



# Electronic Funds Transfer Code of Conduct (EFT Code)

Compiled by  
Ian Gilbert, Director  
6 June 2007

## Table of Contents

---

Section 1 - Other Issues-----	3
Section 2 - Marketplace developments-----	5
Section 4 - Regulatory developments -----	12
Section 5 - EFT Code, Part A (Scope and Interpretation)-----	13
How the scope of Part A is defined-----	13
Notifying Changes to Fees -----	16
Issuing Transaction Receipts -----	16
Merchant Identification on Transaction Receipts-----	17
When a Transaction Receipt Should Disclose Remaining Balance. -----	17
Consistency between Part A and Corporations Act-----	18
Are there aspects of the legal framework that the EFT Code should adopt? ---	19
Obligation to Advise Account Holder of Discrepancies -----	19
What is a Complaint? -----	19
Standard for Internal Complaint Handling-----	20
Meaning of “immediately settled” Complaint -----	21
Time Frames for Resolving Complaints -----	21
Internal Complaints Handling -----	21
Investigating Complaints and Availability of Record -----	22
Time Limit on Resolution of Complaints under the EFT Code-----	22
Section 7 - EFT Code, Part A (Liability; mistaken payments) -----	23
Liability for losses resulting from deceptive phishing attacks -----	23

---

<b>Code security breaches by user attracting account holder liability (cl 5.5 (a) and 5.6)</b> .....	<b>23</b>
<b>Unreasonable delay in notification (cl 5.5 (b))</b> .....	<b>24</b>
<b>No fault liability limit (cl 5.5 (c))</b> .....	<b>25</b>
<b>Liability allocation and 'book-up'</b> .....	<b>25</b>
<b>Liability in cases of system or equipment malfunction (cl 6)</b> .....	<b>25</b>
<b>Mistaken payments</b> .....	<b>26</b>
<b>Section 8 - EFT Code, Part B (Scope and interpretation)</b> .....	<b>26</b>
<b>Part B scope and interpretation: other aspects</b> .....	<b>27</b>
<b>Section 9 - EFT Code, Part B (Requirements)</b> .....	<b>27</b>
<b>Right to exchange/replace stored value (cl 15)</b> .....	<b>28</b>
<b>Right to unilaterally vary terms and conditions</b> .....	<b>29</b>
<b>Complaint investigation/dispute resolution (cl 19)</b> .....	<b>29</b>
<b>Payment finality</b> .....	<b>29</b>
<b>Section 10 - EFT Code, Part C (Privacy and electronic communications)</b> .....	<b>30</b>
<b>Privacy obligations (cl 21)</b> .....	<b>30</b>
<b>Section 11 - EFT Code, Part C (Administration and review)</b> .....	<b>33</b>
<b>Modifying the EFT Code</b> .....	<b>33</b>
<b>Monitoring Compliance</b> .....	<b>33</b>
<b>Reviewing the EFT Code</b> .....	<b>34</b>

## **Submission to ASIC re Electronic Funds Transfer Code of Conduct (EFT Code)**

---

In the ABA's view, increased participation is a key issue for the future of the EFT Code. For that reason, questions relating to participation are addressed first.

### **Section 1 - Other Issues**

#### **Question 68: In your view, why has membership of the EFT Code remained limited generally to providers of generic banking services?**

Possible explanations for low take up outside of ADIs include:

- a) There may be provisions of the EFT Code that non-members may regard as unnecessarily onerous or prescriptive, making the EFT Code unattractive for them. A more principle based approach to the EFT Code and simplification of its provisions, such as to more accurately identify the transaction types to which it applies, would make membership more attractive. In particular, simplification could reduce compliance costs, which the ABA understands are likely to be a major disincentive to subscription.
- b) New market participants being unaware of the EFT Code and the positive benefits the EFT Code could make to their businesses.
- c) Exemptions enjoyed by certain market participants under chapter 7 of the Corporations Act 2001 (FSR) in relation to the issuing of certain facilities for making non cash payments, possibly leading to the assumption that their activities should be entirely unregulated.
- d) Unlike the Code of Banking Practice (CBP) there is no obligation on ASIC to actively promote the EFT Code.
- e) Because membership of the EFT Code is voluntary non-members may take the view that it is unnecessary for them to adopt the EFT Code.

#### **Question 69: What steps could/should be taken to broaden EFT Membership?**

EFT Code membership would be more attractive if consumers had a preference to deal with subscribers to the EFT Code. ASIC should encourage consumers to question whether the facilitator of their EFT transactions subscribes. ASIC could also provide positive press highlighting those institutions that do subscribe. One way to do this would be to introduce and publicise a symbol that subscribers could display and use in their documentation.

Added to this, there could be an "if not why not" approach to non membership. Organisations that could be expected to be signatories to the EFT Code but who are not could be asked to explain to ASIC as part of the public record why they have not taken up the EFT Code if it could apply to them. This review process would be an excellent opportunity for ASIC to seek to do this. It could help understanding, and identify what barriers to membership of the EFT Code exist.

ASIC could publish these membership and non-membership details in its annual compliance report.

**Question 70: How much of the EFT Code's requirements do non-subscribing entities take into account even though they do not subscribe to the EFT Code?**

The ABA has not conducted research into this. A survey of terms and conditions for relevant products and services of non-subscribing entities may give some indication.

**Question 71: What changes could/should be made to the way the EFT Code is written, designed and presented to make it a more user friendly and accessible document?**

The ABA has identified the style and presentation of the EFT Code as a possible barrier to adoption by organisations. There seems to be general agreement that the current version of the EFT Code is technical, prescriptive and in need of a plain English re-write. We are aware that ASIC is keen to do this and the ABA would be happy to discuss what contribution it might make in the course of this review.

There would be wide-spread support among ABA members for the design and drafting of the EFT Code to move to a more principles based approach, and to rationalise its provisions taking into account relevant provisions of the FSR and any other overlapping legislation or codes of conduct which may already cover areas the EFT Code seeks to regulate.

**Question 72: Should the EFT Code include a statement of objectives? If so, what should the objectives of the EFT Code be?**

The ABA would support the inclusion of a statement of objectives. The ABA submits that the objectives of the EFT Code are:

- to protect consumers and promote consumer confidence in transacting in an EFT environment;
- to provide a package of protections that promote sound business practices, recognising the need to balance costs and benefits to consumers and industry;
- to promote informed decision making;
- to provide clear guidance to consumers and industry about their rights and obligations; and
- to promote membership of the EFT Code.

**Question 73: Are there other issues not covered in the Consultation Paper that the review should address?**

As noted in the covering letter to this submission, the ABA has largely confined its submissions on the EFT Code to those areas in relation to which ASIC invited comments. However, if, during the course of ASIC's inquiry, other issues relevant to our members arise, the ABA would appreciate an opportunity to consult with ASIC.

## **ATM Reform**

The ABA notes ongoing discussions around reform to regulation of the ATM industry. As ASIC has noted, a large proportion of ATMs are now operated by non-bank entities, which typically do not subscribe to the EFT Code.

The EFT Code governs the relationship between the customer and the card issuer, but does not address the relationship between the customer and other parties that may also provide services to the customer, for example the ATM operator. For the sake of customer security and competitive neutrality, ATM operators should be subject to the same obligations that would apply to banks if they provided those services.

To what extent amendments to the EFT Code will be able to address those issues will of course depend on the form of any other new regulatory arrangements for ATM operators, but at a minimum existing provisions should recognise the emerging issue.

For example, the EFT Code should reflect that:

- card issuers cannot control the setting, disclosing or charging of fees by non-bank ATMs; and
- where a complaint has arisen in relation to a transaction involving a non-bank ATM operator, a bank may face difficulties in resolving the complaint in a timely manner, despite endeavours to do so. The difficulties arise because disputes can arise due to conduct of a non-bank ATM operator, which does not subscribe to the EFT Code, and delays are experienced in liaising with these network providers to resolve disputes.

However, how these issues are to be addressed cannot be finalised until the nature of the ATM reforms has been settled.

## **Overlap between the EFT Code and the Credit Card Scheme Rules and BPay Scheme Rules**

ASIC has identified overlap between the EFT Code and other instruments as an issue for the current review, particularly in relation to some specific issues. One of the areas that would benefit from attention is the overlap between the EFT Code and the Credit Card Scheme Rules. While the Rules are not legislation, they are mandatory for participating banks. One of the areas of overlap is in relation to complaints, which is discussed further in response to question 21 below.

Similar issues arise in relation to the BPay Scheme Rules.

## **Section 2 - Marketplace developments**

### **Commentary: Emerging Payment Systems**

#### **Background**

The global payments landscape is complex and diverse. Many of the elements of this landscape are in the process of being superseded by new innovations which offer increased convenience, consumer security and fraud control. It is important

that the application of the EFT Code is consistent with principles of competitive neutrality.

Payment systems within Australia's financial transaction market consist of two elements — payment products and payment channels. Every payment requires a product to hold value ('payment product') and a channel through which to conduct the transfer ('payment channel'), either cash or the information required to exchange balances. The major payment products are cash, payment cards, paper products (cheques, money orders etc) and electronic products.

Payment channels facilitate the use of a payment product by providing a mechanism to establish contact between the payer and the payee. Within Australia's financial transaction market there are four categories of payment channels: electronic, over the counter, negotiable instruments and emerging systems. Electronic channels facilitate the use of a number of payment products, such as credit cards, debit cards, and direct entry products.

### **Overview of Emerging Channels**

Emerging payment channels constitute innovative mechanisms for facilitating the use of a payment product by providing new and more convenient ways to establish contact between the payer and payee.

Some of the key innovations are:

- Near Field Communications (NFC) – a short range wireless connectivity technology. Communication between two NFC compatible devices occurs when they are within four centimetres of one another, using an NFC connection and wireless technology such as Bluetooth or Wi-Fi. The short transmission range means NFC enabled transactions are inherently secure. NFC can be used within a variety of devices, including mobile telephones.
- Radio Frequency Identification (RFID) – an automated data capture technology, which is used in most contactless payment system products. There are three main technology components of an RFID system: a tag, a reader and a database. RFID is already used in Australia. For example, in 2002 Telstra introduced a mobile telephone payment facility to pay for parking in some areas of Sydney and Melbourne. The system was subsequently extended to buying soft drinks from vending machines.
- Biometrics – the use of physical attributes to enable payments, such as fingerprints instead of a signature or PIN. While some US supermarkets have a 'pay by touch' application, biometric payment systems are generally seen to be at least five years away from widespread use in open payment networks.

A number of innovative security technologies have been, or are about to be, deployed across banking sector products worldwide. These include:

- EMV (Europay MasterCard Visa) Chip Cards and consists of credit or debit cards that include an embedded microprocessor (smart card) chip. Rather than swiping the magnetic chip of a traditional

payment card the EMV cards are dipped into a slot that reads data from the chip;

- 3-D Secure technology protocols: Internet transaction targeted technologies which require cardholders and merchants to enrol in a program to obtain a password;
- Digital Signatures - Incorporate technologies that use private and public key methods to authenticate both parties to the transaction. Digital signatures are primarily used in high risk environments such as B2B transactions;
- Passmark Authentication: Involves provision of alternative personal identity information to provide assurance to the authenticating party that the transaction initiator is properly identified. These allow a user to enrol in the program and select an icon/picture that is unique to the user;
- PC Fingerprinting: Enables the network to identify the unique characteristics of the Internet access device to prove that this device was used to make the transaction; and
- 2 factor authentication: Uses the traditional username/password or PIN along with a small electronic device (e.g. mobile) that creates a random login number required to complete access.

**Question 1: What do you see as emerging trends in the consumer payments marketplace over the next few years?**

In addition to the discussion above an informative publication by the Australian Department of Communications Information Technology and the Arts entitled "Exploration of Future Electronic Payments Markets" June 2006 is available at [http://www.dcita.gov.au/data/assets/pdf\\_file/40522/Exploration\\_of\\_Future\\_Electronic\\_Payments\\_Markets.pdf](http://www.dcita.gov.au/data/assets/pdf_file/40522/Exploration_of_Future_Electronic_Payments_Markets.pdf). This publication provides a comprehensive forward-looking view of future payments markets.

**Question 2: Are there trends or developments that the Review Working Group should particularly consider in reviewing the EFT Code? What implications might these have for the regulatory scheme of the Code?**

The volume and value of electronic payments have increased dramatically over the last decade and growth is expected to continue. However, some significant changes are expected in the nature of electronic transactions, including:

- an increase in the provision of services by non-traditional participants, such as mobile telephony providers, internet trading facilitators (e.g. EBay Paypal) and suppliers of prepaid cards;
- increased use of debit transactions, including due to fee structures increasingly allowing unlimited transactions, and an increased ability to transact over the telephone and internet;
- growth in the use of 'reverse EFTPOS' facilities, such as direct rebates provided by health insurance providers,

- growth in contactless payments e.g. using NFC or RFID, and in unattended payment terminals, for example new card ticketing facilities being introduced by NSW and Queensland government public transport authorities;
- introduction of mobile banking and mobile payments services, which could potentially use a number of technologies, such as SMS, Java and mobile broadband;
- developments in chip card technology;
- increased use of PIN verification in place of signature verification (e.g. PIN@POS), which will result in a potential increase in transactions being dealt with under the EFT Code, whereas they would previously have been dealt with primarily under the Credit Card Scheme Rules;
- growth in the provision of ATMs by non-banks (see issues raised in response to question 73).

**Question 3: What are the issues associated with the emergence of 'non-contact' payment facilities?**

Key issues associated with the emergence of non-contact payment facilities include:

- an increase in the participation by non-ADIs, including government authorities and mobile telephony providers, who are not typically subscribers to the EFT Code, making broader membership vital to give consumers confidence in electronic transactions and provide for competitive neutrality;
- the potential for the introduction of new parties into payment systems, such as networks and back end database providers, again raising issues about the application of the EFT Code to all parties that may be involved in the provision of services to customers;
- the need for new rules regarding the issue of receipts. Use of non-contact payment facilities is likely to be in situations requiring faster, lower value transactions, in situations similar to cash. In many situations, giving receipts will be impractical, for example, while passing through a public transport turnstile.

**Question 4: What do you see as the main challenges in relation to online fraud over the next few years? Are there trends or developments that the Review Working Group should particularly consider in reviewing the EFT Code?**

Unfortunately, online fraudsters are becoming increasingly sophisticated. It can be expected that new forms of fraud, such as those identified by ASIC, will be attempted. It is in the interest of consumers and banks to prevent fraud to the highest degree possible, and to identify any fraudulent activity quickly. Steps taken by the banks are discussed in response to question 5 below.

Challenges in relation to online fraud include:

- ensuring that consumers are aware of risks involved in electronic transactions;
- ensuring that consumers are well educated about the steps they can take to mitigate those risks;
- ensuring that all industry members that participate in electronic transactions take steps to protect the security of transactions; and
- ensuring that the regulatory regime is flexible enough to take account of new threats and new technology, and stays up to date, so that it provides a strong tool to address online fraud.

**Question 5: What information can you provide to the Working Group (including on a confidential basis) about online fraud countermeasures being considered or deployed by Australian financial institutions? How does the Australian response compare with that of other comparable countries, in your view?**

Banks have been proactive in taking steps to reduce the risks of fraud, and to identify and mitigate fraudulent activity. Key measures undertaken by banks include:

- prevention – customer and merchant education, authorisation processes and merchant card acceptance procedures;
- detection – fraud detection tools for monitoring spending and merchant activity patterns, exception reporting, behavioural analysis and surveillance at ATMs; and
- investigation – specialist in-house investigation teams, liaison with law enforcement agencies and card schemes.

With the advent of electronic banking, banks also introduced technological safeguards, which are continually upgraded, and are increasingly sophisticated.

Recent initiatives to improve online fraud countermeasures include:

- deployment of more advanced detection capabilities;
- deployment of stronger identification such as 2 factor identification, provision of alternative personal identity information and computer fingerprinting, enabling a bank to identify a user's PC;
- banks are cooperating with each other and industry bodies such as AusCERT via various forums to exchange information regarding new/emerging threats.

Just as banks are trying to keep abreast of developments in fraud and best practice, so must regulatory instruments and the bodies that enforce them. Sufficient resources should be in place to ensure that this can occur. The fast pace of change would support more frequent reviews of instruments such as the EFT Code.

Examples of some of the measures introduced by member banks are set out below.

### 1.1 Education and technology

Banks and industry bodies such as the ABA have very significant investments in measures to address online fraud including:

- customer education - the ABA invites ASIC to visit members' websites for further information about banks' extensive customer education programs. The ABA also has a financial literacy information centre (see [www.bankers.asn.au](http://www.bankers.asn.au) and click on "financial literacy"); and
- technology - a wide variety of technologies are used by banks to prevent online fraud and other crimes. Again, banks' websites are a good source of further information.

### 1.2 Process

Bank processes are designed to prevent online fraud and other crimes. For example, banks employ rigorous customer identification procedures to ensure they are dealing with the right person.

In order to detect crime, they deploy sophisticated transaction analysis systems, which identify unusual transactions.

### 1.3 Overseas comparison

Australian banks are very well positioned in relation to comparable institutions overseas, in each of the dimensions described above, and undertake regular reviews of their capabilities and technology against overseas best practice.

**Question 6: Is the growth in, and growing publicity given to, fraud issues having an impact on online transacting in Australia at present? (Again, you may wish to provide information on a confidential basis.)**

It is very difficult to measure any effect on consumer confidence of transaction volumes.

The ABA has no evidence that the incidence of fraud is having a negative impact on online transacting. Anecdotally, transaction volumes and usage are on a steep increase on a constant basis, suggesting that the convenience provided to internet bankers continues to draw new and increased transactions and online fraud has little impact on actual volumes.

The most recent data available (March 2006), from the Market Intelligence Strategy Centre, indicates that registrations for online banking continue to climb: they doubled in the four years covered by the report (from 30 September 2001). In that same period, the number of online accounts tripled, and transaction volumes increased by 130%.

Conversely, the ABA is unable to gauge whether added publicity about fraud issues has meant that there would have been a higher rate of increase in on-line transacting but for the increased publicity.

It should also be noted that fraudulent transactions represent a very small proportion of overall transactions, and of total volumes processed.

**Question 7: What information can you provide to the Working Group about the online fraud mitigation skills of Australian online users?**

Australian users are still in the process of "coming to grips" with the vast array of security measures required to secure their computers.

In general terms, it seems that awareness of online threats is improving, but on the whole, online transactors have deployed minimal counter-measures to combat online fraud. It would be difficult to quantify this claim, but it is suspected there is a large apathy in relation to having up to date security software and deploying regular operating system updates. In many cases, anti-virus software may be installed, however, anti-spyware, software firewalls, patches, security updates etc are often not installed or not up to date, negating any tangible protection afforded by the installation of anti-virus software.

Banks can offer customers advice about minimum protection standards. New threats arise as fraudsters become more sophisticated, so security arrangements need to be constantly updated.

The ABA understands from anecdotal evidence that online users are increasingly aware of specific threats such as phishing, but there are still users who respond to such emails, some on multiple occasions.

Banks have responded to emerging fraud risks through offering additional security options, such as 2 factor authentication, discussed further above. ABA members will continue to combat fraud through a combination of education, process and technology.

The following extract from the Australian Institute of Criminology provides some background on online fraud in Australia:

*The Australian Institute of Criminology (AIC) reports that: "Australian online traders are usually provided with numerous suggestions for fraud prevention strategies by their financial institution, which are intended to reduce the risk of businesses accepting fraudulent online transactions (National Australia Bank 2002b; Westpac 2000). These suggestions usually centre on manually screening orders prior to sending the goods in addition to obtaining electronic authorisation. Retailers are told of possible 'warning signs' which may indicate a customer who is not genuine, such as an overseas mailing address or a postal box address instead of a physical address. Retailers are also warned about:*

- \* orders comprising duplicate items (they may be sold on);*
- \* orders placed on a rush or with immediate delivery (fraudsters are not concerned with delivery costs and want the items quickly);*
- \* cards that have been used previously and found to be fraudulent; and*
- \* customers who provide an email address from a free email service (Tomlinson 2002).*

*In addition to being wary when these 'warning signs' appear on an order, online traders are advised to:*

- \* verify the order with the customer by telephone or email;*
- \* confirm the address with the financial institution or recent telephone directory;*
- \* establish a database which records good and bad customers (to ensure speedy approval and no unnecessary screening); and*
- \* request information from the customer which only the cardholder would know (address, digits on back of card, bank who offers the card, and so on).*

*Although there are clearly numerous methods recommended to Australian traders to prevent online credit card fraud, it is important to know the degree to which they are employed in day-to-day processing. This would help to establish whether additional strategies need to be developed or existing ones implemented. Further, it is important to know why businesses do not use particular strategies. This latter point is yet to be investigated.*

*The Cybersource survey from the United States (2003) found that 65 per cent of online traders manually screened orders, with each retailer reviewing an average 23 per cent of orders placed on their web site. The study reported that the manual review techniques employed (in order of common use) were:*

- \* phoning the customer (78%);*
- \* checking customer records (64%);*
- \* emailing the customer (61%);*
- \* phoning the bank (58%); or*
- \* checking a 'bad customer' database (40%).*

*In the UK it was similarly reported that 55 per cent of the sample employed manual fraud detection systems and 15 per cent had automated systems for fraud detection (Experian 2001). To date, there have been no surveys published examining the use of these strategies in Australia, hence the importance of probing these issues in the present study."*

## **Section 4 - Regulatory developments**

**Question 8: Are there developments in the regulatory environment that the Review Working Group should particularly consider? What are the implications for these developments for the EFT Code?**

### **ATM reform**

As discussed in response to question 73, there will be the need to consider the implications of the final and outstanding item on RBA's reform of payment instruments, including ATM direct charging, access and disclosure. If this

becomes a reality, then organisations outside of regulated institutions will be able to establish a direct relationship with customers by setting fees for cash access. These organisations typically do not subscribe to the EFT Code or the CBP. It will be important to ensure the appropriate accountability is placed together with this capability.

### **Corporations Act 2001**

The ABA supports the inclusion in the EFT Code of Conduct of risks to be covered in information materials or at the request of the customer, or where applicable, Product Disclosure Statements for all non-cash payment facilities taking into account recent changes made to disclosure required under the Corporations Act. Subscribers should be able to formulate these disclosures themselves rather than through prescription in the EFT Code.

### **CBP**

Any changes to the EFT Code that are also applicable under the CBP should be consistent between both codes for example Electronic Communications.

### **Anti money laundering reforms**

The ABA agrees with ASIC's observations in the Consultation Paper about AML/CTF reforms and assumes that the EFT Code would not seek to set different standards, procedures, systems or controls for customer ID than are contained in the AML/CTF Act and Rules.

## **Section 5 - EFT Code, Part A (Scope and Interpretation)**

### **How the scope of Part A is defined**

**Question 9: Do you have any suggestion as to how the scope of Part A of the Code might be defined more simply? Should Part A include a non-exhaustive list of the main types of transactions to which it applies?**

The ABA agrees that the key EFT Code definitions that provide the scope of the Code are complex and can be simplified.

A suggested approach to simplifying these definitions could be to describe the electronic payments services intended to be captured by the Code. These should be technology neutral, so that they capture any mobile device, including mobile telephones, Blackberries and PDAs. This would be a functional approach in the same way the FSR is structured, and would make it easier for financial institutions to identify transactions and disputes falling under the EFT Code.

For example, the Hong Kong Association of Banks Code of Banking Practice defines "electronic banking (e-banking) services" as

- *"Banking service delivered over the internet, wireless network, automatic teller machines (ATMs), fixed telephone network or other electronic terminals or devices"*.

This definition could be modified to be included in the EFT Code for instance by replacing "Banking services" with "Electronic transacting services".

The technical means of initiating, accessing and completing electronic transactions by the methods described are built into and form an integral part of those electronic payment facilities. It would be unnecessary to further define these facilities as their descriptions are of sufficient generic understanding to satisfy a code based regulation.

This approach would capture any institution providing an electronic payment facility. It serves a consumer need and provides a reason why non-EFT Code subscribers should subscribe to the EFT Code.

To the extent that other definitions should be modified and retained, for example "access method", this will be necessary where those expressions are used in Part A of the Code.

**Question 10: Should biller accounts continue to be excluded or should small cl 1.4 be modified or, alternatively, removed altogether?**

The ABA's members do not provide biller accounts and therefore do not offer a view on whether there should be a blanket exemption for biller accounts.

However, the ABA submits that even if there is a prima facie exemption for biller accounts, the EFT Code should be drafted such that billers can opt in to the EFT Code and elect to comply with it. For example, as discussed above in relation to encouraging membership, it is possible that a biller may wish to comply with the EFT Code in order to obtain a reputational benefit.

The ABA also submits that a bank should have the ability to resolve a dispute arising in relation to use of B-Pay under the B-Pay Scheme Rules, as discussed further in response to question 21.

**Question 11: Do small businesses experience problems in relation to their banking services that need to be addressed? Does the EFT Code provide an appropriate framework for addressing any problems identified?**

In paragraph 5.19 of the Consultation Paper there is a proposal that the extent of problems small business users of banking services experience should be examined to determine whether there is a problem that needs regulatory intervention.

The ABA agrees that this an appropriate first step to be taken before deciding whether small business should fall within the scope of the EFT Code. Assuming a market failure is identified, the further steps in process should include evaluating alternative options including whether there is a need to do anything at all and then a cost and benefit analysis if the EFT Code option is chosen.

This step should extend to all institutions providing small business electronic transacting facilities, not simply those provided by banks.

The ABA notes that any such review would require the identification of what constitutes a small business, as opposed to a large business. This is not a simple task. First, it requires the identification of parameters, which could be based on number of employees, or level of turnover. Neither of these is static, and turnover may not be able to be predicted ahead of time. A bank may not know from time to time whether its customer falls into the definition of a small business. The

point in time at which a classification is undertaken will also be important: is it when an account is opened, when a complaint arises or some other time? Each presents challenges.

Obviously it is necessary to have good disclosure to small business customers of the benefits, costs and risks and technical requirements associated with any product, but the existing disclosure regimes for small business customers already achieve the required high level of disclosure. Small business customers already have adequate protection under the CBP and the ability to raise disputes with the Ombudsman. Generally small business accounts involve and demand far greater levels of security than consumer accounts due to the much larger amounts concerned. In addition, small business is able to insure against the risk of loss. A further point to consider is that small business may have an additional level of complexity of transactions as often it will be staff employed who initiate and conduct transactions.

It should be noted that little in the nature of small business accounts has changed since the last review of the EFT Code when the question on the inclusion of small business was raised. The higher value and frequency of small business electronic transacting compared with consumer transacting could necessitate changes to some of the EFT Code's provisions, such as liability for unauthorised transactions and complaint investigation and resolution procedures that could operate as a disincentive to small business users' use of many products. Small business and consumer users have fundamentally different needs in relation to transaction volume, value and payment channels. The range of transactional needs of small business customers, and therefore the services utilised by small business customers, are substantially more complex than those utilised by consumers, as the skills and resources available to business customers are also more complex.

The EFT Code has set rules on the sharing of risk between account institutions and consumers intended to meet the objective of the EFT Code in protecting consumers. The EFT Code does not take into account the complexity, sophistication, or risk of the service, consistent with the objective of having a clear document easily understood by the consumers it is designed to protect. Applying the EFT Code to small businesses customers would be inconsistent with both the current diverse range of transactional products available to small business customers, and to the future development of a wider range of services.

Without substantial evidence of market failure the ABA believes that the EFT Code should continue to apply only to consumer transactions.

### **Section 6 - EFT Code, Part A (Requirements)**

In this section, there are opportunities to harmonise the provisions of the EFT Code and the CBP.

## Notifying Changes to Fees

**Question 12: Should the requirements of cl3.1 to provide written notification in advance of an increase of a fee or charge be replaced<sup>1</sup> by another process? For example, should the notice appear in the national or local media on the day on which the increase starts?**

The CBP provides explicit notice requirements (clause 18) where changes are made to terms and conditions of banking services.

Under the CBP a "banking service" means any financial service or product provided by a bank to a customer. A banking service includes a facility for making non-cash payments or, in other words, an electronic funds transfer facility.

For banks that have adopted the CBP, clause 3 of the EFT Code should defer to clause 18 of the CBP. The CBP permits notification of variations in bank fees and charges by newspaper advertisement which is recognised as an efficient and effective means of notifying customers and could be adopted also in the EFT Code.

Banks should also be permitted to notify customers of changes by electronic means, particularly where customers have nominated to receive electronic statements. For example, a bank could post notice on its website and/or in the "messages" section of a user's internet banking page, send an email, or, where a customer has provided a mobile telephone number, send an SMS message.

## Issuing Transaction Receipts

**Question 13: Should cl4.1 (a) be revised to allow users to "opt in" to receive a receipt?**

The ABA supports ASIC's view that provided the user is required to consider whether to have a receipt the policy objective is satisfied and that the EFT Code should be amended accordingly. As noted in the ABA's comments in response to question 68, excessive prescription in the EFT Code is a disincentive to subscription. The issue of receipts is an example of an area in which prescription could be reduced to encourage greater participation.

A number of ATM deployers already offer the customer the option of proceeding with a transaction without a receipt. There is no evidence to suggest that this option is disadvantageous to customers. In addition to that option, the EFT Code could also allow the issue of an electronic receipt, for example by SMS message, but that should not be mandatory, consistent with a general desire to minimise unnecessary prescription.

The ABA would support a change to the EFT Code that recognises the practice of customer choice whether to receive a receipt rather than mandating the provision

---

<sup>1</sup> Clause 18.4 of CBP will require amendment following the amendments to the Corporations Act 2001 removing certain disclosure requirements relating to basic deposit products and related non-cash payment facilities. The CBP should provide that clause 18 applies to a change of fees and charges in relation to basic deposit products and related non-cash payment facilities.

of a receipt unless the customer opts out. This approach is more attuned to customer service and customer preference.

**Question 14: Should cl4.1 (a) be revised to deal with the problem of ATMs or other machines running out of paper for receipts? If so, how should it be amended?**

The ABA agrees that a more flexible approach is needed in the EFT Code. If the receipt provision is to remain in its current form a "best endeavours" test is not preferred. Rather the ABA believes a "reasonably practicable" test is more relevant.

This approach takes into consideration that some ATMs are located in remoter areas and the contracting of maintenance services for ATMs are performed on a cyclic periodic basis where paper shortages could arise between maintenance periods.

The ABA does not support a requirement to place stickers on ATMs advising of the approach to issuing receipts, including because they could be removed.

A common approach where technical difficulties will prevent the issue of a paper receipt is to advise the customer and to allow the customer to choose whether to proceed. As well as being practical, that approach is more convenient for the customer than denying the customer the opportunity to access funds.

### **Merchant Identification on Transaction Receipts**

**Question 15: Should cl4.1 (b) (v) be changed to allow a receipt for an EFT transaction by voice communication to specify the merchant identification number instead of the name of the merchant to whom the payment was made?**

The ABA agrees with the proposal in paragraph 6.18 of the Consultation Paper for the phrase "or biller identification number" to be included in the relevant EFT Code clause. However, it should not be mandatory for the merchant identification number to be disclosed together with the merchant name.

### **When a Transaction Receipt Should Disclose Remaining Balance.**

**Question 16: Should the EFT Code give more guidance on cl4.1 (a) (vii) regarding balance disclosure on receipts? If so, what guidance should be added?**

There are privacy and security issues involved with disclosure of closing balances on receipts and the ABA recommends that banks should retain the flexibility to decide whether it is appropriate to provide balances in EFT transactions, noting that existing privacy legislation already applies.

## Consistency between Part A and Corporations Act

### **Question 17: Is there duplication or inconsistency between Part A of the EFT Code and requirements of the Corporations Act that should be reviewed? How should any such issues be dealt with?**

The ABA is not aware of any inconsistency between the EFT Code and the law. To the extent there is any inconsistency our view is that the law prevails.

In the case of duplication, there is the question of duplication between the EFT Code and the law and the further question of duplication between the EFT Code and the CBP.

In relation to receipts, the Consultation Paper identifies duplication between the Code and the FSR reporting that the EFT Code goes further than the FSR. The ABA submits that the Corporations Act provisions should apply, as the standard applying to subscribers and non-subscribers would then be consistent. For that reason, it would be possible to remove requirements in relation to receipts from the EFT Code.

The CBP does not make provision for receipts therefore there is no duplication with the EFT Code.

In the case of credit statements of accounts the CBP standard is based on the uniform Consumer Credit Code requirements and this duplicates and extends the EFT Code model considerably.

In the case of periodic statements there is duplication between the FSR and the EFT Code and also duplication between the EFT Code and the CBP. For deposit accounts the CBP is similar to the EFT Code requirement. However the EFT Code is more prescriptive whereas the CBP simply requires "a statement of all transactions". The ABA submits that the multiple overlapping regimes should be simplified. The ABA's view is that where an aspect is regulated by the Corporations Act, it should not be further regulated under the EFT Code or CBP, as overlap provides an opportunity for inconsistency. For example, the Corporations Act (S1017D (7)) allows for periodic statements not to be given where the prescribed information has already been provided to the customer by another means. However, clause 4.2 the EFT Code does not offer that flexibility. To the extent such obligations remain in the EFT Code, equivalent flexibility should be provided.

As an example of where the EFT Code and the Corporations Act differ, clause 4.5 requires a bank to restate access method security guidelines to customers at least annually. This is inconsistent with the Corporations Act and the UCCC. It would be appropriate to require that the information be provided at the time an electronic product is obtained, when requested by the customer, and if the information changes. This is particularly the case in a dynamic environment in which change is likely to occur relatively frequently.

## **Are there aspects of the legal framework that the EFT Code should adopt?**

### **Question 18: Are there aspects of the product disclosure regime under the Corporations Act that should be adopted as part of the regulatory framework under Part A of the EFT Code?**

The significant work undertaken by banks to better inform the community about risks associated with not protecting the security of access codes could be supported if the EFT Code required subscribers to provide information to customers about these significant risks prior to the customer's first use of the access code. Such a provision should recognise that most banks disclose aspects of risk as part of their terms and conditions particular to specific electronic transacting channels and should not require additional disclosure obligations over and above these disclosures. Further disclosures would be onerous and unnecessary.

Subscribers should be free to determine the content and presentation of these disclosures.

## **Obligation to Advise Account Holder of Discrepancies**

### **Question 19: Should cl7 be revised to specifically require subscribing institutions to identify and correct discrepancies between amounts recorded on the user electronic equipment or access method as transferred, and amounts recorded by the institution as received? What are your views on the suggested re-drafting?**

The ABA is happy with the clarification that has been proposed to substitute for "deposit" "...transfer for the credit of an...".

There is a question whether the disparity between the amount recorded as having been credited and the amount received is more or less than the actual amount to which the customer is entitled or is liable. This raises the question whether the account institution for example a bank, is able to debit a customer's account without the authority of the customer. If the proposed sub clause (c) is to be included we suggest that the sub clause be prefaced with the words "with the agreement and cooperation of the account holder".

The ABA does not support any further changes to clause 17, as no market failure has been identified.

## **What is a Complaint?**

### **Question 20: Should the EFT Code include a definition of the terms "complaint" under cl10? If so, should it adopt the definition in ASISO10002-2006? Does the standard sufficiently address uncertainty about what is a complaint for the purposes of the EFT Code? Are there any other steps that might be taken to assist stakeholders to understand what is meant by a complaint under the Code?**

The ABA would like to see the question of what is a complaint resolved in the same way as under the CBP, consistent with a more general harmonisation of

approach between the EFT Code and the CBP. The application of a common standard across the wider industry is desirable.

Under the CBP "complaint" is not a defined term. Instead the CBP uses the expression "dispute". A "dispute" under the CBP

*"Means a complaint by you in relation to a banking service, that has not been immediately resolved when you bring the complaint to our attention."*

To avoid the EFT Code becoming unnecessarily complex and prescriptive we suggest that a commonsense approach is needed to what is essentially an expression of dissatisfaction or grievance of the customer with the account institution. If the expression of dissatisfaction or grievance by the customer is not immediately resolved and the situation continues then it follows that the matter of concern becomes a "dispute".

Also the EFT Code could draw a clear distinction between a "complaint" and an "inquiry" or "query". A "query" can precede a "complaint" about a questioned transaction but the "query" is not necessarily a complaint or something that inevitably leads to a "complaint".

In this and other aspects of the EFT Code the objective should be to try and reduce the terms of the EFT Code to simple statements and ordinary language that is readily understandable.

In relation to ASIC's specific query in section 6.41, the ABA submits that it would not be appropriate to say that a complaint has arisen where the interaction set out has occurred.

### **Standard for Internal Complaint Handling**

#### **Question 21: Should ASISO10002-2006 become the require standard for internal complaint handling under the EFT Code?**

The ABA is not aware if ASIC has declared ASISO10002-2006 to apply to the CBP. Were ASIC to do so then the ISO Standard would apply under the CBP and in that case it would be necessary in the interests of consistency for this to be replicated in the EFT Code.

While a first priority should be harmonisation with the CBP, there is also scope to improve the complaints handling regime under the EFT Code through removing unnecessary duplication with other dispute resolution regimes. The ABA submits that it would be appropriate for the EFT Code to include an exemption to the complaint handling provisions where an equivalent complaint handling regime already exists. For example, the Credit Card Scheme Rules and the BPay Scheme Rules provide for complaints handling procedures, which should be explicitly recognised as an equivalent complaints handling regime under the EFT Code, which should also allow for additional regimes to be classified as such in the future.

## Meaning of “immediately settled” Complaint

**Question 22: Should account institutions be given a brief period within which to investigate a complaint before they must give the complainant written advice on how they investigate and handle complaints (as required under cl10.3)? If so, what is an appropriate period?**

The CBP says “immediately resolved”.

The ABA’s preference is for the question of immediacy to be left to the judgment of the parties thereby avoiding unnecessary complexities and prescription being added to the EFT Code.

However if the EFT Code is to make specific provision for this circumstance the ABA suggests that if a complaint can be resolved within **21 days** the requirements of clause 10.3 need not be followed.

## Time Frames for Resolving Complaints

**Question 23: Should any changes be made to the time frame for resolving complaints under cl10 of the EFT Code?**

The ABA notes that the 21 day period specified in cl 10 can be unworkable where a third party, such as a non-bank ATM deployer, is interposed between the bank and the customer. In those circumstances, a longer time frame would be appropriate.

## Internal Complaints Handling

**Question 24: Do you have information or views about the level of compliance with cl 10?**

The ABA does not have a general view about the level of compliance, but notes potential difficulties in obtaining information from non-subscriber deployers of ATMs in a timely manner.

**Question 25: Has the procedure in cl 10.12 been an effective incentive to compliance? Are further incentives required, and if so what form should they take?**

The ABA considers a “penalties” approach will not necessarily improve the level of compliance. A more constructive approach would be for the EFT Code to require that a subscriber establish an internal compliance committee to which a complaint about an incident of non-compliance with clause 10.12 could be made. The committee would be required to investigate and report to the head of the relevant business unit with any appropriate recommendations for changes to the compliance system. The committee would monitor implementation of any changes it recommends.

## Investigating Complaints and Availability of Record

**Question 26: Should the EFT Code be amended to cover situations when the subscribing institution is unable to, or fails to, give the dispute resolution body a copy of the record within a certain time? If yes, should the Code specify that the dispute resolution body is entitled to resolve a factual issue to which a record relates on the basis of the evidence available to it?**

If the record is unavailable, the dispute resolution body should be required to adjudicate on the basis of available evidence. However, there should be procedural fairness in establishing the availability or otherwise of the record to be produced, taking into account the relevant circumstances, and for adequate notice to be given to the subscriber institution of the consequences if the record is not produced. An invitation should be given to the subscribing institution to provide such other information that it may have that will be taken into account in resolving the factual issue.

The ABA also suggests that the EFT Code refer to "information" rather than "evidence".

## Time Limit on Resolution of Complaints under the EFT Code

**Question 27: Should there be a time after which EFT Code subscribers are no longer required to resolve complaints about EFT transactions on the basis set out in Part A of the Code?**

Taking the example of chargeback rules under credit card schemes, it is common for time limits to apply to consumers seeking to chargeback a disputed transaction. Under the CBP banks are required to provide information to their credit card customers about times for disputing and charging back a questioned transaction.

Determining appropriate time frames involves weighing the necessity of giving the customer sufficient time to notice and report an error against the need to ensure that relevant records, such as merchant receipts, are available to assist in investigations. In addition, for complaints to serve as a valuable tool in fraud detection and prevention, fraudulent activity needs to be identified as quickly as possible.

A statement of account is often the first notice a customer gets that a transaction may be unauthorised or erroneous. A reasonable period of time after issue of the statement of account information should be set for a complaint to be made. Otherwise the account institution may suffer disadvantage due to the customer's delay in making the complaint.

If the time is to be specified, the ABA suggests that the specification of a time needs to take account of credit card scheme rules on time limits for customers to claim a chargeback where a chargeback right exists and allowing sufficient time for a customer to check and verify entries on the periodic statement of account. This issue requires further consideration and it is recommended that a discussion of this issue by ASIC with card schemes, issuers and other stakeholders would be appropriate.

In the case of ATM disputes where the customer claims to have received no cash or less cash than the amount requested the ABA recommends that a customer should complain within one month of the event. The customer is aware immediately of the shortfall and should report the matter quickly. Delays in customers' reporting of these events can impact on a bank's ability to resolve the matter quickly.

### **Section 7 - EFT Code, Part A (Liability; mistaken payments)**

The ABA appreciates the helpful summary analysis in the Consultation Paper on the operation of the liability allocation regime under Part A of the Code.

**Question 28: Should account holders be exposed to any additional liability under cl 5 for unauthorised transaction losses resulting from malicious software attacks on their electronic equipment if their equipment does not meet minimum security requirements? Do the benefits and costs of extending account holder liability justify such an extension of cl 5? What implementation would have to be addressed?**

The ABA supports the continuation of the current approach in Part A of the Code. The ABA does not believe that there is any reason to change the existing provisions regarding liability.

### **Liability for losses resulting from deceptive phishing attacks**

**Question 29: Should an additional example be included in cl 5.6 (e) specifically referring to the situation when an account holder acts with extreme carelessness on responding to a deceptive phishing attack?**

As noted above, the ABA does not believe that there is any reason to change the existing provisions regarding liability.

**Question 30: Apart from this possible clarification, should account holders be exposed to any additional liability under cl 5 for unauthorised transactions losses because of a deception-based phishing attack? Do the benefits and costs of extending account holder liability justify such an extension? What implementation issues would have to be addressed?**

The ABA does not believe that there is any reason to change the existing provisions regarding liability.

### **Code security breaches by user attracting account holder liability (cl 5.5 (a) and 5.6)**

**Question 31: To what extent has the restriction on using a user's name or birth date under cl 5.6 (d) been relied on?**

Although not frequently relied upon by banks it is important that the provision remains in the EFT Code. The bank has no knowledge of the customer's self selected code and would only know of the connection to the customer's name or birth date if the customer told the bank.

There would be merit in the EFT Code recognising that an EFT Code subscriber could obtain a written acknowledgement from a customer that a customer was aware of the risk and the relevant EFT Code provision dealing with this matter.

Apart from any liability issues associated with this provision, it has the benefit of reducing the instances in which the customer selects a predictable PIN, in turn reducing fraud.

**Question 32: Should the restriction on users acting with extreme carelessness in failing to protect the security of all "codes" under cl 5.6 (e) be further elaborated or extended in some way? Should additional examples of extreme carelessness be given?**

The ABA recommends that cl 5.6 (e) remain in its present form and that further examples of extreme carelessness will add complexity and possibly disturb existing interpretations of an expression that has been operating in the Code for over 5 years.

**Question 33: Should the EFT Code specifically address the situation when an unauthorised transaction occurs after a user inadvertently leaves their card in an ATM?**

The ABA submits that the change would be consistent with the "least cost avoider" principle.

**Unreasonable delay in notification (cl 5.5 (b))**

**Question 34: To what extent is unreasonable delay in notification of security breaches by account users currently an issue? Please provide on the frequency and cost of such delays, if possible. (You may wish to provide this information on a confidential basis)**

The ABA believes that this issue needs further consideration. The customer is usually best placed to identify if the security of the customer's transactions has been compromised and that unauthorised transactions have been made. These events are readily identifiable from periodic statements of account that customers receive from their bank.

The ABA does not have information on costs occasioned by delay but as a matter of practice the later an irregularity is reported, the longer it can take to retrieve information and hence delay resolution.

Occasionally, a bank may receive a dispute going back more than seven years where records may be difficult to access. The longer the time that has elapsed since the transaction, the harder it can be to retrieve the information.

**Question 35: Should the circumstances when an account holder is liable on the basis of unreasonably delayed notification under cl 5.5 (b) be extended to encompass unreasonable delay in notifying online security breaches of which the user becomes aware?**

A customer should be timely in reporting a compromise of the security of the on-line equipment, and in acting on advice from a bank that a security breach has been detected. Whether this should necessarily result in additional liability is a matter for discussion between ASIC and relevant stakeholders.

There is an important distinction made in the Consultation Paper between a compromise of the access method and of the on-line electronic equipment. It is true that with internet-based debit and credit card transactions the customer

need enter only the card number and possibly a further identifying factor. The real risk is the compromise of the access to the electronic equipment.

**Question 36: Should the standard of 'unreasonably delaying notification' under cl 5.5 (b) be replaced by a specific time after which the account holder is liable? What would be an appropriate time, if such a change were introduced?**

The existing provision is able to be applied to a variety of circumstances that works fairly for both customer and account institution according to the circumstances. An arbitrary time limit would not operate in the same way.

#### **No fault liability limit (cl 5.5 (c))**

**Question 37: To what extent do subscribing institutions currently use the other 'no fault' liability provision in cl 5.5 (c)?**

ABA members' use of this provision varies. Where it is used, it is an effective and efficient means of resolving many cases.

**Question 38: Is there a case for increasing the current 'no fault' amount of \$150? If so, on what basis and what should the new amount be?**

The ABA supports retaining the current 'no fault' level.

#### **Liability allocation and 'book-up'**

**Question 39: Should subscribers prohibit in their merchant agreements the practice of taking customers' PINS or other access codes as part of a 'book-up' arrangement? If so, should this be subject to any exceptions; and if it should, what should those exceptions be?**

ABA's members have developed individual approaches to this question.

The ABA and member banks have supported the Government's efforts to restrict poor book up practices, and the ABA has engaged extensively with ASIC in relation to this matter.

#### **Liability in cases of system or equipment malfunction (cl 6)**

**Question 40: Should cl 6 be reformulated to clarify that the subscribing institution is liable for any failure resulting from equipment malfunction when they have agreed to accept instructions through that equipment?**

If the RBA's proposed direct charging model for ATMs is introduced a foreign ATM owner will be able to charge a user a fee for service directly (as opposed to the user being charged a foreign ATM fee by their issuing bank). It follows that liability for equipment malfunction should reside with the owner, not the issuer. Further issues in relation to ATM reform are discussed in response to question 73.

## Mistaken payments

**Question 41: To what extent, and how, should the Code address the issue of mistaken payments? Discuss the usefulness, practicality and cost of implementing some or all of the measures outlined, as well as any other measures you consider appropriate.**

The ABA appreciates the constructive thought that ASIC has put into the table of possible solutions to this issue that appears as Table 10 in the Consultation Paper.

Some of the suggestions could involve substantial system changes and cost for banks and the preference is to avoid this and look for an effective but simpler solution.

To illustrate the dimension of direct entry transactions, in December 2006 there were over 119,000,000 transactions over direct entry for a value in excess of \$780,000,000,000. Daily averages are 6,200,000 transactions for a value of \$40,000,000,000.

The ABA recognises the importance of a means of reducing mistaken payments, and for addressing any mistaken payments. The ABA notes that APCA intends to establish a working group to formulate an appropriate policy for addressing mistaken payments. The ABA submits that it would be appropriate for the EFT Code to defer to APCA's review in dealing with mistaken payments.

However, the ABA would support the EFT Code including provisions relating to appropriate disclosures in relation to payments, which the ABA submits are:

- that the intended beneficiary's account name will not be used to process the transaction;
- that the customer should ensure that the BSB and account number are correct; and
- that if either the BSB or the account number is incorrect, the customer may not be able to recover the payment if it is received by a person other than the intended beneficiary.

## Section 8 - EFT Code, Part B (Scope and interpretation)

**Question 42: Should the scope of Part B of the EFT Code continue to be defined by reference to the concepts of 'stored value facilities' and 'stored value transactions' as at present; or should a different approach be taken? What issues are raised by possible alternative approaches?**

Care should be taken to ensure that any amendments made to Part B do not operate as a barrier to membership to the EFT Code. Current membership in relation to Part B is low.

Regarding the first part of this question, the ABA believes a clear definition of what constitutes a 'stored value facility' and a 'stored value transaction' should be developed, especially with regard to the distinction made in section 8.13 of the Consultation Paper. That is, with regard to whether payment is authorised remotely or if microchip technology is used. The use of a PIN in the transaction

authorisation should also be addressed in Part B. The definition should be consistent with other legislation regulating stored value products, including the Anti-Money Laundering and Counter-Terrorism Financing Act.

Regarding the second part of the question, in order to better form alternative approaches, a clearer view needs to be gained on what new types of products are being considered for release, and what kinds of products would best suit the Australian electronic commerce network.

One view is that SVF facilities are a legacy of the independent and disconnected networks being used in overseas markets, making the use of SVFs necessary, whereas in Australia there is a more connected and standardised network that facilitates the use of many cards in many locations. The relevance of a large part of Part B of the Code to the Australian market may need to be revisited.

In the absence of this information the preferred approach is not to change the scope of Part B until this information is available as the possible issues have yet to emerge sufficiently clearly to warrant a response in the EFT Code and to proceed without further information may lead to premature amendment.

Another consideration is that SVFs are typically low value/'at cost' facilities such as store gift cards, tertiary student facilities and transport cards. Given the low margins involved, overly prescriptive obligations may inhibit subscription to the EFT Code due to compliance costs.

### **Part B scope and interpretation: other aspects**

**Question 43: Assuming the scope of Part B of the EFT code continues to be defined in terms of the concepts of "stored value facilities", what changes, if any, should be made to the definitions and other provisions of cl 11?**

Another factor to consider is whether these SVFs are used in conjunction with a signature or with a PIN. Depending on the transaction authorisation and verification method employed, the facility may either not be covered by the EFT Code at all, or covered only under Part A.

The ABA repeats its view that a scoping exercise should be undertaken in the Australian context before consideration is given to changing these provisions of Part B.

### **Section 9 - EFT Code, Part B (Requirements)**

**Question 44: Should any changes or additions be made to cl 14?**

In general no, but a clearer indication of whether loyalty program points are deemed as 'value' should be put forward for consideration.

**Question 45: Should operators of facilities regulated under Part B be required to make a transaction history for the facility available on request for a specified period?**

A transaction history will generally be kept by the bank for its own accounting records but there are privacy issues that arise when considering making this transaction history available to end users. Card details may be linked to the

original purchaser but it is generally recognised that the end user may be a different person to the one who purchased the card. Privacy issues may arise in making transaction histories available when it is unclear as to who is making the enquiry and who is actually using the facility.

### **Consistency between Part B and Corporations Act (cl12-14)**

**Question 46: Are any aspects of Part B of the EFT Code incompatible with the requirements of the Corporations Act? How should any incompatibility be addressed?**

There are some requirements in the EFT Code that, while not incompatible with the Corporations Act, do cover different operational aspects of the same products that are covered by the Ch 7 (FSR) requirements of the Corporations Act. An example of this is where the EFT code has specific requirements for receipts issued following transactions on certain products, whereas Ch 7 of the Corporations Act has specific requirements for providing information on certain, and in some cases, the same products.

It is generally accepted that the Corporations Act applies over the EFT Code in any case of incompatibility. Any other ambiguities can be addressed by ASIC as they administer both sets of regulation and can address these inconsistencies by industry discussion and policy statement issue.

### **Right to exchange/replace stored value (cl 15)**

**Question 47: Should the rights to exchange stored value under cl 15 be narrowed?**

No.

**Question 48: Should the EFT Code include a requirement that all prepaid facilities regulated by Part B must have a minimum use time (i.e. the time before value expires) of at least 12 months?**

Yes.

**Question 49: Should the EFT Code include a requirement that the use period or date be displayed on any physical device (such as a card) used to make payments in connection with a prepaid facility?**

Yes. This is required for practical purposes at the point of sale as the merchant should be able to view if the card is still valid before they attempt the transaction.

### **Right to refund of lost or stolen stored value (cl 16)**

**Question 50: Should the right to a refund of lost or stolen stored value under cl 16 only be mandated for facilities that allow more than a certain amount of value to be prepaid? If so, what should the minimum amount be?**

The ABA understands that many stored value/prepaid card issuers will not refund for lost or stolen cards and advise customers to treat them as if they were cash. The ABA recommends that this issue should be further discussed by ASIC with users.

**Question 51: Should there be a requirement that regulated facilities over a certain value include a mechanism (such as PIN security) that allows users to control access to the available value on the facility?**

The ABA does not support this proposal under the current definition of stored value facilities, because:

- additional significant costs are involved;
- another layer of IT infrastructure would be required;
- as the end user is not always the purchaser it is difficult to establish ownership of the card for PIN management, administration or resetting;
- other security measures in place enable users to report missing cards, and there is an ability to immediately block their use.

In addition, given that there are a number of providers of stored value cards that are not subscribers to the EFT Code, the competitive position of providers could be compromised by the imposition of this requirement.

**Right to unilaterally vary terms and conditions**

**Question 52: Should the use of unilateral variation clauses in the terms and conditions for facilities regulated under Part B be restricted?**

No.

**Complaint investigation/dispute resolution (cl 19)**

**Question 53: Should the complaint investigation and dispute resolution regime under cl 10 of the EFT Code apply without limitation to Part B facilities and transactions under cl 19?**

No - we recommend it should apply with limitations. We recommend that cl 19 be amended to read "where we know the identity and contact details of the user / purchaser", as in cl 13.

**Payment finality**

**Question 54: Should Part B of the EFT Code address the issue of payment finality?**

Yes. We recommend the code give a clearer indication of each party's responsibilities (that is the card user, the merchant and the issuer) in the event of a dispute after a transaction has been processed. In doing so, the EFT Code should be consistent with general banking law principle.

## Section 10 - EFT Code, Part C (Privacy and electronic communications)

### Privacy obligations (cl 21)

#### **Question 55: Should the provisions about privacy under cl 21 be modified and/or extended to cover other areas or issues?**

A uniform approach is required across all organisations with regard to providing information on mistaken EFT payments (i.e. where funds are credited to the wrong account). This is discussed further above in response to question 41.

Should the review to be undertaken by APCA identify privacy related issues; this question should be re-examined.

#### **Question 56: Should the status of the cl 21.2 guidelines be changed to make these provisions contractually binding requirements?**

No. As long as privacy principles are met, the code should not be prescriptive in this area.

#### **Question 57: Should the EFT Code require that transaction receipts include only a truncated version of the account number?**

The ABA submits that it is appropriate for financial institutions to have the discretion to decide whether to truncate the account number, having regard to the relevant circumstances including the security of the channel through which the receipt is provided.

#### **Question 58: Should the EFT Code require that transaction receipts not include the expiry date and/or other information that is not required for transaction confirmation purposes?**

The ABA submits that it is appropriate for financial institutions to have the discretion as to whether to include the expiry date, noting that to prohibit the inclusion of the date could have adverse consequences for fallback processing arrangements, as the date may be required to complete a transaction in instances of system failure.

#### **Question 59: What would be the cost of implementing the suggested changes? Are there any implementation issues that should be considered? What would be an appropriate implementation time frame?**

As noted above, the ABA does not support mandating the suggested changes. The response below sets out the ABA's position should ASIC nonetheless decide to implement them.

Some systems will already allow for the changes. However, some systems will not. In order to reduce systems costs, the ABA would request that ASIC consult with industry to determine appropriate transitional arrangements. One suggestion is that, should ASIC ultimately mandate truncation or prohibit the inclusion of expiry dates on receipts, where current systems do not allow for the changes, the requirement should be that any new systems must be capable of compliance.

**Question 60: Should cl 22.1(b)(ii) be deleted or amended in some way?**

Yes – amendment to this clause is recommended as it was written about five years ago when the impact of these services was not properly known.

In addition to the clear security implications, there should be an onus on users who elect to receive information electronically that they must advise their account institution of any changes to their e-mail address so that a current address is held at all times.

More generally in relation to clause 22, simplification is required.

The last paragraph of clause 22.1 means that subscribers cannot accept requests from customers to receive information electronically without first providing the customer with an 'explanation of the implications of making such an election'. This can convey the impression to customers that banks think they are asking for something complex and they are not in a position to make that choice. Electronic communication is now well entrenched in the community and subscribers should be able to act on customer requests for electronic delivery without detailed prescription of what a bank needs to tell the customer.

Clause 22.1(b) (i) requires subscribers to tell the customer when an electronic statement or message has been made available for them. There are a number of issues here.

First, advice that a communication (such as a statement) is available for retrieval should not be required when the information is made available as an attachment or at times previously made known to and agreed by the customer. Many customers access their account information on a daily or near-daily basis. They are constantly receiving updated information, so the concept of a "statement cycle" is not really relevant to them. Any customer with electronic access can view information that would appear on a statement at any time. The separate advice should only be required when information becomes available for retrieval on an irregular basis – e.g., advice of a change to terms and conditions.

Secondly, the words "and the nature of the information" in Clause 22.1(a) (i) should be removed. Emails and SMS are not secure media and customer privacy could be breached if the notification is intercepted or seen by a third party.

Further, ASIC has sought comment on whether Clause 22 inhibits introduction of products which allow only the electronic delivery of information. We believe that this is in fact the case. Under Clause 22.1, customers need to make a positive election to receive electronic communications. This means that paper communications must be provided if customers do not make such an election. That in turn requires the set up of physical mail-out facilities, plus testing of mail-outs, which both increase the cost and reduce the speed to market of new products. This may potentially inhibit the trial of innovative products in an electronic environment and limit choice. In addition, under Clause 22.1, customers are able to terminate the agreement to receive information electronically. With electronic delivery only products, pricing is based on the economies of electronic delivery. The practical effect is that if a customer terminates their agreement, the provider will need to send paper statements and physical mail-out facilities are required. This adds to the cost of providing the

product. Alternatively, the customer can opt-out by closing the account and can move to another (potentially more expensive) product.

Consequently, the Code requirement that customers must make a "specific positive election" to receive electronic communications (after being advised of the ramifications of the decision) and have a permanent right of opt-out, are inappropriate. Products and services built around electronic delivery provide efficiency and convenience benefits to both providers and customers. Whilst the *Electronic Transactions Act* ("ETA") requires that persons must consent to receiving communications in electronic form, ETA does not mandate the requirements that are imposed by Clause 22. (ETA in fact goes as far as providing that inferred consent will be sufficient.)

Clause 22.3 imposes an obligation to provide a paper copy of information provided electronically when requested within 6 months of the electronic communication. This is unnecessary and should be removed. Normal business practice is to be able to provide on request a copy of prior communication to customers and the Code does not need to be prescriptive in this area.

**Question 61: Should cl 22.2(b) (ii) be deleted or amended in some way?**

Yes, it should be deleted.

**Question 62: Should changes be made to the EFT Code to address issues associated with products that only allow electronic communication of account information? If so, what changes should be made?**

Yes, as these products play a significant role. We suggest that the restriction for electronic communications be disclosed prior to acquiring the relevant product.

Users should also be given various options for receipt of account information (including the Security Advice information stated in clause 4.5 of the existing EFT Code). The ABA does not suggest that the EFT Code should prescribe those options. However, the list below has been provided by one bank to assist ASIC in its thinking on what the options could include:

- (1) Receipt of email to their nominated email address advising that a statement is now available for viewing (note – a URL to the account institution address should not be supplied in the e-mail because of potential security risks).
- (2) Authorisation to allow the account institution to advise the user of the availability of their statement for viewing, via a Message Centre.
- (3) No e-mail or Message Centre advice to be issued if the customer elects not to receive such a notification. The statement information is available at any time and members have suggested that many customers request that no e-mail notification be sent.

**Question 63: Should the EFT Code address the situation when an account institution receives a mail delivery failure message after sending a communication mandated under cl 22? If so, what approach should be adopted? How is this situation currently handled?**

Email should be treated in an analogous manner to hard copy mail. Financial institutions already have procedures in place to cover circumstances where a letter is returned from a customer's last known postal address, and analogous principles can be adopted in relation to email addresses. These processes differ between institutions, and subscribers should be free to determine what is appropriate, depending on the individual circumstances. Customers should keep their email address up-to-date just as they should their postal address.

**Section 11 - EFT Code, Part C (Administration and review)**

**Question 64: Should ASIC continue to be primarily responsible for administering the EFT Code? Are there other arrangements that should be considered?**

Yes, the ABA considers that ASIC is the most appropriate entity for administering the EFT Code. ASIC is a key regulator who enforces and regulates financial services laws and companies who deal and advise in deposit taking and credit. ASIC plays a central role in promoting consumer confidence and protecting consumers.

**Modifying the EFT Code**

**Question 65: Should the EFT Code allow its requirements to be modified in certain circumstances? If so, what modification powers should be included and how should they be administered?**

The ABA considers that the appropriate means by which the EFT Code should be changed is the current review process. Given the importance of the EFT Code to industry and consumers, and its role as a voluntary code of conduct, it is crucial that appropriate consultation be held before changes are made. Consultation ensures that amendments are operationally sound, and enhances industry's confidence in the EFT Code, which in turn makes membership more attractive.

**Monitoring Compliance**

**Question 66: How should compliance be monitored? What alternatives to the current self-reporting survey should be considered?**

The ABA considers that the current self monitoring approach should be continued. However, the ABA recommends some changes to the current survey process. The ABA recommends the establishment of an industry working group to consult with ASIC to improve the current process, both in terms of its workability for industry and usefulness for ASIC. General comments that could form the beginning of working group consultations are set out below.

The previous survey was made up of two main sections: -

Part A - Code Conduct Checklist;

Part B - Complaint Statistics.

We consider that ASIC should simplify the self reporting survey process contained in Part A of the previous survey checklist. The previous checklist was based directly on the provisions of the EFT Code. It was a very detailed and granular approach, which focussed on every provision of the Code including those that have minimal risk impact. We consider that this monitoring technique has not been very efficient as it was quite a labour intensive process, with a number of businesses involved in its completion. For example, one bank estimates that for the June 2005 EFT survey 10 staff spent 360 person hours completing it.

We recommend that future monitoring should be based on a 'risk approach' i.e. the provisions or activities that have been assessed as 'high risks' to both the consumer and subscribing institutions. This may be arranged thematically with one question/section covering several provisions of the Code, in a similar manner to the Code of Banking Practice Compliance Statement.

In relation to Part B, complaint statistics, we do not consider that the monitoring should collect information on EFT complaint or transaction statistics. Many EFT subscribers experience problems associated with data collection and quality. There has been an ongoing mismatch between the complaint data requested by ASIC in the annual surveys, and the information provided by subscribers. This has compromised the integrity of data and the publishing of reports.

The banks are generally unable to provide all EFT transaction and complaint data as requested by ASIC due to system constraints. Reporting all EFT complaints comprehensively is difficult as we have a number of specialist business units resolving them. These units use different system applications and complaint categories for recording EFT complaints.

The EFT monitoring report published by ASIC as a result of the monitoring survey should be available in a timely manner. This will allow institutions to use the report to benchmark themselves against the industry. We also would recommend that ASIC engages EFT subscribers about emerging EFT issues or monitoring other aspects of the EFT Code on an ongoing basis.

## **Reviewing the EFT Code**

### **Question 67: How should the EFT Code be reviewed? What alternatives to the current approach should be considered?**

Ideally, there should be flexibility in terms of the frequency of reviews, given the speed with which technological developments are occurring in this area.

If a time limit needs to be specified, the ABA submits that a five year review process is appropriate.