MinterEllison
LAWYERS

E-COMMERCE - IMPLICATIONS FOR FINANCIERS

UPDATE ON REGULATORY ISSUES

Presented by

Gillian Brown
Partner

Minter Ellison
Lawyers

BACKGROUND

There has been a considerable amount of regulatory activity over the past few months which will have implications for the provision of financial services electronically ('e-banking"). One of the difficult things, even for lawyers, is to keep up to date with developments in this area. The purpose of this paper therefore is to provide an update on the regulatory issues which may affect e-banking.

The size of the national consumer credit market (over $100 billion in the 1998/99 financial year) means that one of the key factors which will influence the development of e-banking is the extent to which the Uniform Consumer Credit Code ('UCCC') will recognise electronic communications. This might be achieved by amendments to the UCCC, or applying the Electronic Transactions Bill 2000 to all or part of the UCCC or (most likely) by a combination of these approaches.

This paper therefore looks first at the current position in relation to the introduction of national electronic transactions legislation and the Regulator's views on recognising electronic transactions under the UCCC and then gives a brief overview, and considers the implications for e-banking, of:

- the *Privacy Amendment (Private Sector) Bill 2000* (Cth);
- CLERP 6 - the *Draft Financial Services Reform Bill;*
- the *Second Draft EFT Code of Conduct;*
- the *Banking Code of Practice;* and
- the *Treasury Best Practice Model.*

REGULATORY FRAMEWORK

1. *ELECTRONIC TRANSACTIONS ACTS AND POST IMPLEMENTATION REVIEW (UCCC)*

The *Electronic Transactions Act 1999* (Cth) commenced on 15 March 2000. The purpose of the Act is to introduce 'functional equivalence' for transactions to which Commonwealth laws apply. Put simply, this means that the requirements of Commonwealth laws can be met by electronic communications.

The Act applies before 1 July 2001 only to Commonwealth laws specified in the Regulations. The Commonwealth legislation specified in the Regulations, includes the *Banking Act 1959*, the *Financial Corporations Act 1974*, the *Privacy Act 1988* (Section 63), the *Superannuation Acts of 1922, 1976 and 1990* and a substantial number of superannuation regulations.

The intention is that the States and Territories will enact uniform legislation this year. On 3 April, Federal Attorney-General, Daryl Williams announced that the standing committee of Attorneys-General had endorsed a uniform Electronic Transactions Bill 2000 ('ETB') which is based on the Commonwealth Act. As at 12 May, New South Wales and Victoria have both passed an Electronic Transactions Act. The commencement date of the New South Wales legislation is to be fixed by proclamation. The Victorian legislation commences on 1 September 2000. Both Acts apply to 'any law in force in this jurisdiction whether written or unwritten, but does not include a law of the Commonwealth'.

The Regulations made under the ETB may exempt specified legislation or specified requirements or permissions from all or part of the Act. In this respect the State legislation with its 'opting-out' approach differs from the Commonwealth Act with its 'opting-in' approach.

The future development of e-banking in the consumer credit area will, to a large extent, depend on how the Regulators decide the ETB should apply to the UCCC. In that context, it is useful to consider the recommendations made in the final report on the Post-Implementation Review of the UCCC, which was released in August 1999. The recommendations include (relevantly):

1. Recognise electronic transactions, by harmonising the UCCC as far as possible with the *Electronic Transactions Act 1999*. In addition, the UCCC will need to adopt specific consumer protection measures to respond to the issues that arise specifically out of the consumer credit environment.

2. Amend the UCCC's definitions of 'writing' and 'sign' to make it clear that the UCCC recognises both electronic records and the electronic authentication of records.

3. Give further consideration to those types of contracts, such as real property mortgages, which need to be exempted from being able to be entered into electronically.

4. Permit electronic communications where the consumer has an electronic address, the means to notify a change of address, elects to receive communications electronically and has a right to cancel this election.

5. Prohibit documentation under the UCCC that triggers an enforcement process being able to be provided electronically.

6. Implement the following seven points in relation to storage and reproduction of information:

   (a) ensure that the pre-disclosure statement and the contract is capable of being stored both before and after the transaction is completed;

   (b) ensure that all electronic communications delivered electronically are capable of being retained and are accompanied with instructions on how to do so;

   (c) ensure that the capacity to store or retain electronic communications includes both the capacity to copy them on a personal electronic file and make a paper print-out of it;

   (d) ensure that any electronic communications so retained be able to be done in a manner that satisfies conditions of reliability and identification of place, time and date of origin and receipt of the information;

   (e) ensure that electronic communications permit the display of text messages in a clear and readily understandable format;

   (f) require that credit providers take reasonable steps to ensure that the pre-contractual information and the contract are complete and unaltered at the point at which the consumer receives them. Of course, this needs to be done in a way that does not prevent the electronic information from being stored by the consumer;

   (g) give further consideration to the kinds of documentation or other information that would not be considered to be appropriate to post on a web site for the purposes of providing that information to the consumer.

7. Require that pre-contractual and contractual information is able to be scrolled through before any contract can be entered into. This documentation should be required to be sent in a form that enables consumers to download it or print it out if they choose.

8. Amend Section 162 of the UCCC or make a regulation under Section 13 to ensure that important electronic communications are clearly and conspicuously expressed without distractions.

9. Ensure that the UCCC's minimum requirement for font size for paper based documentation is also required for electronic communications.

10. Ensure that consumers are given the opportunity to challenge unfair presumptions concerning the sending and receipt of messages.

11. Ensure that consumers are given the opportunity to challenge unfair contractual terms concerning the attribution of a message to them.

12. Require credit providers to disclose a physical address in the context of electronic communications only.

13. In relation to confirmation of consent to purchase credit, support a two stage process by:

    (a) requiring the introduction of a multi-clicking process at the stage which the consumer is considering the loan product and expressing their interest in proceeding to the formal contracting process; and

    (b) requiring the introduction of a mechanism that does not involve clicking at the stage at which they express their agreement to enter into legal relations. This mechanism would involve some kind of electronic signature, which is reliable in authenticating the identity of the consumer and to the intent of that person to be associated with the message. The consumer ought to have the option at this stage to enter into the contract by other means.

14. Address the issue of currency of disclosure in the electronic commerce context only.

15. In adhering to the objective of functional equivalence, the issue of a right of reflection ought not to be addressed in the context of electronic communication only.

The Ministerial Council on consumer affairs is still to advise which of the recommendations made in the final report, is to be adopted. This may not occur until after the current National Competition Policy review of the UCCC is completed. This process may be advanced by the need for State and Territory Governments to decide how much (if any) of the UCCC will be 'opted-out' of the ETB. For instance, recommendation 2 (above), can be achieved without amending the UCCC, if Sections 8 and 9 of the ETB apply to the UCCC.

Over the next few months, we should get a clearer picture of:

- whether all or any part of the UCCC will be excluded from the operation of the ETB; and

- how the UCCC will be amended to facilitate electronic transactions, whilst satisfying the consumer protection policy objectives of the UCCC.

I hope that in undertaking this task the Regulators will take a 'whole of transaction' approach and, at the same time, consider impediments to e-banking in other legislation (such as the requirement for documents to be witnessed under the *Land Titles Act* and *Bills of Sale and Other Instruments Act* in Queensland).

2. *PRIVACY AMENDMENT (PRIVATE SECTOR) BILL 2000 (Cth)*

This Bill was introduced into the House of Representatives on 12 April 2000. If passed, it will not come into operation until the later of 1 July 2001 or 12 months after the legislation is enacted.

This Bill grafts on to the *Privacy Act 1988* (Cth) (which applied only to Commonwealth government agencies, credit providers who obtain credit reports, credit reporting agencies and organisations which use tax file numbers) standards for the way that private sector organisations deal with personal information.

What does the Bill seek to regulate?

The Bill is based on the Privacy Commissioner's *National Principles for the Fair Handling of Personal Information* and sets standards for the way organisations deal with personal information, by regulating:

- collection;
- use and disclosure;
- data quality and security;
- storage;
- openness;
- individual access and correction; and
- international transfers; of personal information.

Personal Information is information or an opinion about an individual through which the individual's identity can be ascertained. Some types of personal information are also considered to be sensitive information, with the collection, use and disclosure of the latter being dealt with more strictly.

Sensitive Information includes information regarding racial/ethnic origin, political opinions, religious/philosophical beliefs, trade union membership or details of someone's criminal record, health or sex life.

Who will be exempt from the Act?

(a) Small Businesses

It is proposed that all small businesses, apart from those engaging in activities where there is a privacy risk such as trading in personal information, are exempt. Small businesses that are not exempt have a year of grace to ensure they comply with the legislation.

A small business is defined as a business with an annual turnover of $3 million or less.

(b) Individuals acting in a non-business capacity

Personal information collected and used for non-business reasons will be exempt from the operation of the legislation.

(c) Political parties

Registered political parties will be exempt from the operation of the legislation with respect to activities that involved participation in the political process, such as elections and referendums.

(d) Employee Records

Where an act or practice is directly related to a current or former employment relationship, personal information about the work record of an employee will be exempt from the legislation. The information is likely to include information about training, resignation, termination, terms and conditions of the employment contract, wages or salary, personal and emergency contact details and health information.

Employers cannot use the employee records exemption for commercial purposes unrelated to the employment context.

(e) Journalism

The Bill includes an exemption for acts done, and practices engaged in, by organisations 'in the course of journalism'. This exemption will principally apply to media organisations, but may extend to other groups disseminating news and current affairs.

(f) Others

State and Territory authorities are exempt (unless opted in under Regulations) Other exempt categories include organisations acting under Commonwealth or State contracts, providing specific criteria are met.

Who will be affected by the expanded Privacy Act?

The proposed legislation will apply to the acts and practices of 'organisations'. An organisation may be any of the following:

- an individual;
- a company, or other unincorporated association or organisation;
- a partnership; or
- a trust.

Principles

The key provisions of the Bill relate to:

(a) Collection

Only necessary information may be collected by lawful and fair means, without being intrusive.

Reasonable steps must be taken to inform the individual of all of the following:

- the identity of the organisation who is collecting the information and how they can be contacted;
- the individual's right to gain access to the information;
- the purposes for which the information is collected;
- to whom the information is likely to be disclosed;
- any laws requiring the information to be collected; and
- the main consequences to the individual if he or she fails to provide all or part of the information required.

Personal information must be collected from the individual directly where it is reasonable and practicable to do so. Where it is necessary to collect information about an individual from someone else, reasonable steps must be taken to inform the individual of the matters listed above unless this would pose a serious threat to their life or health.

Sensitive information is not to be collected by an organisation unless:

- the individual has consented
- the collection is required by law
- the collection is necessary to prevent or lessen an imminent threat to life or health of any individual and the individual is incapable of giving consent; or
- in other limited circumstances (for example, research by authorised medical bodies).

(b) Use and disclosure

The legislation makes a distinction between the use of information for the primary purpose of collection and the use for a secondary purpose. Personal information may only be used for a secondary purpose where the two purposes are related and where the individual would reasonably expect the information to be used or disclosed for the secondary purpose. Otherwise, in general, consent is required before use for a secondary purpose is permitted.

The Bill does set out certain limited circumstances where information may be used for secondary purpose that is not related to a primary purpose. These include:

- *direct marketing* - this secondary purpose is available when:
  - the information is not 'sensitive'
  - it is impracticable to seek the individual's consent
  - the individual has been given, but has not taken, the opportunity (without charge) to opt out of receiving direct marketing material;
- *to report unlawful activity* - when an organisation must use or disclose personal information in reporting its concerns to authorities;
- *to prevent threats to life, health or public safety;*

- *when it is authorised by other law;* or
- *activities of enforcement bodies* - for the prevention, detection or investigation of crime or for the enforcement of other laws.

(c) Quality and security

Reasonable steps must be taken to ensure that personal information collected, used or disclosed by an organisation is accurate, complete and up-to-date.

Personal information must also be protected from misuse, loss and unauthorised access, modification or disclosure.

Where data is no longer needed for any authorised purpose, an organisation must destroy or permanently de-identify it.

(d) Openness

An organisation's policies on the management of personal information must be clearly set out in a document available to anyone upon request. The document should explain, in general terms, what sort of information is held and why, and how the organisation collects, holds, uses and discloses that information.

(e) Access and correction

Generally, an organisation must provide an individual with access to his/her own personal information on request. There are exceptions to this rule, such as if the request is frivolous or vexatious or if providing access would reveal a negotiation position. An organisation must state its reasons for refusing to give an individual access to their records.

If an individual can show that records are not accurate, complete and up-to-date, an organisation must take reasonable steps to correct the records.

Organisations may charge a small fee for providing access to the information.

(f) Anonymity

Wherever lawful and practicable, individuals must have the option of protecting their anonymity. Organisations will therefore have to consider carefully whether they really need to collect specific personal details from individuals. Where information can be collected anonymously, organisations need to give individuals the option of leaving out identifying details, such as their name.

(g) Transferring information overseas

The Bill seeks to introduce quite onerous restrictions on the transfer of personal information overseas, reflecting the measures complied with by countries in the European Community.

An organisation under Australian jurisdiction can only transfer personal information to someone in a foreign country (other than internally within its organisation or to the individual concerned) if one of the following occurs:

- the individual consents to the transfer;

- the recipient of the information has a similar law, binding scheme or contract which is substantially similar to the *National Principles*;
- the transfer is necessary for the performance of a contract between the parties or is necessary to conclude a contract in the interests of the individual;
- the transfer is for the benefit of the individual, it is impracticable to obtain the individual's consent and, if it were practicable, the individual would consent;
- the organisation has taken reasonable steps to ensure that information transferred will not be held, used or disclosed by the recipient in a manner inconsistent with the *National Principles*.

(h) Transfer to related bodies corporate

A body corporate that is related to another body corporate will be permitted to share non-sensitive information. However, in using or holding the information, related bodies corporate will be required to comply with the *National Principles* or a binding approved privacy code.

How does the Bill affect existing databases?

The requirements of the *National Principles* relating to *collection, use and disclosure, access and correction* of personal information and *sensitive information* will only apply in relation to personal information *collected after the commencement of the Act*.

However, the provisions relating to *quality of existing databases, data security, openness and transborder data flows* will have a retrospective effect and will apply to personal information *collected both after and prior to the commencement of the Act*. Organisations will therefore need to put in place systems to ensure their existing databases of information comply with these provisions.

What if the privacy principles are breached?

An individual should make a complaint to the organisation concerned in the first instance. If the complaint is not adequately dealt with by the organisation, the Privacy Commissioner or an independent adjudicator (if the organisation in question is subject to a privacy code and that code requires an independent adjudicator to review any complaint) may investigate the complaint.

The Privacy Commissioner or code adjudicator may investigate the complaint and may make a determination that:

- the conduct constitutes an interference with the privacy of an individual
- the conduct shall not be repeated or continue
- any loss or damage suffered by the individual be redressed by means such as compensation (loss or damage includes injury to feelings or humiliation).

The Bill makes determinations enforceable through the Federal Court or Federal Magistrates Court. A determination will also be reviewable under the *Administrative Decisions (Judicial Review) Act 1977*.

The Privacy Commissioner can make public interest determinations, and temporary public interest determinations lasting up to 12 months, to permit the breach of a privacy principle where it is in the public interest.

Developing specific privacy codes.

The Bill permits the development by private sector organisations of their own information privacy codes on an individual or industry basis. However, these codes must provide at least as much privacy protection as the *National Principles* and must be approved by the Privacy Commissioner. The legislative framework will apply in default where industry codes are not adopted.

Some implications of the Bill for E-banking

1. The Bill does not expressly recognise that consents can be given, and disclosures made, electronically. This could be done by applying the *Electronic Transactions Act 1999* (Cth) to the *Privacy Act* after it is amended.

2. If electronic disclosure is recognised, the privacy policy of a financial services provider will have to be disclosed on its web-site, or in documents which will be opened by an individual at or before the time that the individual provides personal information to the financial services provider.

3. Personal information about a person (ie a guarantor) must be obtained only from that person unless it is not reasonable or practicable to do so. The fact that the information may be provided electronically by the applicant for a loan, is unlikely (in my view) to make it not reasonable or practicable to obtain the information from the guarantor. If personal information about another person (say a guarantor) is obtained from an applicant for a loan, the financial services provider must take reasonable steps to inform the guarantor of its privacy policy. Financial services providers will have to design their online systems to obtain personal information wherever possible, from the person to whom the information relates.

4. Financial services providers will also have to be able to authenticate a person providing personal information as the person to whom the information relates.

5. A financial services provider must by encryption or other means ensure that personal information provided on-line is kept secure.

6. A financial services provider must respond to a request from individuals for information about the personal information the financial services provider holds on the individual.

3. *CLERP 6 - FINANCIAL SERVICES REFORM BILL*

The draft Bill was released for public consultation in February of this year. The closing date for submissions on the draft Bill was 12 May. It is intended that the Bill will be introduced into the Commonwealth Parliament in Winter sittings 2000 with a proposed commencement date of 1 January 2001. The Bill will replace current chapters 7 and 8 of the Corporations Law.

The purpose of the Bill is to give effect to a recommendation of the Financial System (Wallis) Inquiry that there be a single licensing regime for financial sales, advice and dealings in relation to financial products; consistent and comparable financial product disclosure; and a single authorisation procedure for financial exchanges and clearing and settlement facilities.

Some key features of the draft Bill are set out below.

Financial Products

A financial product is defined as a facility through which, or through the acquisition of which, a person does one or more of the following:

(a) makes a financial investment;

(b) manages a financial risk; or

(c) makes non-cash payments.

Importantly, credit is not a financial product. A Consultation Paper which was issued in March 1999 had proposed that credit which was not for personal, domestic or household use (and therefore not regulated by the UCCC) would come within the regulatory framework for financial products. As a result of concerns expressed in submissions made in response to the Consultation Paper, credit has **not** been included in the definition of 'financial product'.

The disclosure requirements in Part 7.8 of the draft Bill will not therefore apply to the electronic processing of a loan or other credit facility, but will apply to the extent that the transaction involves the sale of a general insurance product (ie home insurance) or the establishment of a deposit account for interest offset purposes (see definition of 'financial product' discussed below).

The Government proposes, in the final Bill, to give ASIC jurisdiction over consumer protection in relation to all credit (including credit regulated under the UCCC). This will be done by:

- including credit within the range of financial services over which ASIC has jurisdiction under the general consumer protection provisions which are currently contained in the ASIC Act. This will involve a transfer at the Commonwealth level of regulatory responsibility for consumer protection in relation to credit from the ACCC to ASIC; and
- including the equivalent of Section 51AC of the *Trade Practices Act 1974* (which deals with unconscionable conduct in certain commercial transactions) in the general consumer protection provisions for which ASIC is responsible.

Section 764A of the draft Bill sets out specific examples of financial products. These include:

- a security (the definition of security excludes interests in a registered managed investments scheme);
- interests in a registered managed investments scheme;
- a derivative;

- certain insurance products (including general insurance such as motor vehicle insurance, home building or contents insurance, consumer credit insurance);
- superannuation interests;
- deposit taking facilities made available by an ADI.

Some examples of banking products which involve the making of non-cash payments and which will be regulated by the Bill are given in Section 763D. These are:

(a) direct debit arrangements;

(b) traveller's cheques;

(c) smart cards or other purchased payment facilities within the meaning of the *Payment System (Regulation) Act 1998* (Cth);

(d) cheque facilities.

One of the key issues for determining which payment facilities will be financial products and therefore regulated by these amendments is how the definition of 'credit facility' will be defined in the regulations. The reason for this is that in Section 763D (2) of the draft Bill, making payments by means of a credit facility within the regulations is given as an example of a facility which is **not** for making non-cash payments.

The draft Bill also applies to the provision of a financial service.

Retail Client/Wholesale Client Distinction

The draft Bill distinguishes between retail clients and wholesale clients and as a general rule, the disclosure requirements in Part 7.8 of the draft Bill (discussed below) apply only to dealings with retail clients.

The test for retail client depends on the type of financial product involved.

Where the financial product being provided is a general insurance policy of the following type, then the person acquiring the policy is a retail client. Policies are:

- motor vehicle insurance;
- home building insurance;
- home contents insurance;
- sickness and accident insurance;
- consumer credit insurance;
- travel insurance;
- personal domestic property insurance; and
- such other general insurance as is prescribed by the regulations.

A person who acquires any other type of general insurance policy is a wholesale client.

Where a financial product or a financial service is not or does not relate to a general insurance product, then the product or service is deemed to be provided to a retail client unless:

- **(monetary exemption)** the price of the financial product, or of the product in relation to which the financial service is provided, exceeds the prescribed amount. This amount will be set by regulation. It is proposed that the amount be $500,000; or

- **(business exemption**) if a business is acquiring the product or service, the business employs at least:

  (i) if the business is or includes the manufacture of goods - 100 people; or

  (ii) otherwise, 20 people; or

- **(sophisticated investor exemption)** the person acquiring the product or service provides an accountant's certificate stating that the person:

  (i) has net assets of at least $2.5 million; or

  (ii) has a gross income for each of the last two financial years of at least $250,000 a year.

  Any person acquiring a product or service who satisfies one of these tests is a wholesale client.

Disclosure Requirements

The draft Bill contains the following protections (in the form of disclosures) which are required to be given to retail clients:

- the Financial Services Guide;
- the Statement of Advice;
- Product Disclosure Documents.

(a) **Financial Services Guide ('FSG')**

The purpose of the FSG is to ensure that retail clients receive key information about the type of services being offered by a financial service provider. The provisions relating to FSG's are based on requirements currently applying under both the Corporations Law and life insurance regimes, but extend the requirements to the offering of financial services in respect of all financial products.

An FSG need not be given to a retail client where:

- the client has already received the information;
- the service provider is a product issuer dealing in its own products (this exemption would apply to a Bank issuing its own financial products electronically or otherwise). A product disclosure statement would still be required in this situation;
- the service provider is operating a registered managed investments scheme - this exemption applies where the service provider is the responsible entity of the managed investments scheme and the financial service provided is merely the operation by the responsible entity of that scheme;

- general advice is given in a public forum; or
- the regulations specify an exemption. No exemptions are contemplated at this stage.

The FSG must be given to the client before the financial service is provided. There is an exemption where the client instructs the service provider to provide a financial service immediately and it is not practicable to give the FSG before the service is provided. In that case, the service provider must give the client an oral statement containing FSG information that is relevant to the service requested by the client, and must give the client the FSG within 3 days after being given the oral statement.

Section 911G of the draft Bill provides that the FSG may be sent to the client at an electronic address and may be in electronic form.

(b) Statement of Advice

This is required only where personal advice is provided to a retail client. Personal advice is advice that is given to a person where:

- the provider of the advice has considered the objectives, financial situation and needs of a person; or
- the person might reasonably expect the provider to have considered those matters.

The statement of advice may be the means by which the advice is given or a separate record of the advice. A statement of advice is not required where the advice is 'execution related telephone advice'. This is advice given by telephone relating to financial products that are able to be traded on a licensed financial market, that is given by the service provider as an integral part of the execution or transfer of, or order for, those financial products and it is advice for which no fee is charged in addition to the commission fee execution of the transfer or order. This exemption is based on the current Corporation Law except for execution related telephone advice provided in relation to securities. The exemption has been extended to cover all financial products that are able to be traded on a licensed market.

The statement of advice must include the following:

- a statement setting out the advice;
- information about the basis on which the advice is or was given;
- a statement setting out the name and contact details of the provider; and
- information about any conflicts of interest (including commissions or relationships) that might reasonably be expected to be or have been capable of influencing the provider in giving the advice;
- a warning - if the service provider knows or suspects, or must reasonably know or suspect that the advice is based on incomplete or inaccurate information about the client's objectives or financial situation or needs; and
- any other information required by the regulations.

A statement of advice may be given to the client at an electronic address and may be in electronic form.

(c) Product Disclosure Documents

These provisions are found in Part 7.8 of the draft Bill. The disclosure regime in this part will replace the disclosure requirements for:

- superannuation interests under the *SIS Act and Regulations* to the extent that they are dealt with under Part 7.8;
- retirement savings accounts under the *Retirement Savings Account Act 1997 and Regulations*;
- life insurance under Circular G.I.1;
- the products of deposit taking institutions under the *Banking, Building Society and Credit Union Codes of Practice* and the *EFT Code of Practice;*
- interests in managed investment schemes under the fundraising provisions of the Corporations Law; and
- futures under Chapter 8 of the Corporations Law.

Part 7.8 applies only to financial products that are issued, or will be issued, in the course of a business of issuing financial products. However, an initial public offering of interests in a registered managed investments scheme will be regarded as the issue of a financial product in the course of a business of issuing financial products.

A Product Disclosure Statement can take the form of an 'issue Statement' or a 'sale Statement'. An issue Statement is a Product Disclosure Statement that has been prepared by, or on behalf of, the issuer of a financial product. A sale Statement is a Product Disclosure Statement that has been prepared by, or on behalf of, the person making the offer to sell the financial product.

Section 983C of the draft Bill sets out the content requirements for a Product Disclosure Statement. A statement must include the following statements and such of the following information that a person would reasonably require for the purpose of making a decision whether to acquire the financial products as a retail client:

(a) name and contact details of:

  (i) the issuer of the financial product; and

  (ii) if the statement is a sale Statement - the seller; and

(b) information about any significant benefits to which a holder of the product will or may become entitled and the circumstances and times at which those benefits will or may be provided and the way in which those benefits will or may be provided; and

(c) information about any significant risks associated with holding the product; and

(d) information about:

(i) the cost of the product; and

(ii) the amounts a holder of the product will or may have to pay in respect of the product after its acquisition and the times at which these may be payable; and

(e) if the product will or may generate a return to the holder of it - information about any commission or other payment that will or may impact on the amount of return; and

(f) information about any other significant characteristics or features of the product or terms and conditions attaching to it;

(g) information about the internal and external dispute resolution procedures that are available to deal with complaints by holders of the product and about how those procedures may be accessed; and

(h) information about any significant taxation implications of the product that are specific to it; and

(i) information about any cooling off regime that applies; and

(j) if the product issuer (in the case of an issue Statement) or the seller (in the case of a sale Statement) makes other information relating to the product available to holders or prospective holders of a product, or to people more generally - a statement of how that information may be accessed.

In addition to this, there is a general obligation under Section 983D of the draft Bill to include any other information that is actually known to the persons named in that Section and that might reasonably be expected to have a material influence on the decision of a reasonable person whether to acquire the Product as a retail client.

A statement relating to managed investment products, superannuation products, investment life insurance products or a financial product specified in the regulations must be lodged with ASIC before it is given to any person.

A PDS may be updated by issuing a supplementary PDS.

Section 985C of the draft Bill provides that the PDS may be sent to the client at an electronic address and may be in electronic form.

Part 7.8 of the draft Bill contains other consumer protection provisions in the form of:

- restrictions on dealing with money received for a financial product before the product is issued (Section 988A);
- confirming transactions (Section 988B). The confirmation may be provided electronically;
- requirements for the issuer of a financial product to establish and maintain internal and external dispute resolution procedures to resolve complaints from people who acquire financial products as retail clients (Section 988C);

- advertisements or other promotional material for financial products must refer to the Product Disclosure Statement.

A statutory cooling off period is given to retail clients who purchase:

- a risk insurance product;
- an investment life insurance product;
- a managed investment product;
- a superannuation product of the kind prescribed by the regulations; or
- an RSA product;

in Section 998A of the draft Bill. The retail client may give notice returning the financial product to a responsible person, electronically.

Some implications of the Bill for e-banking

1. Some payment products (such as smart cards) will be regulated.

2. Whilst credit (consumer and non-consumer) is not subject to the disclosure requirements of the draft Bill, if a transaction involves the bundling of credit with other products or services which are financial products or services, the disclosure requirements will apply to those products or services.

3. The draft Bill permits the Financial Services Guide, Statement of Advice and Product Disclosure Documents to be given electronically.

4. BANKING CODE OF PRACTICE

This voluntary code is, by its terms, to be reviewed every three years. A review of the Code has just been announced and submissions are required to be lodged by 16 June 2000. Richard Viney has been appointed as an independent person to oversee and direct the review. He is to report his findings and recommendations to the Australian Bankers Association as close as practicable to 31 August 2000.

The relevance and operation of the Code and its provisions are to be reviewed having regard to (among other things):

- consistency with relevant self-regulatory and regulatory measures; and
- anticipated changes in the banking services market in the next three years.

I hope that the outcome of this review will be to:

1. exempt financial products which are the subject of statutory disclosure requirements (such as consumer credit and financial products or services which are regulated by the CLERP 6 Bill) from the disclosure requirements under the Code;

2. allow the disclosure requirements of the Code to be satisfied electronically.

5. EFT CODE OF CONDUCT

The second draft EFT Code of Conduct was released for public comment in January of this year.

The objective of the draft is to create a technology neutral code which covers all forms of consumer electronic funds transfer. Currently, the Code regulates only ATM and EFTPOS transactions initiated by a combination of a card and a personal identification number. The second draft of the Code is intended to cover telephone and Internet banking, credit card payments over the Internet and stored value products such as smart cards and digital cash.

The principal changes to the earlier draft of the Code (which was released in July 1999) include:

Part A - Funds Transfers involving Electronic Access to Accounts

(a) The Code is not intended to regulate high value funds transfers. The options to limit transaction types which are regulated by the Code have been reduced from five (5) in the first draft to two (2) in the second draft. The current options are:

(i) Option A - this would limit Part A to funds transfers from an account, or received into an account, established predominantly for personal, domestic or household purposes. This would exclude funds transfers on small business accounts which are covered by the existing code;

(ii) Option B - would limit Part A to funds transfers below $40,000 unless the funds transfer is of a kind ordinarily undertaken for personal, domestic or household purposes.

(b) The Code applies to account institutions. These need not be traditional financial institutions. The term includes bodies which pay third parties on the instruction of users and debit users accounts to cover the amount of those payments. The definition of 'account institution' has been tightened up to exclude biller institutions which do not permit users to initiate funds transfers that involve the debiting of users accounts with the institutions. The debiting of pre-paid biller accounts is currently excluded from the operation of the Code. However, the working group has noted that because the use of pre-paid biller accounts in the Internet, is likely to increase, that the issue of user initiated funds transfers to billers from pre-paid biller accounts be reconsidered on the next review of the Code.

(c) The notice period to advise customers of changes to EFT terms and conditions has been amended to bring it into line with the requirements of the UCCC.

(d) The first draft of the Code required that the receipt issued at the time of an EFT transaction show, where possible, any fee applicable to the transaction. This requirement has been removed from the second draft although the issue of whether there needs to be improved disclosure of fees and how this can be achieved is still on the table for discussion.

(e) Liability for unauthorised transactions - three options for allocating liability were put forward in the first draft of the Code. The second draft provides for an initial no fault allocation of liability to the user in all cases where a secret code is required to perform the unauthorised transaction. The user is liable for a maximum of $150 unless the account institution can prove on the balance of probabilities that the user contributed to the losses through unreasonably

delaying notification or that the users fraud or contravention of the requirements of clause 5.6 of the Code was the dominant cause of the loss.

(f) The obligations on users to safeguard secret codes, in clause 5.6 has been upgraded and the user will now breach clause 5.6 if, despite being warned by the account institution not to select a secret code which represents the user's birthdate or name, the user selects such a numerical or alphabetical code.

(g) Clause 5.7 (b) in the second draft expressly recognises the ability of account institutions to provide in their terms and conditions or other communications to users, guidelines for users on ensuring the security of an access method, if the guidelines are consistent with clause 5. However the terms and conditions or other communication must make clear that the guidelines are not the basis on which the user is assessed for liability for losses resulting from unauthorised transactions and that such assessment will be determined under the Code.

(h) Under clause 5.5 of the Code, the account holder's liability for unauthorised transactions resulting from a failure to comply with the requirements of clause 5.6 of the Code or an unreasonable delay in notifying misuse, loss or theft of a device forming part of the access method or a breach of the security of the Code forming part of the access methods, does not extend to losses in excess of the daily transaction limit.

In the review of the first draft, it became clear that not all account institutions apply daily transaction limits to withdrawals from electronic terminals. Clause 5.11 of the Code now sets the daily transaction limit at $1,200 (unless a lower amount has been notified to the account holder by the account institution). To set a daily transaction limit exceeding $1,200, the account institution must propose that amount to the account holder, disclose the risks of that higher amount to the account holder and obtain the account holder's specific and unambiguous consent to that higher limit by a positive act. **The commentary on this provision says that the intention of the requirement for a positive act is that mere use of the access device following receipt of the proposal is insufficient to amount to a consent and a response by a positive act such as ticking a box on a form or clicking an 'I agree' button on a web page is required.**

Part B - Rules for Consumer Stored Value Facilities and Stored Value Transactions

(a) This part has been significantly revised with the intention of making it simpler and shorter and giving greater flexibility of implementation, in recognition that stored value products are still developing. This part applies to the use of a stored value facility by an individual. This requires that the facility is used by the user predominantly for personal, domestic or household purposes.

(b) Part B of the Code imposes obligations on a 'stored value operator' which means an entity which subscribes to the Code and which is an issuer or a payment facilitator or both an issuer and payment facilitator in respect of the stored value facility. These obligations relate to:

- availability and disclosure of information and terms and conditions applicable to the stored value facility - stored value operators may provide a summary of the terms and conditions and other pre-use information if it is not feasible to provide the full information;

- changing the terms and conditions of use - where the stored value operator knows the identity and contact details of a user, the stored value operator must provide the information directly to the user. Otherwise, the stored value operator must publicise the changes in the manner which is likely to come to the attention of as many users as possible;

- exchanging stored value for money or replacement stored value - in certain circumstances;

- ensuring that, to the maximum extend practicable a user whose stored value is lost or stolen will be provided with either an equivalent amount of stored value or the equivalent amount of money;

- establishing internal complaint handling procedures similar to those provided for funds transfers under clause 10 in Part A of the Code.

(c) The stored value facility must enable the user to ascertain the amount of stored value which is available for use.

Part C - Privacy, Electronic Communication, Administration and Review

(a) Clause 21 - the privacy provisions which were in Part A and Part B in the first draft are now in this clause. The prescriptive requirement as to privacy which are in clause 10 of the existing Code have been replaced with an obligation on subscribers to comply with:

- before the *Privacy Amendment (Private Sector) Bill 2000* is enacted - the *National Principles for the Fair Handling of Personal Information*; and

- on or after the date referred to in the preceding paragraph - the information privacy principles in the national privacy legislation or in codes which are approved under that legislation to which the EFT Code subscriber has also subscribed.

(b) Clause 22 dealing with electronic communications is substantially unchanged from the first draft. However, in the context of this paper, it is worth noting that this provision allows a Code subscriber and a user to agree to provide information which the Code requires to be provided (by writing or other means) by electronic communication. Where a Code subscriber has provided information electronically, the Code subscriber is required to provide a paper copy of that information to the user if the user so requests within six months of receipt of the electronic communication.

Some implications of EFT Code for e-banking

1. Part A will apply to consumer or small value funds transfers transacted on-line.

2. Part B will apply to smart cards and other purchased payment facilities.

3. The Code permits provision of information electronically.

6. COMMONWEALTH TREASURY'S E-COMMERCE BEST PRACTICE MODEL FOR BUSINESS

The final version of the Best Practice Model was released last month (May 2000). As its title suggests, the Model aims to set out best practice for business to consumer electronic commerce. Compliance with the Model is voluntary except to the extent that the Model reflects existing laws.

The Model's objective is to guide businesses on:

(a) their business practices - in this context, the Model requires businesses to ensure that:

- electronic delivery of goods or services can be achieved without specialised software or hardware, unless the requirement for such specialised software or hardware is made clear to the consumer before hand.

(b) Advertising and marketing - the Model requires businesses to ensure that:

- advertising material is clearly identifiable and can be distinguished from other content;
- the business does not send commercial email except to people with whom the business has an existing relationship or to people who have already said they want to receive commercial email;
- the business has simple procedures so that consumers can let them know they do not want to receive commercial email;

(c) Disclosure of a contracts terms and conditions - the Model requires that:

- businesses should give consumers a clear and complete text of a transactions terms and conditions. This information should be clear enough so that the consumer can access and retain a record of that information, for example, by printing or electronic record;
- businesses should put in place procedures that let consumers:
  - (i) accept or reject the terms and conditions of the contract;
  - (ii) identify and correct any errors; and
  - (iii) confirm and accept or reject the offer.
- businesses should promptly acknowledge receipt of the order.

(d) Privacy - as a minimum, businesses must comply with the *National Principles for the Fair Handling of Personal Information.*

(e) Using and disclosing information about payment, security and authentication mechanisms - the Model requires that businesses:

- make sure consumers have access to information about the security and authentication mechanisms the business uses in clear simple language which helps consumers assess the risk in relying on those systems;
- provide the security appropriate for protecting consumer's personal and payment information;
- provide security appropriate for identification and authentication mechanisms to be used by consumers;
- discourage consumers from giving confidential information in a way that is considered insecure;
- update their security and authentication mechanisms at the time to make sure that security offered is maintained at its appropriate level; and
- not to try to contract out of their responsibility for losses arising from the misuse or failure of authentication mechanisms.

CONCLUSION

The regulatory framework for e-banking is dynamic and evolving fairly quickly. The challenge for regulators is to determine how to achieve a balance between facilitating new ways of doing business and adhering to the consumer protection objectives of existing laws.

The challenge for the financial service sector is to participate in this process and to develop the new technologies which can deliver this balance.

These are exciting times!