systems Inc, op.cit. p. 38.

[21] "BoozAllen releases first in-depth study of consumers who use account aggregators to consolidate all their financial accounts onto a single webpage", BoozAllen and Hamilton media release 18/01/01, available from www.bah.com.

[22] Star Systems Inc, op.cit. p. 37.

[23] Altman, L et al, op.cit.

[24] BoozAllen and Hamilton media release 18/01/01, op.cit.

The BoozAllen Hamilton study also found that, of those surveyed who used portal or non-financial businesses for their aggregation services, 36% spent less time at the websites of their own financial institutions, and 9% stopped visiting these sites entirely.[25]

The Star System survey found that issues such as privacy, liability for unauthorised transactions, and compliance with federal banking regulations, were either very important or somewhat important for the vast majority of those surveyed.[26]

In terms of functionality of aggregation services, both the Star System and BoozAllen Hamilton surveys showed that interest in the ability to make transactions is high, but not overwhelming.[27]

Finally, the BoozAllen Hamilton study found that a high percentage of current and potential users of aggregation services are relatively young, with incomes between US$50,000 and $149,000. On average, users aggregate nearly 5 accounts, of which nearly half (41%) are financial accounts.[28]

Why are businesses offering aggregation services?

There are a number of reasons why account aggregation services are attractive to businesses – in both the financial services sector and other sectors.

First, account aggregation services can increase the attractiveness of a site. Such services can increase the overall number of visitors, the duration of visits, and the number of repeat visits. If an effective aggregation service is provided on a website, consumers will have less need to leave the website in order to view personal information stored by other websites. In fact, as noted earlier, the BoozAllen Hamilton survey discussed above found that 45% of users of aggregation services provided by non-financial portals either stopped visiting, or reduced the number of visits to the sites associated with traditional financial institutions.[29]

Establishing an aggregation service can also be a defensive mechanism for financial institutions wanting to reduce the likelihood of losing their customers to an aggregation service provided by another financial institution or by a portal. As an officer from the US Office of the Comptroller of the Currency has noted:

---

[25] Altman, L et al, op.cit.

[26] Star Systems Inc, op.cit. p. 39 – 41.

[27] Star Systems Inc, op.cit., p. 41 (57%); BoozAllen and Hamilton media release 18/01/01, op.cit., (49%).

[28] BoozAllen and Hamilton media release 18/01/01, op.cit.

[29] BoozAllen and Hamilton media release 18/01/01, op.cit.

> "… banks could lose important opportunities and face some risk of being relegated to mere data providers if they do not make account aggregation available to customers who are in the market for such services. Put starkly, the choice for banking organizations may be to aggregate, or be aggregated."[30]

Of course, the more time a consumer spends on a website, the greater the opportunities for advertising revenue and/or product promotion.

Account aggregation creates opportunities for targeted marketing and product promotion. Subject to any privacy and security policies promoted by the aggregation service, the information aggregated on the website by a consumer can be analysed to identify whether other products may be suitable for the consumer. The BoozAllen Hamilton study found that 90% of aggregation customers would find personalised offers of additional financial services very or somewhat valuable.[31]

Australian aggregation services have already recognised the marketing and promotion opportunities created by aggregation. One company has noted:

> From a market share perspective, capturing a user's aggregated data, with the user's permission, will provide an institution with the first real insight into a consumer's wallet. Knowing what other products and services a consumer has with other providers presents a huge opportunity for institutions to target and more importantly cross-sell to high value customers.[32]

In the future, it is also possible that account aggregators could use a consumer's aggregated information to provided targeted financial advice or information – perhaps at a cost. Again, offering such services would be subject to relevant privacy and security policies and customer permission.

In the long term, when the functionality of aggregation services expands, commissions and referral fees may provide a significant part of the business case for aggregation services.[33]

Some businesses that offer an aggregation service also provide aggregation software to third parties. For these businesses, we assume that a large part of their revenue will be generated by license and other fees paid by those who are using the software.

---

[30] Julie L Williams, 1st Senior Deputy Comptroller and Chief Counsel, Office of the Comptroller of the Currency, *The Impact of Aggregation on the Financial Services Industry*, Speech to the American Banker's 2nd Account Aggregation conference, 23/04/01.

[31] BoozAllen and Hamilton media release 18/01/01, op.cit.

[32] Robert King (Chief Executive of Financial Enrichment Pty Ltd), "Account aggregation the next 'killer application'", *Australian Banking and Finance*, 31/3/01, p.16.

[33] Altman, L et al, op. cit.

How does account aggregation work?

Currently, account aggregators gather a consumer's account and other information in one of two ways – screen scraping or direct feed.

Screen scraping does not require the involvement, or even knowledge, of the financial institution from which account information is sought. Using the consumer's account number, password and username, a screen-scraper becomes electronically indistinguishable from the actual account holder. For each account nominated by the consumer, the screen-scraping software enters the consumer's username and password, collects the information that would be available to the account holder, and displays the data on a single web page for the consumer.

In Australia, there are currently two distinct aggregation models using screen-scraping technology – the third party model, and the user-driven model.

In the third party model, the consumer's account details (including username and password) for each of their nominated accounts are stored on the server of the aggregation service provider or the aggregation technology supplier. The information collected using screen scraping is stored on the aggregator's server, and is collated by the aggregator for presentation to the consumer.

In the user driven model, consumer's account details are stored in a digital safe on the consumer's PC. The consumer activates the aggregation application on their PC, and the application uses the account details to 'scrape' the nominated sites. The balance and other information collected is collated and displayed onto a single page.

Account information can also be collected by aggregators using a direct feed arrangement. In this situation, the aggregator enters into formal agreements with financial institutions where the information originates. When the aggregator requests access to consumer information, the financial institution concerned confirms that the aggregator is authorised to access that information (demonstrated by the fact that the aggregator has the consumer's account number, password, and username). If confirmed, the financial institution transmits the account information to the aggregator using a standard communication protocol. The aggregator then displays this information to the account holder through its website.[34]

Direct feed provides the benefits of security, currency, and reliability for all parties. However, it may be costly and time-consuming for aggregators to establish direct feed arrangements with each of the institutions that it wishes to access information from.

In contrast, screen scraping does not require any involvement or authorisation from the original institution. It can therefore be an attractive option for aggregators wishing to be able to quickly offer access to information from a large number of institutions.

[34] See also Star Systems Inc, op.cit., p.4-5 for more details.

However, one disadvantage of using the screen-scraping process is that whenever the account institution's website is reconfigured, specific data fields may be moved. In those circumstances, inaccurate or incomplete data may be collected and displayed to the consumer until such time as the software can be brought up to date with the reconfigured screen.

Also, screen-scraping technology that uses batch processing to retrieve account information[35] can also place a high demand on a financial institution's computer systems, thus detrimentally affecting the system's speed.

The vast majority of account aggregation services surveyed use screen-scraping, rather than direct feed. However, we understand that experts expect that direct feed arrangements will dominate in the longer term.[36]

---

[35] Eg the aggregation service 'scrapes' account information for all of its customers at a certain time each night. Aggregation using the third party model commonly uses batch processing.

[36] ASIC consultations with Australian aggregators and financial institutions.

Section 3

Account aggregation services in Australia

This section of the report details the results of our survey on the current availability and functionality of account aggregation services in Australia. The survey was conducted between November and December 2000, and the results were updated in April 2001.

Current providers of account aggregation

To assess the availability of account aggregation services in Australia, we reviewed the websites of:

- all banks licensed in Australia;
- approximately half of the building societies and credit unions that are licensed in Australia and have an internet presence;
- all Australian online brokers; and
- all known aggregation sites that have an Australian domain name, and are not associated with a financial institution.

Appendix A shows the number and type of sites surveyed and Appendix B shows the URLs of the sites surveyed.

We found that, at this time, there are only a small number of businesses providing account aggregation services (see Table 1). Of these:

- two are hosted or provided by financial institutions;
- one is hosted by a stockbroker;
- two are retail or other portal sites that offer another service provider's product; and
- one is an application development company.

Table 1 also includes information about another aggregation service that is currently being promoted on a portal site and is due to be launched during 2001.

There are also some financial institutions that provide, on one web page, information about all of a consumer's accounts with that institution. These services can be offered as part of the normal Internet banking service, or as a separate product. Some of these services also include user-specified non-financial information (eg news, weather, stock prices, etc).

However, these types of services can be provided without aggregation or screen-scraping technology. We have therefore not considered them in this paper.

As at April 2001, the three main account aggregation service providers in Australia were:

- AMP Limited (Account Minder);
- eWise.com.au Pty Ltd;
- Financial Enrichment Pty Ltd (a subsidiary of Macquarie Bank).

Our survey also found that there are only a small number of technology suppliers used by the current aggregation services in Australia, namely:

- VerticalOne Australia Pty Limited;[37]
- Teknowledge Corporation (represented in Australia by Sybase Australia Pty Ltd);
- eWise.com.au Pty Ltd.

We understand that the proposed aggregation service to be offered by ninemsn will use a fourth technology supplier – Parkers' Edge Pty Ltd.

Table 1 – Aggregation service providers and technology suppliers present in Australia

Aggregation service provider			Aggregation Type	Aggregation product name	Technology supplier
Diversified Financial Institution	1.	AMP Limited	Financial & non-financial accounts	Account Minder	VerticalOne Australia Pty Limited
	2.	Financial Enrichment Pty Ltd (a subsidiary of Macquarie Bank Limited)	Financial & non-financial accounts	Enrichment	Teknowledge Corporation (represented in Australia by Sybase Australia Pty Ltd)
Broker	3.	Egoli.com.au (published by SHAW Stockbroking Limited and Harold Milner, a proper authority holder for SHAW)	Financial & non-financial accounts	My Accounts	eWise.com.au Pty Ltd
Aggregation supplier	4.	eWise.com.au Pty Ltd	Financial & non-financial accounts	eWise	eWise.com.au Pty Ltd
Retail site	5.	SheSaid Pty Ltd	Financial & non-financial accounts	Enrichment (links directly to Financial Enrichment service)	Teknowledge Corporation (represented in Australia by Sybase Australia Pty Ltd)
Non-financial portal site	6.	Free Online Australia Pty Ltd	Financial & non-financial accounts	Enrichment (links directly to Financial Enrichment service)	Teknowledge Corporation (represented in Australia by Sybase Australia Pty Ltd)
	7.	ninemsn Pty Ltd (available May 2001)	Financial & non-financial accounts	Account Master	Parkers' Edge Pty Ltd

We understand that other financial institutions and portals are actively considering offering account aggregation services in the near future.

[37] In the United States, VerticalOne Pty Limited has merged with another technology supplier Yodlee.com, Inc. (See "Yodlee and VerticalOne deal closes", Yodlee media release 17/01/01, available from www.yodlee.com.)

At this stage, it appears that there has not been a large take-up of aggregation services by Australian consumers. One source suggested in April 2001 that there were about 5000 account aggregation users in Australia.[38] However, there are predictions that use will rapidly increase over the next few years.

Functionality of Australian aggregation services

All of the account aggregation services currently operating in Australia can aggregate information about:

- deposit and transaction accounts;
- loan accounts;
- credit card accounts;
- managed funds; and
- broker accounts.

However, the number of accounts that can be aggregated is limited by the design of financial institution websites and the time required to test interfaces.

Most of the aggregation services only offer access to accounts with financial institutions in Australia. However, at least one aggregator appears to provide access to information from some financial institutions in other jurisdictions.

At this time, the aggregation services available in Australia do not have transactional capabilities. In order to make a transaction, a user must leave the aggregation site and enter the site of the institution holding that particular account. The aggregation services usually provide a direct link to the login page of the relevant account provider, and we understand that in many cases, the consumer's login information will be pre-loaded.

Most aggregators in Australia collect account information using screen scraping, and the information is normally updated overnight. However, this information can be refreshed at any time for real-time information.

In contrast, one Australian aggregator uses a user-driven model. In this model, account information is not automatically updated each evening; instead it is refreshed each time the consumer uses the service.

Other functionality of some aggregation services includes the ability to generate reports or alerts to users (for example, an alert when an account balance has reached a specified amount). To date in Australia, only one aggregator appears to have this capacity.

[38] Derkley, Karin "What's happening to aggregation?", *Personal Investor* April 2001.

Only one Australian aggregator has indicated an intention to charge customers for using its aggregation service. Consumers are able to take advantage of a free 2-month trial; after that time, it will cost private users $36 per year.

It is possible that in the future, fees for aggregation services will be introduced more widely, and/or additional features will incur a fee.

Section 4

Account aggregation services in other jurisdictions

Most account aggregation services are located in the United States. The first account aggregation sites appeared in the US in 1999, and a number of financial institutions and portal sites now offer aggregation services.

In contrast, our literature searches suggest that there is little or no availability of account aggregation services in other major English-speaking jurisdictions. One service (AccountUnity) was launched in the United Kingdom in May 2001,[39] and other UK firms are apparently developing aggregation services.[40]

We also found references to the future availability of aggregation services in Canada[41] and New Zealand,[42] however, there were no dates given for launching these initiatives. A fairly basic aggregation service, allowing only aggregation of cheque account information, has also apparently been launched in Spain.[43]

Given the limited availability of aggregation services outside the US and Australia, a range of US sites were surveyed for this report. These, however, represent only a sample of the available services. Table 2 shows that, as is the case with the Australian offerings, there are only a small number of companies providing the technology to support account aggregation.

---

[39] Warwick-Ching, Lucy "Online finance made easier", *Financial Times*, 3/5/01.

[40] Mackintosh, James "FSA will not protect data", *Financial Times*, 16/5/01.

[41] In July 2000, the Royal Bank of Canada announced that it would offer an account aggregation service, including transactional facilities, to its customers (Toonkel, Jessica "Online banking: Royal of Canada nears account aggregation debut", *American Banker*, v. 165, no. 133, p. 14, 13/7/00.). In October 2000, Canada's Bank of Montreal introduced a trial of account aggregation with a small group of its customers (Howlett, Karen, "Big banks roll out personal Web portal sites that collect all of a consumer's financial information and make it available at the click of a mouse are the hottest thing in banking", *The Globe and Mail*, 12/10/00.)

[42] AMP New Zealand has confirmed that "at some point" the AMP screen scraper would be offered in New Zealand, but has not commented on the timing (James Weir, "Site links complete range of AMP's financial services", *The Dominion*, 26/10/00).

[43] "Bankinter becomes first account aggregator in Europe", *Distribution Management Briefing*, 26/02/01, p.4.

Table 2 – Sample of account aggregation services in the US

Aggregation service provider			Aggregation Type	Aggregation product name	Technology supplier
Diversified Financial Institution	1.	Chase Manhattan Corporation	Financial & non-financial accounts	Chase Online Plus	Yodlee.com Inc
	2.	Citicorp Inc	Financial & non-financial accounts	My Accounts	Yodlee.com Inc
Bank	3.	directbanking.com	Financial & non-financial accounts	OneView	Yodlee.com Inc
	4.	EAB (ABN AMRO group)	Financial & non-financial accounts	My Sites	Yodlee.com Inc
	5.	NetBank[44]	Financial & non-financial accounts	OnMoney.com	OnMoney.com
	6.	Wells Fargo	Financial accounts only	Portfolio Manager	VerticalOne Corporation
	7.	Virtual Bank	Financial & non-financial accounts	Virtual View	VerticalOne Corporation
Financial Portal	8.	HD Vest Technology Services Inc	Financial & non-financial accounts	My Accounts	Yodlee.com Inc
	9.	Money Park Inc	Financial & non-financial accounts	Account Minder	VerticalOne Corporation
Aggregation supplier	10.	CashEdge Inc	Financial accounts only	CashEdge Dashboard	CashEdge Inc

Most of the US aggregators surveyed:

- aggregate a broad range of types of financial accounts;
- do not have transactional capabilities;
- collect account information using screen scraping; and
- update account information overnight.

Since the original survey was undertaken, two of the major technology suppliers in the United States (Yodlee.com Inc and VerticalOne Corporation) have merged.[45]

We assume that Australian consumers who hold accounts with relevant US institutions would be able to use aggregation services provided in the US. However, our survey did not find any information that suggested that US aggregators provide access to information from financial institutions based in Australia.

[44] The NetBank product is dual badged: NetBank's name/logo appears on the OnMoney.com site, to which the surfer is taken from the NetBank site.

[45] "Yodlee and VerticalOne deal closes", Yodlee media release 17/01/01, available from www.yodlee.com.

Section 5

Consumer and regulatory issues

Account aggregation services generate a range of consumer and regulatory issues. This section briefly explains these issues.

Disclosure

In order to make an informed choice to use aggregation services in general, or to use a particular aggregation service, consumers need clear, simple and upfront disclosure of relevant information. Good practice suggests that aggregators should provide information on at least the following matters:

- privacy;
- terms and conditions, liability and risk;
- security;
- charges;
- currency of information;
- applicable consumer protection regulations;
- availability of complaints and dispute resolution processes;
- identity of the aggregator; and
- relationship between the aggregator and financial institutions.

Financial institutions should also advise their customers of their attitude to customer use of aggregation services.

Privacy policies

Privacy is a keen concern for consumers, and an aggregator's privacy policy should advise, among other things:

- who has access to the personal information provided by consumers;
- how that information will be used;
- whether that information will or may be sold, or otherwise disclosed, to a third party;
- what steps consumers can take to opt out or opt in to any marketing or cross-selling activities of the aggregator or a third party;
- how consumers can get access to information held about themselves;

- whether and how the site uses with cookies, web bugs, and clickstream data.

Most of the Australian aggregation services do include obvious statements on who has access to customer information, and the purpose for which that information is accessed by the aggregator. However, the survey did not test the quality of this disclosure.

In addition to general privacy policies, aggregators that collect personal information through web-based forms should give consumers specific advice about each particular instance of collection. At the time personal information is collected, consumers should be made aware of:

- the identity of the aggregator and how to contact it;
- the fact that he or she is able to gain access to the information;
- the purposes for which the information is collected;
- the organisations (or types of organisations) to which the aggregator usually discloses information of that kind;
- any law that requires the particular information to be collected; and
- the main consequences (if any) for the individual if all or part of the information is not provided.

Such a statement should be on the relevant webpage or prominently linked to it.

Terms and conditions, liability and risk

It is obviously important that consumers understand the terms and conditions that apply to their use of an aggregation service. Most of the Australian sites surveyed did provide terms and conditions specific to the use of the aggregation service.

Consumers need to clearly understand how liability for loss will be allocated between themselves, the aggregation service, and their financial institutions. A key area of concern is whether, and in what circumstances, consumers will be liable for unauthorised transactions that occur on an account that can be accessed by an aggregation service.

However, it is also important that aggregators explain any other circumstances in which they will accept or disclaim liability for loss. For example, consumers might want to know what liability (if any) will be accepted by the aggregation service if the aggregator's software corrupts the consumer's computer, or if the consumer acts on incorrect information provided through the aggregation service. Often this information about liability is buried in the terms and conditions.

Aggregators should also provide clear and prominent information about the risks in using aggregation services. For example, using one password to access a variety of accounts means that if the one password is compromised, all of a consumer's financial assets may be at risk. This risk is likely to increase as the functionality of aggregation services increase, eg to encompass transaction capabilities.

In addition, most account institutions include in the terms and conditions a requirement that consumers not disclose their PIN or password to a third party. Disclosing a PIN or password to an aggregator may therefore breach the terms and

conditions, and may also mean that the consumer cannot rely on the provisions of the EFT Code of Conduct that limit liability for losses caused by unauthorised transactions. Again, this risk should be prominently disclosed by aggregators.

Some of these liability and risk issues are raised in the terms and conditions or FAQs of Australian aggregators, but there is room for improvement, and better disclosure will facilitate informed decision making by consumers.

Advice on how changes to the terms and conditions will be notified to consumers is also important. Merely posting the revised terms and conditions on the aggregator's site, without drawing specific attention to the change, is not adequate.

Security measures

Aggregators should provide clear information on the security measures taken to safeguard consumer information, both in transmission and in storage. This information should address what method is used to collect account information, how that method works, and the relative risk of that method. Aggregators should also advise of their update schedule.

Aggregators should give the consumer a clear idea of the level of data protection that they can provide against matters such as misuse, loss, unauthorised access, modification and disclosure. Aggregators should also advise where consumer information is stored. For example, whether it is stored within the aggregator's firewall, or with the technology supplier, or in another location (eg the consumer's own PC).

Costs of using the service

As noted above, all bar one of the aggregation services in Australia provide aggregation services for free. However, it is possible that this may change over time, as new services and functionalities are introduced.

As well as information about applicable fees, aggregators that charge fees should also clearly disclose the manner in which fees can be paid, and the consequences (in terms of access to the service and otherwise) of failing to pay the required fees.

Aggregators should perhaps also advise consumers that account institutions might impose fees when an aggregation service makes a balance inquiry or transaction on behalf of the consumer.

Currency of information

In order for the information collected by an aggregator to be useful, consumers need to know how current the information is (i.e. when the information was collected from the financial institution).

Applicable consumer protection regulations

It is important that consumers understand whether any standard consumer protection regulations do or do not apply to the use of the aggregation service. The key regulation here would be the EFT Code. In the absence of specific disclosure, consumers might be entitled to expect that the EFT Code will apply.

In the United States, the National Consumers League has suggested that, until there are common safety, security and privacy standards for all aggregators, they should be required to:

> "disclose on their web sites, in big bold letters, which consumer protection regulations do or do not apply. And the consumer should not have to click a dozen times to get to it – it should be right up front."[46]

The identity of the aggregator

Websites that promote aggregation services should provide information about the legal entity operating the site and, if different, the legal entity providing the aggregation service. The information should include the physical address, other relevant addresses, and relevant contact details.

The relationship between the aggregator and financial institutions

Consumers may assume that, because an aggregator collects information from a particular institution, there is a relationship between the aggregator and the financial institution. This is even more likely where the aggregation service is promoted or hosted by a financial institution. Consumers may also assume that the security and other practices of the aggregator are of the same level as those of the financial institution.[47]

It is therefore important that there is clear disclosure about the relationship between:

- the aggregator and any financial institution that hosts or provides direct links to the aggregator; and
- the aggregator and the financial institutions from which data is collected.

Among other things, this information can assist consumers to assess the risk of using the aggregation service.

---

[46] Star Systems Inc, op.cit., p. 22.

[47] The terms and conditions for one Australian aggregation service make it clear that they are not, however, this clause is not more directly drawn to the attention of consumers.

Complaints process

Finally, aggregators should have clear and accessible information about the process for making and resolving consumer complaints about the aggregation service or its operation. This should include information about any external dispute resolution process that might be available if a consumer is not satisfied with a result of the internal complaints process.

Disclosure by financial institutions

Financial institutions would know that aggregation services are now being provided in Australia. Given this, it is probably good practice for institutions to clearly advise consumers of their attitude towards aggregation services.

In the United States, Netbank's terms and conditions for deposit accounts clearly state the institution's position on consumers using aggregation services. In summary, they warn that account aggregators are not affiliated with Netbank; that consumers who choose to use an aggregator will assume all risks inherent in disclosing their passwords or PINs to a third party, and that Netbank accepts no responsibility for any use or misuse of account data by any such third party.[48]

It is, however, interesting to note that NetBank itself offers a multiple institution aggregation service.[49]

Another example of disclosure by a financial institution comes from the United Kingdom. Here Egg, the e-commerce company created by Prudential, has taken a different approach. The terms and conditions for the Egg card permit customers to disclose their PIN or password to aggregation services that have been approved by Egg. If disclosure is made to an approved aggregation service, then the company will not treat that disclosure as a breach of the terms and conditions.[50]

Both the Netbank and Egg clauses are buried in the terms and conditions documentation, and thus are perhaps not immediately accessible to consumers. However, these institutions are at least beginning to address this issue.

With one exception, our survey did not find any obvious warnings or other information on the websites of Australian financial institutions. The terms and conditions on the website of one financial institution hosting an aggregation service do note that disclosure of personal information to the aggregation service may result in loss of legal rights. However, this clause could be made clearer – for example, it does not explain the nature of the rights that might be lost. The information could also be more directly drawn to the attention of consumers.

---

[48] See http://www.netbank.com/terms_dda.htm (viewed 2/3/01).

[49] See *Account consolidation* http://www.netbank.com/banking_consolidation.htm (viewed 2/3/01).

[50] See http://new.egg.com/visitor/0,2388,3_11087--View_149,00.html (viewed 4/4/01).

Liability for unauthorised transactions and other losses

Unauthorised transactions

There need to be clear and fair rules to protect consumers from unauthorised transactions that occur on accounts that have been accessed through an aggregation service. Unauthorised transactions can occur in a number of different ways, for example they can occur through:

- system malfunction;
- employee or agent fraud;
- disclosure of password to a third party; or
- hacker attack.

In addition, in some cases, there may be no clear cause of the unauthorised transaction. It is worth noting that appropriate record keeping practices (including retention of session information) by account aggregators and financial institutions should, among other things, assist in determining the cause of an unauthorised transaction.

The way in which an unauthorised transaction has occurred will be relevant to assessing the question of who should be liable for that transaction. Depending on the cause of the unauthorised transaction, it might be most equitable to impose liability on the aggregator, the financial institution holding the account in question, the consumer, or some combination.

However, there is currently no regulation or other document that governs liability and other relationships between financial institutions, aggregators and consumers. In order to understand where liability will fall in the event of unauthorised transactions, the liability rules between aggregators and consumers and between financial institutions and consumers need to be considered separately.

In allocating liability for an unauthorised transaction between a consumer and an aggregator, the normal laws of contract will apply, as there are no regulatory or self-regulatory rules applicable. In practice, this means that aggregation services are generally free to set the terms and conditions for liability.

Our survey found that a number of aggregation services expressly disclaimed any liability for losses caused by unauthorised transactions. Others did not have a specific clause covering unauthorised transactions; however, they had a general disclaimer of liability for loss occurring through the use of the service.

However, one aggregator (in its recently revised terms and conditions) specifically accepts liability for losses caused by unauthorised transactions that are caused by the aggregator's negligence or wilful misconduct concerning the security of the storage of account information. Liability is capped at $100,000.

In most cases then, it appears that liability for unauthorised transactions will be borne by consumers rather than aggregators. In these circumstances, could a consumer transfer this liability to their financial institution?

Rules for allocating liability between consumers and financial institutions where an unauthorised transaction occurs are detailed in the EFT Code. The relevant provisions of the Code are generally incorporated into the financial institution's terms and conditions.

Under the EFT Code, consumers who disclose their PIN or password to a third party will generally be liable for losses caused by an unauthorised transaction that resulted from the disclosure. As explained earlier in this paper, disclosure of PINs or passwords to a third party (eg the account aggregator) is an integral part of some aggregation services.

However, we understand that the user driven model of account aggregation is a non-disclosure model and does not involve deliberate disclosure to a third party because the account information is stored on the consumer's own PC.[51]

Question for consideration

1. Do financial institutions regard a consumer's use of the user driven model of account aggregation as involving a disclosure of their PIN or password to a third party?

The revised EFT Code (released in April 2001) modifies, in some limited circumstances, the operation of the current contractual provisions on liability. The Code includes a qualification to the rule that a consumer may be held liable for unauthorised transactions if he or she has disclosed the PIN or password (clause 5.6):

> 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.

In this clause, an account access service will include an aggregation service.

An examination of the current liability allocation rules between aggregators and consumers, and between financial institutions and consumers shows that, where there is disclosure to a third party, and unless the circumstances in clause 5.7 of the revised EFT Code apply, consumers will be most likely to wear liability for losses caused by any unauthorised transactions.

In private briefings to ASIC, individual aggregators have indicated that they would accept liability if loss arose from negligence or poor performance on their part, and the revised terms and conditions of one aggregation service also incorporate a term

---

[51] *Executive Summary* provided by eWise to ASIC on 22/11/00.

along these lines. However, it would be preferable if all aggregators included in their terms and conditions and other documents the circumstances in which they will accept liability for loss or damage.

There is also a need for a proper public debate on a fair allocation of liability in cases of unauthorised transactions. The current situation appears to place most liability for loss on consumers. This is similar to the situation at the time of the introduction of debit cards and ATM and EFTPOS devices. A primary driver for the development of the original EFT Code was to more equitably share the burden for losses arising from unauthorised transactions.

Whatever the allocation of liability might be, it is important that *financial institutions* advise their customers whether the use of an aggregation service (whether a third party model or user driven model) will be regarded as a disclosure of the PIN or password in breach of the customer's terms and conditions if an unauthorised transaction occurs.

Encouraging breaches of terms and conditions

A related issue is that, by asking consumers to disclose their passwords, aggregators are arguably encouraging consumers to breach their agreements with their financial institutions. In our survey, we found that only one Australian aggregator explains (in its terms and conditions) that financial institutions may not endorse the practice of disclosing PINs or passwords to a third party. It advises consumers who are unsure to seek permission from their financial institution before disclosing their account information to the aggregator. Of course, institutions will need to establish clear policies and systems to ensure that a consistent response is given when such a request is made.

Similarly, it is arguable that it may not be appropriate for aggregators to offer access to a financial institution's information in circumstances where it knows, or should know, that the particular institution does not allow consumers to disclose their information to an aggregator.

Choosing and safeguarding aggregator passwords

Most financial institutions in Australia publish general guidelines for choosing and safeguarding passwords in the context of EFT transactions. Currently some aggregators provide similar guidance for aggregator passwords and usernames. However, there is no consistent approach and some of the guidance is relatively limited.

In assessing appropriate liability rules for unauthorised transactions, it will be important to give consideration to what, if any, obligations should be placed on consumers to protect their password and usernames for accessing the aggregator service. Similarly, consideration will need to be given to what, if any, liability should be imposed if a consumer fails to safeguard this information and an unauthorised transaction occurs.

Other losses

Many aggregation services in Australia and in the United States include in their terms and conditions a general disclaimer of liability for losses caused by using the service. Aggregators exclude liability for matters such as:

- representations made by or through parties found at, on, through or from the service;
- the timeliness, accuracy, reliability, and completeness of the information provided by the service;
- inaccuracies, omissions, errors or delays in the service;
- non-performance or interruption of the service;
- the quality of the service;
- the user's access, use, or interaction with the service;
- downloading material from the service.

These general disclaimers might also govern liability for fraudulent or unauthorised transactions that are not EFT transactions (eg unauthorised share trades).

Most terms and conditions also disclaim liability – to the extent possible – under any express or implied conditions or warranties.

Finally, a number of the terms and conditions also try to limit the aggregator's liability for loss to a specific amount or remedy, for example, to resupply of the service, or the cost of resupplying the service.

The survey shows again that the terms and conditions of aggregation services transfer most responsibility for loss away from the aggregation service to the consumer. Implied statutory conditions and warranties, such as those in s. 12ED of the ASIC Act or s. 74 of the Trade Practices Act, may reduce the effects of these wide disclaimers in individual circumstances, where a consumer has the knowledge and resources to pursue a dispute. However, it would be preferable if the terms and conditions reflected an appropriate and fair weighting of liability.

Privacy

Some key privacy issues for consumers using account aggregation services are:

- is there a clear and obvious privacy statement?
- what personal and account information is collected and/or stored by the aggregator?
- who has access to personal and account information (including passwords, usernames, balances and types of accounts)?
- how will personal and account information be used by the aggregator?

- will personal and account information be used for cross selling by the aggregator or a third party?[52]
- if so, will an opt-in or an opt-out system be used for consumers who do not want their information used in this way?
- will the aggregator sell or otherwise disclose personal and account information to a related business or a third party, with or without consumer consent?
- does the privacy statement address the security risks of transmitting personal information over the Internet?
- what happens to personal and account information if a consumer chooses to discontinue using the service?
- will the privacy statement continue to have effect if the aggregation service goes into liquidation?[53]

The Star Systems survey referred to earlier found that 79% of those surveyed were very concerned about the privacy or security of their personal financial information available on the Internet, and 15% were somewhat concerned.[54]

Each of the Australian aggregator sites surveyed did have an obvious privacy statement. In some cases, it was the privacy statement for the overall site, and was not specific to the aggregation service.

However, the content and detail of these statements varied. In general, disclosure about privacy issues was generally good. The majority of the questions listed above could be answered by reading the privacy statement of an aggregation service.

However, issues relating to the fate of personal information if the consumer chooses to discontinue the service, or if the aggregator goes into liquidation, were not generally addressed in the privacy statements. This is an area that could be improved. Information about the risks of transmitting personal information across the Internet was also not always provided in a clear and direct manner.

In addition, not all aggregators offered the same level of privacy standards to consumers. For example, a number of aggregators used customer information for cross-selling their own products and services unless a consumer specifically requests that their information not be used in this way. However, privacy advocates (including the Office of the Federal Privacy Commissioner) consider that an 'opt in' approach is more acceptable when it comes to use of customer information for unsolicited marketing. In particular, a 'tick-box' on a web page should not default to an indication that the consumer is willing to accept direct marketing material.

---

[52] A US survey showed that consumers would not want to use aggregation services if they were subject to a barrage of marketing messages about new products. Toonkel, Jessica "As aggregation gains, doubt on cross-selling", *American Banker*, 19/9/00. But compare the results of the BoozAllen survey (BoozAllen Hamilton media release 18/01/01, op.cit.).

[53] In the US, a company tried to sell its customer database to raise cash during bankruptcy proceedings, despite its privacy commitment not to disclose this information to third parties See http://www.thestandard.com/article/0,1902,21425,00.html (viewed 03/05/01).

[54] Star Systems Inc, op.cit., p. 31.

A similar approach should apply for any third party disclosures or direct marketing from third parties.

There may also be room for improvement in the statements to the extent that they disclose the use to which the customer's information will be put.

The Privacy (Private Sector) Amendment Act 2000 will come into effect on 21 December 2001. The Office of the Federal Privacy Commissioner has advised that, in its view, aggregators will be subject to the provisions of this Act, and will have to comply with the National Privacy Principles in Schedule 3 of the Privacy Act. These privacy principles relate to the collection, use and disclosure, data quality, data security, openness, accuracy, and correction of personal information. Other principles apply to identifiers, anonymity, transborder data flows, and sensitive information.

The Privacy Act provisions, however, may have limited application if a consumer is using an aggregation service that is based overseas.

Security

For consumers, security issues include the security of their information as it is transmitted when the aggregation service is used, and the physical and electronic security of the location where account information is stored.

It is pleasing to see that each of the surveyed sites in Australia gave assurances and explanations as to the security of their aggregation facility or their online access generally. However, it may be difficult for consumers to assess whether the disclosed security standards provide an appropriate level of protection. Security requirements are not controlled by industry or government standards, and there is therefore the potential for different levels of security standards to apply.

As noted earlier, most aggregators use screen-scraping methodology. However, information collected over the Internet through screen scraping may also be less secure than information collected by direct feed over a telephone line.[55]

The consequences of a security breach may be very serious for consumers, aggregators and financial institutions. For example, breaching the security of the storage facility for account information would provide access to account information, including usernames and passwords, to a large number of consumer accounts.

In the user driven model of account aggregation, we understand that there is no centralised storage of usernames and passwords. Instead, account information is stored on the consumer's PC in an encrypted form, with the decryption key held on the aggregator's server. However, the security and system integrity of the consumer's PC and connection to the Internet will also be relevant.

[55] Star Systems Inc, op.cit., p. 9.

Whatever aggregation method or model is used, robust security protection should be applied to passwords, usernames, and PINs.

Consumer education

Account aggregation services are new to Australian consumers, and there is likely to be some uncertainty about how they operate. Consumer education initiatives that help consumers to understand:

- how aggregation services work;
- what risks are involved;
- how any risks can be minimised;
- the general relationship between aggregators and financial institutions; and
- what questions they should ask when considering using an aggregation service;

would assist consumers to make informed choices about these services.

Those developing consumer education initiatives on aggregation services will need to have regard to existing consumer messages regarding the security of passwords, and ensure that the messages given on account aggregation are consistent with consumer responsibilities. For example, one commentator has noted:

> "Banks have spent a lot of time over the years teaching people not to give our their personal identification numbers. … Now we are going to tell them to give us all of their PINs and we will put all of their information together."[56]

The more functionality that aggregation services provide, the more consumer education will be needed.

Consumer education is a responsibility of industry, consumer affairs agencies, regulators, and consumer organisations.

Complaints and dispute resolution

It is now well accepted in Australia that companies in the financial services sector should generally provide their customers with access to effective procedures for handling and resolving consumer complaints. Given the novelty of aggregation services, and the potential risks involved for consumers, it is important that aggregation services also have effective complaints procedures.

The terms and conditions and other information available on the surveyed aggregator sites in Australia did not include any information on procedures for dealing with complaints about the aggregation service. In addition, only one

[56] Toonkel, Jessica "As aggregation gains, doubt on cross-selling", *American Banker*, 19/9/00..

aggregator provided information on responsibility for handling complaints and disputes.[57]

Where a financial institution with an already established complaints procedure provides an aggregation service, we expect that the procedure would be able to deal with complaints about the aggregation service. In addition, we would hope that any external dispute resolution scheme to which the institution belongs would also be able to accept complaints about the aggregation service.[58]

In this case, information about the complaints process might be found on the main website of the financial institution. However, it is also important to provide this information more directly to users of the aggregation service – for example, by providing an obvious hotlink from the aggregation web page to the complaints information. This will be particularly important if there are customers of the aggregation service that do not otherwise have a relationship with the hosting institution.

There are currently no legal or self-regulatory requirements for non-financial institution aggregators to provide their customers with access to internal or external complaints handling procedures.

The Best Practice Model for E-commerce does include some basic standards on complaints handling, however, this Model has not, to our knowledge, been adopted or implemented by any of the Australian aggregation services.

The proposed Financial Services Reform Bill (FSRB) will make it compulsory for financial institutions to have approved internal and external dispute resolution schemes. However, it is not clear whether the FSRB requirements will apply to account aggregators.

Another issue that may arise in the case of complaints about unauthorised transactions is a failure by both the aggregator and the account institution to accept responsibility for dealing with the complaint. In the context of complaints about EFTPOS transactions, there had been concerns that the merchant and the financial institution involved have each alleged that the other is responsible for investigating the matter. To overcome this, the EFT Code was amended in 1998 to introduce a requirement that account institutions not require customers to raise their complaints with agents or others in the network (see clause 8.3). This provision has been carried over to the revised EFT Code (2001).

The fact that aggregators do not necessarily have formal agreements with account institutions may make it more difficult to address this issue than it is in the EFT Code. In addition, neither the aggregator nor the account institution may have the authority to seek information from the other that might assist in investigating or resolving the complaint. Finally, the current privacy statements of both aggregators

---

[57] The terms and conditions for this aggregation service specifically note that concerns about unauthorised transactions or errors in third party information should be raised directly with the third party operator.

[58] A preliminary view from the office of the Australian Banking Industry Ombudsman is that the office would have jurisdiction to examine complaints about an aggregator if the aggregator were hosted by a bank.

and financial institutions would probably make it difficult to share information for the purpose of investigating or resolving a complaint. Institutions and aggregators may need to consider whether their privacy statements should be amended to facilitate complaints handling.

Cross-jurisdictional issues

Depending on the manner in which an aggregation service is established, the consumer may have a contractual relationship with the technology supplier and not the service provider (i.e. the financial institution or portal offering the service).

As noted earlier, disclosure of the entity that is providing the aggregation service is important.

However, other issues could potentially arise in circumstances where the promoter of the service does not provide the aggregation service. For example, many of the suppliers of aggregation technology are based in the United States. If the consumer's contractual relationship is with a technology provider based outside Australia, it may be difficult for the consumer to resolve any complaints or disputes that arise.

Whether the contract between the consumer and the technology provider is governed by the law of Australia (or of a jurisdiction within Australia) or is governed by the law of another country will normally be detailed in the contract or terms and conditions. It is not generally mandatory for the jurisdiction clause to specify that the contract be governed by Australia law, or that Australian courts and tribunals have jurisdiction to hear disputes. It is therefore possible that a consumer could find that the law of another country governs their contract. In those circumstances, any action for breach of contract may have to be commenced in an overseas court.

Additionally, if consumer account information is stored outside Australia, for example, because the technology provider is located outside Australia, consumers may have difficulty enforcing any rights if the information is disclosed to a third party or otherwise misused.

Of course, if an overseas-based aggregator offers services to Australian consumers in Australia, it will be subject to the general consumer protection laws in the ASIC Act or Trade Practices Act, such as the prohibition against misleading or deceptive conduct. However, enforcing an order from an Australian court can be difficult if the party concerned is not based in Australia, and has no assets in Australia.

Where the aggregation service involves some direct legal relationship between the local consumer and a foreign technology supplier, ASIC would normally expect any local financial institution hosting or endorsing the aggregation service to take a measure of responsibility for that relationship and to act as a 'go-between' should any problems arise, in addition to fulfilling its own legal responsibilities.

Cost of aggregation services and debt recovery

Although the majority of aggregation services do not currently charge fees for use of the service, it is possible that this will change over time and as the functionality of aggregation services increases.

However, even in the absence of direct charging by aggregation services, it is possible that the use of aggregation services will not be free to the consumer. For example, the financial institution could charge fees for balance enquiries and other requests for account information. It is important that consumers are aware of the potential (if any) for such fees.

If an aggregation service begins charging fees, it will be important for it to consider how those fees might be recovered if they are not paid.

For example:

- Could a third party aggregator deduct the fee from one of the consumer's accounts without specific authorisation?
- If the consumer uses an aggregation service provided by a deposit-taking institution, would the institution be entitled to deduct the fee from the consumer's account with that institution under its right to combine accounts?
- Would an aggregator be able to deny access to the aggregation service if a fee is unpaid?

Aggregators will have to ensure that their policies for debt recovery are both fair and clearly disclosed.

Regulation of aggregators

If account aggregators were to offer transactions services through their sites in addition to information services, this could broaden the risk, privacy and security issues.

For example, there would be nothing to prevent a business offering an aggregation service with limited privacy and security procedures in place, limited capital to cover any losses, and limited insurance to protect from loss. In the virtual world of the Internet, consumers would not necessarily be able to distinguish these aggregators from more reputable operators.

As well as the consumer and disclosure issues for which ASIC carries regulatory responsibility, the operations of account aggregators facilitating account transactions may fall within the jurisdiction of other regulators. Depending on the nature of its operations an aggregator could be considered to be a participant in a payment system and as such subject to the Payment Systems (Regulation) Act and the oversight of the Reserve Bank.

In addition, undertaking transactions could enmesh aggregators with authorised deposit-taking institutions (ADIs), and APRA as prudential supervisor might need

to be satisfied that any prudential risks to the ADIs, whether financial or operational, were appropriate and properly managed.

Aggregators and the Financial Transaction Reports Act

While the aggregator services available in Australia do not have transactional capabilities at this time, consideration has to be given to the implications of aggregators becoming "signatories" or operators of consumers' accounts.

In addition to the obvious implications of unauthorised transactions by an aggregator, there are regulatory implications. As a deterrent to money laundering and tax evasion, the Financial Transaction Reports Act 1988 (FTR Act), requires all "signatories" of "accounts" as defined by the FTR Act to be identified by the deposit taking institution. While not all the financial products to which aggregation will apply will be "accounts" for that purpose, some may be. If an aggregator were authorised to operate such an account, the aggregator would have to be identified as required by the FTR Act.[59]

Depending upon the activities being conducted by aggregators, there may be other regulatory issues. For example, an aggregator that is also a "cash dealer" under the FTR Act will have reporting obligations under the FTR Act.[60]

Questions for consideration

2. Are there other relevant consumer or regulatory issues that have not been identified in this section?

3. Are there any issues that should be given a higher priority than others when it comes to developing appropriate solutions?

4. What is the likely scope or effect of the identified issues on consumers, financial institutions and/or aggregators?

[59] Email communication from AUSTRAC, 3/5/01.

[60] Email communication from AUSTRAC, 3/5/01.

Section 6

Responses by regulators and industry groups

This section of the report discusses specific regulatory or industry-wide responses to the consumer issues discussed above. Given the relative immaturity of the market for aggregation services in Australia and other non-US jurisdictions, most of the developments or proposed responses have occurred in the US.

Regulatory responses

Privacy regulation

On 24 May 2000, the US Federal Trades Commission (FTC) published a Final Rule to implement Title V of the Gramm-Leach-Bliley Act. Title V deals with privacy issues and restrictions on a financial institution's ability to disclose non-public personal information about consumers to non-affiliated third parties. The Federal Banking Agencies and the other Federal Regulatory Authorities published similar rules.

Title V imposes obligations on "financial institutions". In its final rule, the FTC confirmed that the text of the relevant legislation "brings into the definition of financial institution an Internet company that compiles, or aggregates, an individual's on-line accounts (such as credit cards, mortgages and loans) at that company's website as a service to the individual, who may then access all of its account information through that Internet site."[61]

Thus, for the purposes of the privacy provisions of the Gramm-Leach-Bliley Act, account aggregators are considered to be "financial institutions".

Note that, in Australia, the National Privacy Principles (NPPs) included in the Privacy Act 1988 will come into effect on 21 December 2001. They will apply to a large portion of the Australian private sector. Advice from the Office of the Privacy Commission suggests that the NPPs and the Privacy Act are likely to apply to account aggregators. The requirements of the NPPs are summarised earlier in this paper.

---

[61] Federal Trade Commission, 16 CFR Part 313, *Privacy of consumer financial information; Final Rule*, Federal Register, Vol 65, no 101, 24 May 2000, p. 33655.

Question for consideration

5. Will the National Privacy Principles and the Privacy (Private Sector) Amendment Act adequately address the privacy issues associated with account aggregation services?

EFT regulation

On 23 June 2000, the Federal Reserve Board in the US published for comment a proposed rule to revise the Official Staff Commentary to the Board's Regulation E (Electronic Funds Transfers). Regulation E implements the Electronic Funds Transfer Act, which provides a basic framework establishing the rights, liabilities, and responsibilities of participants in the EFT system. It includes provisions on disclosure of terms and conditions, receipts, account statements, limits on consumer liability for unauthorised transactions, and error resolution procedures.

In the discussion accompanying the proposed rule, the Board noted that it has been asked whether Regulation E applies to aggregation or screen-scraping services. To assist the Board in providing guidance on this issue, the Board sought comments on:

- How the services operate or plan to operate;
- Are aggregators providing or planning to provide bill-payment or other EFT services (in addition to information services)?
- To what extent do agreements exist between aggregators and account-holding institutions, governing matters such as procedures for access to information and for electronic transfers?
- What the implications would be of a determination that aggregators are or are not financial institutions for the purposes of Regulation E generally or under s. 205.14.[62]

The Board also noted that the security code issued by the aggregator arguably meets the definition of an "access device", and thus the aggregator could be a financial institution for the purposes of Regulation E.[63]

A final rule was released on 1 March 2001, but this did not provide any guidance on the application of Regulation E to account aggregators. However, we understand that guidance is still pending.

Banking industry associations had apparently urged the Board to consider aggregators as "financial institutions" and subject them to Regulation E. The associations raised concerns that, if aggregators were not subject to Regulation E, banks would be liable if unauthorised transactions took place using the aggregation service. They also argued that consumers should be entitled to the same protection

[62] Federal Reserve System, 12CFR Part 205, Regulation E; Docket No. R1074, Electronic Funds Transfers, p. 14.

[63] Ibid. p. 14-15.

when they initiated a transaction through an aggregator site as when they initiated a transaction directly through their financial institution.[64]

Note also that, under Regulation E, consumers are not liable at all for carelessness with their PIN or password. Instead they are liable for losses caused by delays in reporting lost or stolen cards, or failing to report unauthorised transactions appearing on a periodic statement. This means that regulatory choice as to who should be liable for unauthorised transactions is between the aggregator and the financial institution.

In contrast, in Australia under the current regime, the choice will be between the aggregator, the financial institution and the consumer. The consumer can be held liable if he or she has contributed to the loss by disclosing their password. (Details of the EFT Code are provided earlier in this paper.)

Question for consideration

6. Should account aggregation services be considered to be "account institutions" for the purposes of the revised EFT Code? Would this be an effective way to establish fair liability rules where account aggregators are involved?

Guidance from the Office of the Comptroller of the Currency

On 2 March 2001, the US Office of the Comptroller of the Currency (OCC) released a bulletin that outlines the risks for national banks in offering account aggregation services, and the management controls that are needed to minimise these risks. The OCC is a bureau of the Treasury department, and its primary function is to supervise the national banking system.

The guidance is directed towards banks, and its focus is specifically on minimising the risks for financial institutions, rather than the risks for consumers. However, compliance with the guidelines is likely to create a safer environment for consumers wishing to use aggregation services.

Key points from the Bulletin include:

- "Aggregation business models and services are evolving, as are the underlying legal and operational structures. That evolution accentuates strategic, reputational, transaction, and compliance-related risks.
- Key controls involve security, compliance, vendor management, data gathering and use, contracting, and customer education, disclosures, and service.
- Banks should implement risk management controls to safeguard customer information, to select and monitor vendors, to comply with legal and regulatory requirements, and to educate and disclose information to customers."[65]

---

[64] Electronic Commerce & Law Report, Vol 5, No 35, 31/9/00, p. 911. See also the submission from Independent Community Bankers of America http://www.icba.org/news_views/c1083100.html, downloaded 22/11/00.

[65] OCC Bulletin 2001-12, *Bank-Provided Account Aggregation Services*, p.1, available from www.occ.treas.gov.

Compliance with the guidelines is voluntary.

The issues raised in the Guidelines were expanded in a speech given by an OCC officer to the American Bankers' 2nd Account Aggregation conference in April 2001. Among other things, the importance of adequate management and oversight of third party relationships was discussed.

It was noted that banks have typically opted to use third parties to perform the aggregation functions the bank offers to its customers. However, this use of a third party to provide the functions behind account aggregation may be completely invisible to the consumer.

The speech emphasised the importance of managing such third party relationships, and noted that responsible management of third party relationships typically requires four essential elements:

- understanding the risks associated with the outsourcing arrangement;
- exercising due diligence in selecting the service provider;
- ensuring that written contracts address key risk factors associated with the activity; and
- overseeing performance by the service provider.[66]

Question for consideration

7. Do financial institutions in Australia see a need for the relevant regulator(s) to develop guidelines on account aggregation that are similar in scope to those released by the OCC?

Identifying aggregators

In the case of financial institutions, the Federal Reserve Board already has a procedure to identify financial institutions and create an audit trail for electronic communications. Any financial institution that communicates electronically with the Board must first place an identifier on its computer system so that the Board can immediately and accurately trace any communication originating from that institution.

According to the Star System report, the Board has suggested that aggregators could establish a similar system on a voluntary basis.[67]

Another commentator notes that aggregators have already begun supplying financial institutions with identifying codes for their servers, so that the financial

[66] Julie L Williams, 1st Senior Deputy Comptroller and Chief Counsel, Office of the Comptroller of the Currency, *The Impact of Aggregation on the Financial Services Industry*, Speech to the American Banker's 2nd Account Aggregation conference, 23/04/01.

[67] Star Systems Inc, op.cit., p. 11.

institution knows whether the person looking at the data on their site is their customer or an aggregator.[68] A move towards setting up direct data feeds between aggregators and institutions will also overcome the problems of lack of identification.

Question for consideration

8. Is identification of aggregators currently a problem for financial institutions and/or regulators in Australia? If so, would the problem be addressed if aggregators provided identifying codes?

Financial Services Authority Statement

On 15 May 2001, the Financial Services Authority (FSA) in the United Kingdom stated its views that it will have no powers to regulate the provision of account aggregation services.[69]

The FSA clarified that regulated firms will have to undertake proper checks (particularly in relation to legal, security, and systems and control issues) for any new business activity, including account aggregation. However, the actual activity of account aggregation will fall outside the FSA's jurisdiction.

Unregulated firms will not be required to obtain FSA authorisation before they offer account aggregation.

The FSA also warned consumers that, because the FSA has no powers to regulate, it cannot guarantee consumers the protection of the regulatory system if something goes wrong.

The FSA is planning to release a discussion paper on e-commerce in June 2001, and this paper will present a more detailed analysis of account aggregation and the issues that it raises.

AUSTRAC Research

The Australian Transaction Reports and Analysis Centre (AUSTRAC), the regulator under the Financial Transaction Reports (FTR) Act is undertaking research with a view to issuing a discussion paper regarding the money laundering and tax evasion implications of aggregator services later in 2001. This will form part of a general study of the implications of new payment systems and products on Australia's anti-money laundering system and the FTR Act in particular.

---

[68] Miriam Leuchter, "Aggregation, Aggravation", *US Banker*, 10/2/00, p. 28

[69] "New online 'account aggregation' service will not be regulated, warns the FSA", FSA media release 15/05/01, available from www.fsa.gov.uk.

Industry initiatives

Various press reports indicate that financial institutions in the United States are concerned about the growth in third party aggregator sites. Some of the issues for these institutions include:

- Customer privacy and control of customer information;[70]
- Inadequate security by aggregators – which may lead to unauthorised transactions that the bank is held liable for;
- Authentication of the customer;
- Inability to identify whether the site is being accessed by the customer or an aggregator;
- Lack of common audit trails to facilitate tracking of fraudulent transactions;
- Aggregators displaying inaccurate or incomplete data (and reliance on that data by customers);
- Security of screen scraping.

Of course, some of these issues are variations on the consumer issues described earlier, but with a different focus. The interests of consumers and industry members are not necessarily the same. For example, financial institutions may want to see third party aggregators regulated primarily to ensure a level playing field. However, solutions developed by industry members may also benefit consumers.

Press reports suggest that, despite their concerns, banks are keen to take advantage of the opportunity that aggregation offers to provide tailored and personalised financial products and services to customers.

Discussed below are some of the initiatives to address these issues that have been suggested or implemented by industry members.

First Union aggregation guidelines

In order to ensure the privacy and security of customer information, one bank in the US (First Union Corporation) has issued guidelines for third-party aggregators that want to work with the bank. These guidelines require aggregators to:

- Provide full and meaningful disclosures to ensure that customers understand the risks of authorising a third party to access their financial account information;
- Protect customer's bank and aggregator authentication data using industry security standards, including encryption and authorisation;
- Use technologies approved by the financial institution when accessing data and performing transactions on behalf of the institution's customers;

[70] First Union Limited in fact instituted proceedings to ban a screen scraper from accessing its website, citing concern for the security and privacy of its customers. However, the proceedings were later withdrawn.

- Give the financial institution a method to identify and track aggregators' activities on its site and to differentiate them from customer-initiated activities;
- Establish a process to ensure the validity and accuracy of all data displayed;
- Use processes that enable the financial institution to continue adhering to banking and financial services laws and regulations and to its own corporate policies;
- Establish a process that provides end-to-end audit trails at both the system and transactional levels so that the financial institution can validate the source, authorisation and execution of all transactions, and
- Allow a third party approved by the financial institution to perform security and process assessments regularly, at the aggregator's expense.[71]

These guidelines were developed after First Union withdrew legal proceedings that it had instituted to bar a screen-scraper from accessing its website.

BITS Account Aggregation Working Group

The Banking Industry Technology Secretariat (BITS) is formed by the CEOs of the largest bank-holding institutions in the United States. Early in 2000, it established a working group to look at aggregation issues, with subgroups focusing on legal & regulatory issues; security criteria; privacy practices; technology & standards; and customer education.[72]

The BITS working group has organised two industry forums on aggregation services,[73] and on 25 April 2001, released its *Voluntary Guidelines for Aggregation Services*, as Phase I of its aggregation initiative.[74]

The guidelines:

- include suggestions for security requirements for aggregators in their collection and storage of customer information;
- spell out base-level privacy guidelines that are consistent with the legislative requirements in the US;
- provide information on good business practices and the key information that should be shared between aggregation service providers and institutional account holders;
- provide guidance to financial institutions and financial aggregators on the appropriate disclosures to be provided to consumers; and
- provide information on the laws and regulations applicable to financial aggregation.

---

[71] Star Systems Inc, op.cit., p. 11; Kiesnowski, K and Marlin, S, "Web aggregators: pros and cons for banks", *Bank systems and technology*, vol 37, no 4, p. 28-32, April 2000.

[72] BITS Bulletin July 2000, p. 3, available from www.bitsinfo.org.

[73] BITS Bulletin September 2000, p. 5, available from www.bitsinfo.org.

[74] Available from www.bitsinfo.org. See also "BITS spearheads a major breakthrough for consumer protection", BITS media release, 25/04/01., available from www.bitsinfo.org.

The Boards of Directors of BITS and the Financial Services Roundtable, as well as the Roundtable's Consumer Issues Committee have endorsed the Voluntary Guidelines.

Phase II of the BITS initiative will explore additional issues, such as the possibility of cooperation in the areas of data feeds and authentication. Results of Phase II will be reported by the fourth quarter of 2001.[75]

Questions for consideration

9. Do the BITS Voluntary Guidelines have relevance in the Australian context?

10. Is there a need for the development of similar industry guidelines in Australia? If so, who should develop these guidelines?

Formal agreements between financial institutions and aggregators

One commentator in the US has suggested that financial institutions should have aggregators sign an agreement with the bank stating that the aggregator has adequately addressed privacy and security concerns. The agreement could include commitments on:

- protecting customers' log-in, password, and other authentication information;
- limiting an aggregator's activity at a bank website to inquiries on behalf of its customers (eg the aggregator may not initiate any transactions on the customer's behalf);
- consolidating information in a way that protects its confidential nature;
- adhering to privacy laws as well as the bank's own privacy policy and procedures;
- keeping the customer's information confidential and not disseminating the material to any affiliate or third party; and
- informing customers of its screen-scraping practices and implications prior to customer authorisation.[76]

However, such an approach might be difficult for aggregators that offer access to information from a large number of financial institutions.

---

[75] *BITS Voluntary Guidelines for Aggregation Services*, April 2001, p. A-3, available from www.bitsinfo.org.

[76] Keenan, T "Screen-scraping may pose liability threat", *ABA Bank compliance*, 1/7/00, p. 47-51.

Questions for consideration

11. Is there a case for financial institutions and aggregators establishing formal agreements in respect of account aggregation, addressing the issues discussed above?

12. Would such an approach overcome the security, data reliability and privacy issues for consumers?

13. Would direct data feed arrangements be another means of addressing security and data reliability issues?

Use of two passwords

An industry group in the US, the Financial Services Technology Consortium, has suggested that difficulties of identifying aggregators could be overcome by banks issuing two different passwords – one for use by the consumer, and one for use by the aggregator.[77] Such a system would make it easier for financial institutions to identify whether information was viewed by the consumer or by an aggregator.

A different model could be used to reduce the risk of unauthorised transactions. In this model, two passwords could be generated, but only one of the passwords would allow the user to make transactions. The second password could be limited so that it would allow only viewing of account information. This 'view only' password could be the one that is disclosed to the aggregator, and the consumer would have no need to disclose to the aggregator the password that is used for making transactions.

Questions for consideration

14. Would a model that allows for the generation of a consumer password and an aggregator password reduce identification risks for financial institutions?

15. Would a model that allows for the generation of a 'transaction password' and a 'view only password' adequately overcome any consumer risks in using aggregation services? Is such a model technically and practically achievable?

"Due diligence" on aggregators

One commentator has suggested that, where a consumer wanted to use a particular aggregation service, he or she could advise their bank to provide all the necessary account information. The bank could then make a determination – using commonly understood privacy and security standards – as to the advisability of providing data to the aggregator. The bank could then deny access to aggregators that do not meet the agreed standards.[78]

---

[77] Star Systems Inc, op.cit. p. 11-12.

[78] Star Systems Inc, op.cit. p. 12.

Authentication by financial institution

In mid-2000, the Royal Bank of Canada announced that it would be providing an aggregation service to its customers. Although this service does not appear to be available yet, the Bank had stated that, to address some of the security and privacy issues, it will require customers to log in and get authenticated at Royal's online banking site,[79] instead of through the proposed aggregation service. However, without more details, it is difficult to assess whether this approach will provide a higher level of protection for consumers. And this approach is unlikely to be an option for aggregation services that are not provided by a financial institution.

"Trusted aggregators"

In the US, a software company has developed a service that allows financial institutions to establish a "trusted aggregator" process to protect customer's data as it moves about the Internet. The product, Vyoufirst Aggregation Control Services, enables an institution to control third-party aggregation when the financial institution permits the practice, and to prevent unauthorised screen-scraping.[80] The company has apparently indicated that it is close to a deal for licensing the software with two of the nation's 20 biggest banks.[81]

Questions for consideration

16. Are there any other regulatory or industry responses that have been considered in other jurisdictions?

17. Are any of the regulatory or industry responses identified in this section appropriate for the Australian context?

[79] Toonkel, Jessica "Online banking: Royal of Canada nears account aggregation debut", *American* Banker, v. 165, no. 133, p. 14, 13/7/00.

[80] "Vyou delivers World's first solution for controlling account aggregation", Vyou media release, 12/02/01, available from www.vyou.com.

[81] Edmonston, P, "Financial firms belatedly bow to bundling of accounts online", *Wall Street Journal*, 14/02/01.

Section 7

Possible responses for the Australian context

The survey demonstrates that account aggregation services are not yet widely offered in Australia, although from our discussions with industry, it is clear that more services will be launched in the near future.

Those providing aggregation services have advised that consumers have not yet taken up the available services in significant numbers. However, these businesses and others predict that, after a slow start, use of aggregation services will increase rapidly in the coming months and years. This would be consistent with the predictions of increase in the use of aggregation services in the United States.

Given the significant consumer issues involved in aggregation services, we think it is important to begin early discussions about the way in which these issues can best be addressed. In order to encourage discussion and debate, this section looks at some possible responses for consideration by ASIC and other interested parties.

ASIC jurisdiction

ASIC's interest in this area arises from its involvement in the EFT Code and its general consumer protection responsibilities in the financial services sector. Although we may not have jurisdictional responsibility for aggregation services provided by organisations that are not financial institutions, the key driver for account aggregation services is the ability to aggregate information from financial institutions. In these circumstances, ASIC has a key role to play in facilitating discussion and encouraging the development of appropriate solutions. In addition, many of the issues may not necessarily involve legislative solutions or formal regulatory action.

We will also be seeking to involve other relevant regulators. We have already held discussions with the Office of the Federal Privacy Commissioner, the Reserve Bank of Australia, the Australian Transaction Reports and Analysis Centre, the Australian Competition and Consumer Commission and the Australian Prudential Regulatory Authority about the consumer and regulatory issues involved in account aggregation, and will also be talking with Treasury about these issues.

Disclosure

The survey of aggregators demonstrated that most sites do disclose basic information on terms and conditions, privacy and security statements, and other

issues. However, there is room for improvement in the scope, quality and accessibility of the disclosure.

For example, the significant issue of PIN disclosure and the consequent risks is one that needs to be very clearly drawn to the consumer's attention by both aggregators and financial institutions. Similarly, the relationship between the aggregator and the financial institution needs to be very obvious to consumers.

Better disclosure by both third party aggregators and financial institutions will promote consumer understanding of aggregation services and the ability to make informed choices.

There are a number of non-exclusive ways in which ASIC could encourage better disclosure in this area:

1. ASIC could promulgate messages and encouragement to industry members about the need for better disclosure, and the issues that would need to be addressed in order to facilitate consumer understanding and choice. We have already developed a draft good disclosure template that aggregation providers can use to review and improve disclosure on their websites (see Appendix C).

Question for consideration

18. Is the draft good disclosure template (at Appendix C) useful and comprehensive? What changes (if any) are needed?

2. ASIC could develop a formal guide to good disclosure practices, perhaps with relevant examples. Such a guide could be developed with the assistance of industry and consumer representatives. This is the approach that has been taken in the context of the disclosure of transaction fees for deposit-taking institutions. This could be developed in consultation with other relevant regulators.
3. ASIC could explore opportunities for improving disclosure on specific issues through existing self-regulatory forums. For example, the Code of Banking Practice is currently being reviewed, and it might be appropriate to suggest that Code could include an obligation on members to clearly disclose their attitude and response to consumers who disclose their PIN or password to web aggregators generally, or to one or more specific aggregators. Alternatively, a separate section covering aggregator issues, including disclosure, could be introduced into the EFT Code.
4. ASIC could work with aggregation providers to develop a code specifically covering the aggregation sector.
5. If self-regulatory or other initiatives are considered inappropriate, or are not successful, there may be a case for imposing appropriate disclosure requirements through legislation.

Security

The security issues surrounding account aggregation are primarily technical ones, and ASIC is not necessarily in a position to assess whether the security measures taken by aggregators are appropriate. However, other regulators, such as APRA and the RBA, may have more direct input into any solutions.

Question for consideration

19. Should there be industry-wide security standards for account aggregation? If so, should this be a role for a government agency or an industry body?

The most practical solutions for addressing security issues may be developed by industry members working together to develop appropriate minimum security standards for aggregation services. However, consultation with the relevant regulators will also be important.

The development of appropriate standards could be complemented by an accreditation system that could independently identify those aggregation services that meet the relevant standards. Consumers could use this information when choosing an aggregation service. Financial institutions could also use this information to advise their customers about the aggregation services to use or not use. In this instance, however, competition issues will also need to be considered.

Privacy

Many of the privacy issues raised in this paper may be addressed when the extension of the Privacy Act to the private sector comes into force later this year. This legislation also provides for private sector codes. There may therefore be scope for aggregators to develop a code setting out specific privacy standards.

In the meantime, aggregators should consider implementing the National Privacy Principles into their practices. In particular, consumers should have to make a positive election before their information can be used for marketing purposes.

Liability for losses caused by unauthorised EFT transactions and other matters

One question that needs to be addressed fairly urgently is how should liability for losses be allocated between the financial institution, the aggregator, and the consumer. As explained earlier, losses could arise from unauthorised EFT transactions, reliance of inaccurate or out of date information, poor service quality, misrepresentations, software viruses or bugs, and other incidences. And consumer confidence in aggregation services will plummet if they begin to incur losses.

Statutory conditions and warranties may provide some protection for consumers, and aggregation services should be encouraged to ensure that their general disclaimers are consistent with these statutory rights.

In addition, as noted earlier, the revised EFT Code (released in April 2001) will provide liability allocation rules in limited circumstances. However, there may be many other circumstances of unauthorised transactions where these rules do not apply. In addition, the revised EFT Code does not deal with other possible liability issues between consumers and aggregators.

The EFT Working Group recognised that clause 5.7(b) will not deal with the liability issues associated with aggregation services in any detail. Concerns about aggregation services arose only towards the end of the review process, and it was not considered appropriate to provide a rushed response. The Working Group has suggested that it the EFT Code might be amended at a later date to deal with account aggregation issues. Alternatively these issues could be addressed in another forum.[82]

The EFT Code is an obvious vehicle for established fair rules on liability issues, at least where the financial institution concerned and/or the aggregator is a party to the Code. This Code has recently been revised, and the next complete review is due in 3 years time. However, it may be possible to develop a stand-alone aggregation module outside the normal three-year review process.

As mentioned earlier, another possible vehicle for addressing some of these issues might be a separate aggregator code.

Finally, it may also be possible to use internal guidelines for dispute resolution schemes. For example, the Australian Banking Industry Ombudsman has developed guidelines on how the scheme will investigate and resolve particular types of issues. However, there is no guarantee that consistent guidelines or approaches will be taken across each of the dispute resolution schemes in the financial services sector. In addition, this can only be an interim measure, as the development of such guidelines is not a public process.

It may also be appropriate for ASIC to begin discussions towards developing voluntary guidelines that spell out some good practice standards for liability allocation in the event of complaints about unauthorised transactions. Such guidelines could stand alone, or could form the basis for any rules to be inserted into a code or other more formal mechanism.

In addition, if direct feeds become more common in the future, the agreements between financial institutions and aggregators could include provisions that prevent aggregators from disclaiming liability for all possible losses. Again, this is a solution that could be encouraged through an aggregator code, an aggregation module in the EFT Code, or good practice guidelines.

For unauthorised transactions, some possibilities for additional liability allocation rules might include:

- 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 warns consumers that such disclosure is not permitted, either in general, or to one or

[82] Note 19 to revised EFT Code April 2001.

more particular aggregators. Such a warning would only be effective if it was obvious and brought to consumers' attention.

- A provision that restricts aggregators to accessing data only from sites which have authorised their consumers to hand over access codes to the aggregation service. However, such an approach might have a negative impact on competition in the market.

Questions for consideration

20. Would the above suggestions for liability allocation rules address the main liability issues? Are there other, more suitable ways of allocating liability for unauthorised transactions?

21. In what circumstances should consumers, aggregators, and financial institutions bear liability for unauthorised transactions?

While discussion on these and other issues of liability allocation is needed, there are some initial steps that financial institutions can take to clarify their approach.

At a minimum, financial institutions should develop policies on:

- whether they will treat disclosure of a PIN/password to an aggregation service as a breach of PIN security requirements (subject to clause 5.7(b) of the revised EFT Code);
- how they will advise consumers of this information; and
- how they will respond to consumer complaints about unauthorised transactions in circumstances where the consumer has used an account aggregation service.

Financial institution staff should be able to advise their customers on the consequences of these policies and the consequences of using an aggregation service, and this advice should be consistent across all channels.

Question for consideration

22. Are there any practical or other reasons that would restrict the ability of financial institutions to provide this type of information to their customers?

Complaints and dispute resolution

Under the proposed Financial Services Reform legislation, financial institutions that provide aggregation services will be required to have approved internal and external procedures to deal with complaints from their retail customers. However, it is not clear whether the FSRB will apply to third party account aggregators.

This may be an area where aggregators can be encouraged – by ASIC and consumer groups – to join an existing independent dispute resolution scheme, or where an appropriate scheme does not exist, to establish one. Aggregators should also be encouraged to establish internal procedures for resolving complaints. Aggregators could use their commitment to fair dispute resolution as a marketing tool.

There are also a number of specific issues that will need to considered in this context:

- There will need to be some way for information about unauthorised transactions and other losses to be collated. If, for example, the security of password vault is compromised, there could be a large number of unauthorised transactions made on accounts with different institutions, and owned by more than one consumer. Without some way of collating information about losses, it might be difficult to identify that the only link between the transactions is the aggregation service.
- A related issue is that appropriate information sharing procedures between an aggregation service and a financial institution will be needed to facilitate investigation and resolution of complaints. However, such procedures will need to be carefully considered in the light of privacy policies and procedures.
- Finally, it will be important that consumers are not shunted between the aggregation service and their financial institution when a complaint arises, with neither organisation taking responsibility for investigating the matter. Given that financial institutions will be required to have dispute resolution procedures, it may be worth considering imposing (perhaps through the EFT Code) an obligation on financial institutions to be the 'investigator of last resort', unless the complaint does not involve the consumer's account, but relates to the aggregation service more generally.

Question for consideration

23. Assuming necessary amendments could be made to the terms of reference of existing dispute resolution schemes, would these existing schemes be appropriate for dealing with complaints arising from the use of account aggregation services?

Consumer education

ASIC can play a key role in ensuring that consumers have a better understanding of account aggregation services (eg through consumer alerts and other activities). However, aggregators and financial institutions should also play a key role in informing and educating consumers.

One impediment to effective consumer education in this area is the current low take up of aggregation services. Consumers are unlikely to be interested in education about services that they are not yet using.

Overcoming this impediment might involve targeting education material to consumers who are using, or have demonstrated an interest in using, an aggregation service. For example, aggregators could be encouraged to provide a link from the login page to a section on ASIC's consumer website, Fido, that could offer information on the questions to consider when choosing whether to use an aggregation service.

Similarly, banks and brokers could provide links to Fido, as we expect that the people most likely to use an aggregation service are already significant users of Internet banking and brokerage services.

Prudential and other regulation issues

The question of whether or not account aggregators should be required to meet prudential standards or have other regulatory requirements imposed on them is one that will need further discussion and consideration by all relevant parties, including any other regulators having relevant jurisdiction.

APRA has also been meeting with industry participants to discuss and assess the prudential issues arising from account aggregation. The major focus of these discussions has been on the risk management processes in place to deal with the unique risks arising from account aggregation. These risks include security, data reliability, legal and outsourcing risks. APRA is also assessing the potential reputational implications in the event of a security breach where an outside party gains access to PINs/passwords. If this were to occur, it would allow access not only to the accounts held at the specific institution offering the account aggregation services, but also to accounts held at other institutions.

At this stage, APRA's preference is for direct data feed arrangements to address the security and reliability concerns.

As to the cross-border issues jurisdictional issues, APRA will, in its role as the home supervisor, continue to closely monitor local financial institutions offering account aggregation services and share information with other overseas regulators where relevant.

Industry participants should also be aware that the conduct of aggregators could in some circumstances raised consumer protection issues under the Trade Practices Act. Also, the development of industry guidelines and standards regarding aggregation services, if they were to exclude or otherwise place some aggregators at a competitive disadvantage could also raise some competition issues under the Trade Practices Act. In some cases, such industry arrangements could require authorisation by the ACCC in order to proceed.

Questions for consideration

24. Are any or all of the solutions identified appropriate? If so, which should have priority, and who should be responsible for progressing or implementing the solution(s).

25. Should rules or guidelines for aggregation services be contained in an aggregators' module in the EFT Code, in a separate aggregators' code, in ASIC good practice guidelines, or in another format?

26. Are there other possible solutions, not identified here, that might be more effective or practical?

27. What roles should regulators, aggregators, financial institutions, and consumer groups play in identifying, developing and implementing solutions?

28. Is there any danger of rules or guidelines being used for anti-competitive purposes? What safeguards could be introduced to reduce the risk of anti-competitive conduct?

Section 8

Where to from here?

Facilitating discussions

ASIC has released this paper to encourage discussion on aggregation services and on the best way to ensure that these services can meet the needs of consumers for information and for appropriate standards on privacy, security, liability, and other matters.

ASIC will be using this paper as a basis for further discussions with industry and consumer representatives, as well as relevant government representatives. We will be seeking to develop some consensus on the best ways to move the issues forward.

We believe that the issues raised in the paper need to be addressed, although some are more urgent than others. Appropriate rules or practices need to be developed, published and implemented by aggregators and financial institutions. However, we are open to the views of others as to whether this should be through an aggregators' module in the EFT Code, a separate aggregators' code, or an ASIC guide on good practices. In addition, it is worth considering whether there is a need for regulation or legislation.

We plan to hold a roundtable meeting with interested stakeholders later in the year. Among other things, such a meeting would provide an opportunity to:

- confirm the scope and nature of the consumer issues;
- identify any priority issues;
- seek consensus on the most appropriate solution(s), including what format any agreed rules or practices should take; and
- seek consensus on the most appropriate way to progress the development of solutions.

A roundtable meeting could also be an opportunity to facilitate communication between aggregators and financial institutions. In turn, this could increase the likelihood of industry solutions developing to address technical issues such as audit trails and identification of aggregators.

Consumer representatives and government agencies should also have input into the development of practices or principles to govern the relationship between financial institutions and aggregators.

The planned roundtable meeting would be one part of the larger process of ongoing consultation and discussions. Bilateral meetings with industry members, consumer groups and other interested parties will also be an important part of the process.

More information

We welcome comments or suggestions on the issues and proposals raised in this paper, and on any or all of the specific questions offered to guide your response. Your comments should be directed to:

Nicola Howell
Senior Policy Officer, Office of Consumer Protection
Australian Securities & Investments Commission
Tel: (02) 9911 2410
Fax: (02) 9911 2642
Email: nicola.howell@asic.gov.au
Address: GPO Box 4866, SYDNEY NSW 1042

Please indicate whether you wish the whole or any part of your comments to be treated as confidential. All comments will be treated as public information unless you have requested that we do otherwise.

Your comments should be provided by 13 July 2001.

Section 9

Appendices

Appendix A — Internet sites surveyed for this report

Organization/Site Type	Australian	US
Diversified Financial Institution	11	3
Bank	5	7
Building Society	3	-
Credit Union	19	-
Stockbroker	13	-
Financial Adviser	1	-
Responsible Entity	2	-
Insurer	1	-
Financial Portal	3	2
Other Portal	2	-
Aggregation Supplier	1	1
Retail Site	2	-
Total	**63**	**13**

Appendix B – Websites of surveyed institutions

Web site operator	URL	Aggregation facility type offered	Aggregation technology supplier
AUSTRALIAN SITES			
Adelaide Bank Limited	http://www.adelaidebank.com.au/	None	
Advantage Credit Union Ltd	http://www.advantage.net.au/	None	
AMP Limited	http://www.amp.com.au/	Combination	VerticalOne Australia Pty Ltd
APESMA Professionals First Credit Union Ltd	http://www.apesma.asn.au/services/credit.htm	None	
Austock Brokers Pty Ltd	www.webstock.com.au	None	
Australia and New Zealand Banking Group Limited	www.anz.com.au	None	
Australian Central Credit Union Limited	www.accu.com.au	None	
Australian Unity Building Society Limited	http://www.austunity.com.au/home/home_frameset.htm	None	
Bananacoast Community Credit Union Ltd	http://www.bananacoast.com.au/	None	
Bank of Queensland Limited	www.boq.com.au	None	
Bankers Trust Australia Limited	www.btal.com.au	None	
BankSA	www.banksa.com.au	None	
Bankstown City Credit Union Ltd	www.bccu.com.au	None	
BankWest	www.bankwest.com.au	None	
Bendigo Bank Limited	www.bendigobank.com.au	None	
Big River Credit Union Ltd	http://www.brcu.com.au	None	
Blue Mountains & Riverlands Comm CU	http://www.bluemts.com.au/bmcu/	None	
Bridges Personal Investment Services	www.bridgesweb.com.au	None	
Citibank Limited	www.citibank.com.au	None	
City Coast Credit Union Ltd	http://www.cccu.org.au/	None	
Colonial Limited	www.colonial.com.au	None	
Commonwealth Bank of Australia	www.commbank.com.au	None	
Companion Credit Union Limited	http://www.companion.com.au/	None	
Comtax Credit Union Limited	http://www.comtax.com.au/	None	
Connect Credit Union of Tasmania Limited	http://www.connectcreditunion.com.au/	None	
CPS Credit Union (SA) Ltd	http://www.cpscu.com.au/	None	
CPS Credit Union Co-operative (ACT) Limited	http://www.cpsact.com.au/	None	
Credit Union Australia Ltd	http://www.cua.com.au/NewCuaWeb.nsf	None	
DaytraderHQ	www.datraderhq.com.au	None	
Defence Force Credit Union Limited	http://www.adfa.oz.au/defcred.htm	None	
Dicksons Limited	www.dicksons.com.au	None	
Discovery Credit Union Ltd	http://www.discoverycredit.com.au/	None	
E*Trade Australia Securities Limited	www.etrade.com.au	None	
Education Credit Union Co-operative Limited	http://www.edcredit.com.au/	None	
Egoli Pty Ltd	http://www.egoli.com.au	Combination	eWise.com.au
ELCOM Credit Union Ltd	http://www.elcomcu.com.au/	None	
Electricity Credit Union Ltd	http://www.ecu.com.au/	None	
eWise.com.au	www.ewise.com.au	Combination	eWise.com.au
Financial Enrichment Pty Ltd	www.enrichment.com.au	Combination	Teknowledge Corporation
First Australian Building Society Limited	http://www.firstaustralian.com.au/	None	
Free Online Australia Pty Ltd	www.freeonline.com.au	Combination	Teknowldege Corporation
HSBC InvestDirect (Australia) Limited	www.hsbcinvestdirect.com.au	None	
ING Direct	www.ingdirect.com.au	None	
John Fairfax Holdings	http://www.moneymanager.com.au/	None	
Macquarie Bank Limited	www.macquarie.com.au	None	

Web site operator	URL	Aggregation facility type offered	Aggregation technology supplier
Maitland Mutual Building Society Limited	http://www.mmbs.com.au/	None	
My Money Group Pty Limited	http://www.mymoney.com.au	None	
N M Rothschild & Sons (Australia) Limited	www.rothschild.com.au	None	
National Australia Bank Limited	www.national.com.au	None	
Ninemsn	www.ninemsn.com.au	To be offered	Parkers Edge
NRMA Insurance Group	www.nrma.com.au	None	
Reckon Investment Centre Ltd	http://www.quicken.com.au/investments/quickBroker/default.htm	None	
Sanford Securities Limited	http://www.sanford.com.au/sanford/	None	
ShareTrade Australian Stockbroking Limited	http://www.sharetrade.com.au/	None	
SheSaid Pty Ltd	http://www.shesaid.com.au/	Combination	Teknowledge
St. George Bank Limited	www.stgeorge.com.au	None	
Suncorp-Metway Limited	www.suncorpmetway.com.au	None	
TD Waterhouse Investor Services Limited	www.tdwaterhouse.com.au	None	
Todd Partners	http://www.todd.com.au/index.htm	None	
WealthPoint Limited	http://www.quicktrade.com.au/	None	
Westpac Banking Corporation	www.westpac.com.au	None	
William Noall Limited	www.wnoall.com.au	None	
Your Prosperity Ltd	www.yourprosperity.com.au/	None	
US/CANADA SITES			
Bank of America	http://www.bankofamerica.com/	None	
CashEdge Incorporated	www.cashedge.com	Financial accounts only	CashEdge Incorporated
Chase Manhatten Corporation		Combination	Yodlee
Citigroup Inc	www.myciti.com	Combination	Yodlee
directbanking.com	www.directbanking.com	Combination	Yodlee
EAB (ABN AMRO Group)	http://www.eab.com/	Combination	Yodlee.com Inc
HD Vest Technology Services Inc	www.myhdvest.com	Combination	Yodlee
MoneyPark, Inc	http://www.moneypark.com/	Combination	VerticalOne
NetBank	www.netbank.com	Combination	OnMoney.com Financial Services Group
Royal Bank of Canada	www.royalbank.com	To be offered	CashEdge Incorporated
U.S. Bancorp	http://www.usbank.com/cgi/cfm/ubank_online/index.cfm	None	
VirtualBank	http://www.virtualbank.com/	Combination	VerticalOne
Wells Fargo	http://wellsfargo.com/	Financial accounts only	VerticalOne

Appendix C – Draft good disclosure template for account aggregation services

Issue	Good practice
Disclosure of the identity of the aggregator	The site should have full and prominent disclosure of the legal entity operating the site and, if different, the legal entity providing the aggregation service. This should include: - principal physical address; - email address; - mail address; - telephone number; - relevant government license/registration number, including ACN/ABN.
Relationship between aggregator and financial institution(s)	The site should clearly disclose the relationship (if any) between itself and any financial institution that the aggregator provides information from. If known, the site should disclose whether the financial institution has given permission for its customers to use the aggregation service.
Privacy policy	The site should have a privacy policy that complies with the Privacy (Private Sector) Amendment Act. The site should have full and prominent disclosure of the privacy policy. The policy should include information on: - who has access to personal information provided by consumers; - how that information will be used; - whether that information will or may be sold or otherwise disclosed to a third party; - what steps can be taken to opt in or opt out of any cross-selling or marketing activities; - how consumers can get access to information held about themselves; and - how the site deals with cookies, web bugs, and clickstream data. This policy should not allow unsolicited marketing unless the consumer has taken the opportunity to 'opt in' to having his or her information used for this purpose.[83]
Complaints handling procedures	The site should disclose internal complaints handling procedures. These should allow for the resolution of complaints by an independent party where the consumer is not satisfied with the results of the internal complaint process.
Advertising	Advertising on the site must be clearly identifiable as such.
Risks of disclosing financial institution PIN or password	The site should clearly advise the risks (if any) of a consumer disclosing his or her financial institution PIN or password to the aggregator, including whether the consumer may lose any rights under the EFT Code and any steps that consumers can take to reduce the risk.

[83] An 'opt in' approach is recommended as best practice by the Office of the Federal Privacy Commissioner, letter dated 10 April 2001.

Consumer obligations	The site should clearly disclose any obligations imposed on users of the service, including any obligation to safeguard the security of their password for the aggregation service. The site should also disclose the consequences of not meeting those obligations.
Liability and disclaimers	The site should clearly disclose the circumstances in which: - the aggregator; and/or - the consumer will be held liable for losses occurring through use of the aggregation service. Any disclaimer that limits the aggregator's liability should be clearly and prominently disclosed. The site should not try to contract out of its responsibility for losses arising from its own misconduct or negligence, or from misuse or failure of authentication mechanisms. The site should also not try to contract out of any responsibility for losses caused by employee fraud.
Applicable regulation	The site should clearly disclose the primary consumer protection regulatory or self-regulatory rules that govern the provision of the service.
Service information	The site should provide accurate and easily accessible information describing the service offered. This information should be provided in a conspicuous, accurate and accessible manner. Clear disclosure should be made on the site of the services that are free and the services that are charged for. The price of services that are charged for should be disclosed, as should the available methods of payment. The site should warn consumers to check if their financial institution will charge a fee for balance and other inquiries that might be carried out by the aggregator. It should also provide clear disclosure about the regularity with which balance and other enquiries will be made by the aggregator. The site should disclose all relevant details associated with the service including the applicable terms and conditions.
Information collection	The site should disclose how information is collected from the financial institution (eg whether the aggregator is using screen-scraping or direct feed arrangements). The site should also give some information about the relative risks of the method of collecting account information.
Transaction information (if transaction functionality offered)	The site should disclose in a clear and prominent manner: - the manner in which transactions will be made; - the terns and conditions relating to corrections and cancellations; - information on the time within which transactions will be executed.
Currency of information	The site should clearly display the date and time at which the account information displayed was collected from the financial institution concerned.
Security	The site should explain in clear and simple terms what security features are employed to protect information provided by the consumer, both in transmission and storage.
No omissions or misrepresentations	The site must not make any misrepresentation, false statements, or omissions, and must not engage in any practice that is likely to be misleading, deceptive, fraudulent or unfair.