ASIC

Australian Securities & Investments Commission

CONSULTATION PAPER 78

Reviewing the EFT Code

January 2007

What this paper is about

1 This consultation paper initiates the public phase of a review of the Electronic Funds Transfer Code of Conduct (the EFT Code).[1]

2 The EFT Code is a voluntary industry code of practice covering all forms of consumer electronic payments transactions. It has been operating (initially as a set of recommended procedures) since 1986.

3 ASIC administers the EFT Code and is required to periodically review it and associated administrative arrangements, in consultation with other stakeholders: see cl 24.1(a).[2] The Code was last reviewed in 1999–2001.

4 In this paper, we:

(a) provide background information about the EFT Code;

(b) survey changes in the external environment that affect the EFT Code;

(c) raise issues for discussion as identified to date by external stakeholders and ASIC; and

(d) in some areas, outline possible options for revising the EFT Code.

This paper does not represent ASIC policy or the position or views of the Australian Government, or any other government or industry body. No decisions for regulatory change have been made.

Making a submission

5 You are invited to write a submission about some or all of the issues in this paper, and to raise other issues that you see as pertinent to the EFT Code and its regulatory role.

6 Proposed changes to the EFT Code that are likely to have a significant impact on business or individuals, or that are likely to restrict competition, will be subject to regulatory impact and cost to business assessment processes administered by the Office of Best Practice Regulation (OBPR).[3]

---

[1] Copies of the EFT Code and this paper are available on the review website at www.asic.gov.au/eftreview.

[2] All references are to the EFT Code unless otherwise specified. For more on ASIC's role in administering the EFT Code see Section 11 of this paper.

[3] The OBPR's recently revised guidelines give information regarding when a Regulatory Impact Statement is required and when the Government's Business Cost Calculator should be used to assess compliance costs: see http://www.obpr.gov.au.

7 We ask you to consider these requirements when developing your submission. In particular, we ask that you provide information about the benefits and costs of significant proposals for changing the EFT Code, compared with any other feasible options (including no change). If possible, please try to quantify the benefits and costs to which you refer, or suggest how this might be done.

8 You can lodge your submission electronically or by post. We prefer that submissions be lodged electronically if possible.

9 Please indicate if all, or a part of, your submission should be treated confidentially. We will not treat your submission as confidential unless you specifically request that we do so. We will not treat an automatic email confidentiality notice as a specific request to treat a submission as confidential.

Your comments

Comments are due by Friday 13 April 2007 and should be sent to:

eftreview@asic.gov.au

or

Michael Funston
EFT Code of Conduct Review
Australian Securities and Investments Commission
GPO Box 9827, Sydney NSW 2001

Review contact officer

Michael Funston, Consumer Protection Directorate, ASIC.
Phone: 02 9911 2081

What happens next

10 A working group of stakeholder representatives, to be appointed, will consider submissions received and redraft the EFT Code. The working group, chaired by ASIC, will include representatives of relevant industry, consumer, dispute resolution scheme and government stakeholders, as well as experts in the electronic payments area. There will be a further process of public consultation on the revised draft.

11 Depending on the timing of the next review of the Code of Banking Practice, which is expected to start in 2007, we may try to coordinate the later stages of the EFT Code review with that review, to ensure consistency between the regimes.

Contents

Executive summary

Overview of the EFT Code

The EFT Code is a voluntary industry code of practice covering all forms of consumer electronic payments transactions. It provides consumer protection in areas including:

(a) disclosure of terms and conditions;

(b) receipt requirements;

(c) provision of statements;

(e) liability allocation when there is a dispute about an unauthorised transaction; and

(f) dispute resolution.

All retail banks, building societies and credit unions offering electronic banking facilities subscribe to the Code, as do a small number of other organisations.

How the EFT Code is structured

The EFT Code is divided into parts and establishes two regulatory regimes:

(a) Part A sets out 'rules and procedures to govern the relationship between users and account institutions in electronic funds transfers involving electronic access to accounts' including all consumer EFTPOS, ATM and internet and telephone banking transactions.

(b) Part B sets out 'rules for consumer stored value facilities and stored value transactions'.

(c) Part C covers common areas of regulation for both regimes (such as privacy and electronic communication) and the Code's administration.

The external environment

Since the EFT Code was last reviewed in 1999–2001, the external environment in which the Code operates has changed: see Table 1. Some of these changes have prompted issues addressed in this paper.

Table 1: Environmental factors affecting the EFT Code

Marketplace developments	• Consumers' use of electronic payment channels (EFTPOS, ATM, phone, internet) has continued to grow strongly since the last review. Growth in the use of the internet has been particularly notable. • Card-based payments currently account for over half non-cash payments made in Australia, with an almost identical number of credit and debit card transactions. • There has been very considerable growth in the use of both direct debit and direct credit by consumers. • There has been rapid growth in the use of online electronic bill payment services, which utilise the direct credit system. • Credit cards issued by financial services businesses remain the dominant payment method/product used for making online payments, with use of the direct credit system growing. • A range of entities apart from financial institutions issue limited use or closed system electronic payment facilities (e.g. electronic gift cards, e-tags).
Growth in online fraud	• While the level of internet banking fraud has grown, it remains relatively contained to date compared to other forms of fraud (such as cheque fraud and credit card fraud). • Many financial institutions are looking at how user authentication can be enhanced as part of their broader anti-fraud strategy. • Some Australian institutions have taken steps towards implementing two-factor authentication of consumer users. • Other methods used to minimise fraud include encrypting information, warning consumers of risks, monitoring activity, and imposing daily transaction limits. • Despite having concerns about online fraud, most people making transactions online appear not to take adequate steps to secure their equipment against malicious code attacks by fraudsters.
Regulatory developments	• Chapter 7 of the Corporations Act establishes broadly uniform regulation of most financial services and financial products. • The Code of Banking Practice sets out the banking industry's key commitments and obligations to customers on standards of practice, disclosure and principles of conduct for their banking services.

Key issues

Table 2 summarises some of the significant policy issues raised in this paper. For a guide to more specific and/or technical issues, see the table of contents and consolidated list of questions in Appendix B.

Table 2: Significant policy issues in this review

Small business	Should the EFT Code cover small business account holders/ transactions? **See Section 5**
Liability	Should the regime for allocating liability in Part A address the growth in online fraud directed at end users and their equipment? If so, how should this be done? **See Section 7**
Mistaken payments	Should the EFT Code address mistaken payments' issues? **See Section 7**
Scope of Part B	Should the scope of Part B be redefined in a broader, more technologically-neutral way? **See Section 8**
Stored value products	Should the rights to exchange and refund stored value under Part B be altered? **See Section 9**
Transaction receipts	Should transaction receipts be required to include only a truncated version of the account number? **See Section 10**
Monitoring compliance	Should the process for monitoring compliance with the Code be changed? **See Section 11**
Membership	How might membership of the EFT Code be broadened? **See Section 12**

Section 1: About the EFT Code

Table 3: Summary of the EFT Code

Description/transactions regulated	Specific obligations
Part A governs funds transfers involving electronic access to accounts maintained with subscribing account institutions including, but not limited to, traditional financial institutions. This includes: • ATM and EFTPOS transactions; • credit and debit card transactions (other than when comparison of the user's manual signature with a written specimen signature is the principal intended means of authenticating user authorisation);[4] • telephone and online banking transactions (including those made using 'pay anyone' facilities); • telephone and online bill payment transactions; and • other remote access, account-based EFT transactions.	• Requirements about the availability and disclosure of terms and conditions (cl 2) • Notification requirements when changing terms and conditions (cl 3) • Requirements about the provision and content of receipts and account statements (cl 4) • A detailed regime covering the allocation of liability for unauthorised transactions (cl 5), and in cases of system or equipment malfunction (cl 6) • Deposits to accounts by funds transfers (cl 7) • Subscriber responsibilities within payment system network arrangements (cl 8) • Audit trail requirements (cl 9) • Complaint investigation and resolution procedures (cl 10)
Part B was inserted after the last review and applies to stored value facilities and transactions as defined. This includes transactions involving: • stored value cards; and • digital cash products.	• Disclosure and changing of terms and conditions (cl 12 and 13) • Records of available balance (cl 14) • Rights to exchange stored value (cl 15) • Refund of lost or stolen stored value (cl 16) • Liability for system or equipment malfunction (cl 17) • Stored value operator's obligations (cl 18) • Complaint investigation and resolution (cl 19) • No unauthorised transaction liability regime
Part C covers common areas of regulation and applies to all transactions and facilities regulated under the EFT Code.	• Privacy (cl 21) • Electronics communications (cl 22) • Code administration and review (cl 23 and 24)

[4] Clause.1.5(c). Manual signature authorisation is not an 'access method' for the purposes of an 'EFT transaction' under cl 1.1 of Part A. The EFT Code has never covered payment instructions which are authorised by manual signature, and for which liability allocation is regulated under the common law. See also Endnote 4 to the EFT Code.

Brief history

1.1 There has been a regime for EFT transactions since 1986 when Federal and State Consumer Affairs Ministers endorsed a voluntary code known as the *Recommended Procedures to Govern the Relationship between the Users and Providers of EFT Systems*.

1.2 Development of the EFT Code was initially driven by community and government concern about the use of one-sided terms and conditions in allocating liability between the account holder and institution in the event of loss or theft of the account holder's transaction card or PIN. Although voluntary in character, the EFT Code was developed against a background of significant political pressure on financial institutions to subscribe to it or risk the possibility of legislative intervention.

1.3 The *Recommended Procedures* were amended and relaunched as the EFT Code of Conduct in 1989. A third iteration was finalised in 1998 (with final implementation in April 1999) following a review conducted by the ACCC and Commonwealth Treasury.

1.4 As part of the implementation of the Financial System (or 'Wallis') Inquiry recommendations,[5] ASIC became responsible for administering the EFT Code on 1 July 1998.

1999–2001 review

1.5 The EFT Code was most recently reviewed in 1999–2001.[6] As a result of that review, its coverage was considerably expanded. In particular, a broad technology-neutral definition of 'EFT transactions' (the core definition of Part A) replaced the preceding definition, which had limited regulated transactions to electronic transactions effected by the combined use of an EFT card and PIN. The Code was extended to include the range of types of transaction referred to above.

1.6 As noted, a separate regulatory regime (Part B of the current Code) was introduced to cover 'stored value facilities and transactions' as defined. This was intended as a 'lighter touch' regime for regulating newly emerging smart card and 'electronic money' facilities, which have some unique consumer issues associated with them.

1.7 Other significant changes as a result of the review included:

---

[5] For more information about the Financial System Inquiry, see http://www.treasury.gov.au/content/financial_services.asp?ContentID=328&titl=Financial%20Services.

[6] More information about this review and copies of the 1999 -2001 review consultation documents follow links from review website at www.asic.gov.au/eftreview.

(a) further refinement of the unauthorised transaction liability allocation regime (cl 5)—in particular, the revised Code clarifies that the burden of proving fraud or breach of security requirements by the account user lies with the account institution (except in the limited circumstances when liability is allocated on a no-fault basis);[7]

(b) incorporation of the National Privacy Principles into the EFT Code;[8] and

(c) a regime facilitating the provision of information mandated under the EFT Code electronically, subject to the user's agreement and other protections.[9]

Who subscribes to the EFT Code

1.8 The EFT Code only applies to institutions that subscribe to it (subscribers).[10] All banks, credit unions and building societies offering electronic banking services to retail customers subscribe to the EFT Code. The only other entities that currently subscribe are American Express International, Australian Guarantee Corporation, First Data Resources Australia, GE Capital Finance Australia, Money Switch Limited, and the Territory Insurance Office.[11]

1.9 Issuers of payment facilities outside the financial services sector, including entities in the transit, toll-road, telecommunications and retail sectors, have not subscribed to the EFT Code to date, nor have most finance companies. The fact that these providers have not subscribed to the EFT Code is an issue to consider as part of this review: see Section 12.

[7] This clause is discussed in Section 7.
[8] The privacy requirements and guidelines under the EFT Code are discussed in Section 10.
[9] Discussed in Section 10.
[10] Subscribers agree to reflect the EFT Code's requirements in the terms and conditions for their regulated products. Terms and conditions must also include a warranty that the requirements of the EFT Code will be complied with: see cl 2.1 and 12.1.
[11] A list of subscribing entities follow links from review website at www.asic.gov.au/eftreview

Section 2: Marketplace developments

This section summarises some major developments in the retail electronic payments marketplace since the last review.[12] Possible implications of some of these developments for the structure and content of the EFT Code are considered in later sections.

Mainstream banking and payments

Use of electronic channels

2.1 Consumers' use of electronic payment channels (EFTPOS, ATM, phone, internet) has continued to grow strongly since the last review.

2.2 Particularly notable has been the growth in the use of the internet. From being in their infancy at the time of the last review, online banking, bill payment and general e-commerce activities have become part of the regular activities of a significant portion of the online population[13] (which now includes a majority of Australians).[14]

Card payments

2.3 Card-based payments currently account for over half non-cash payments made in Australia, with an almost identical number of credit and debit card transactions.[15] There has been steady growth in the use of EFTPOS cards issued by financial institutions since the last review.

2.4 The great majority of adult Australians have at least one debit card[16] and most use their cards regularly to access cash from ATMs and

---

[12] For a detailed overview of trends in the Australian payments system, see the Reserve Bank's Payments System Board (PSB) Annual Report 2006 (upon which this summary draws substantially). Available at: http://www.rba.gov.au/PublicationsAndResearch/PSBAnnualReports/index.html.

[13] According to the *ANZ Adult Financial Literacy Survey 2005* (ANZ survey) usage of internet banking rose from 28% in 2002 to 40% in 2005, while use of BPAY increased from 50% to 60% over the same period. BPAY growth is discussed further below. The ANZ survey and summary is available at: http://www.anz.com/aus/aboutanz/Community/Programs/FinSurvey2005.asp.

[14] Over 60% of Australian households are connected to the internet and in excess of 10 million Australians actively use the internet on a monthly basis, according to 2005 data published by the Department of Communications, Information Technology and the Arts. There were almost 5.1 million household internet subscribers in June 2006 (ABS Report 8153.0–Internet Activity, Australian, June 2006). According to recent Roy Morgan Research almost 80% of the population over 14 years had ever accessed the internet between April 2005 and March 2006.

[15] PSB Annual Report 2006, at p. 3.

[16] PSB Annual Report 2006, at p. 7 refers to consumer surveys showing that around 91% of adults report they have a debit card (55% for credit or charge card).

to make purchases (and obtain cash) via the EFTPOS system.[17] There has been very substantial growth in the number of ATMs and EFTPOS terminals, as well as in the number and value of transactions undertaken using them.[18] A further development since the late 1990s has been the emergence of independent deployers of ATM machines, which now own around 45% of Australia's ATMs.[19]

2.5 While EFTPOS cards retain a dominant position in the debit card market, there has been considerable growth in Visa debit in recent years. More recently, Mastercard also introduced a branded debit card, and this is currently being widely promoted. Unlike traditional EFTPOS cards, debit cards issued under international schemes allow card-not-present transactions by phone and over the internet.

2.6 Internationally, 'online EFTPOS' or 'online debit' services have been introduced in a number of countries, allowing consumers shopping online to choose a payment option that automatically links details of the transaction to their internet banking facility.[20] Currently, however, there is no widely available facility of this kind in Australia.

2.7 Between 1998 and 2000, credit and charge card transactions were growing at an annual rate of around 30%, much higher than for debit cards.[21] This growth was driven to a significant extent by loyalty programs. More recently, the rate of growth in credit card transactions has slowed considerably, and is now lower than the rate for debit cards.[22]

2.8 This is partly attributed to developments in the pricing of credit cards, as well as to the fact that many financial institutions are now offering unlimited transactions for a monthly fee on their transaction accounts.[23] The average value of credit card transactions is more than double the average value of debit card transactions.[24]

---

[17] According to the ANZ survey, 92% of adults know how to use and 78% use ATMs; 90% know how to use and 74% use EFTPOS.

[18] There were over 518,000 EFTPOS terminals in Australian in June 2005 (up from around 334,000 in June 2000), proportionally one of the highest rates of penetration in the world. Over the same period the number of ATM terminals more than doubled: RBA statistical charts (CO7 Points of Access to the Australian Payments System).

[19] PSB Annual Report 2006, at p. 9.

[20] Discussed in PSB Annual Report 2006, at p. 22.

[21] PSB Annual Report 2006, at pp. 4–5.

[22] See footnote above.

[23] PSB Annual Report 2006, at p. 5.

[24] PSB Annual Report 2006, at p. 6.

Direct entry payments[25]

2.9 There has also been very considerable growth in the use of both direct debit and direct credit by consumers.[26] The number of direct debits per head has doubled in the last five years—from around 11 per head per annum in 2000 to around 22 per head per annum in 2005. There are now as many direct debit transactions each year as cheque transactions.[27] Consumers report a marked increase in familiarity with and use of direct debit.[28]

2.10 Businesses and governments have used the direct credit system for many years for making salary, dividend and social security payments. In recent years, consumer utilisation of direct credit has also increased markedly, a development closely linked to use of the internet as a transaction channel (noted above). In particular, internet banking facilities generally now have 'pay anyone' functionality and consumers are effectively able to make payments to anyone with a bank account using this facility.

Electronic bill payments

2.11 In addition, there has been rapid growth in the use of online electronic bill payment services, which utilise the direct credit system. Expansion of the BPAY scheme has been particularly notable, with around 14 million bills worth $9 billion paid each month using BPAY, three-quarters of them initiated online.[29] The total value of BPAY payments each month now exceeds the total value of EFTPOS transactions per month.[30]

Methods of transacting online

2.12 Credit cards issued by financial services businesses remain the dominant payment method/product used for making online payments, with use of the direct credit system growing. We understand that around 11% of credit and charge card transactions are now undertaken using the internet, a figure that has increased strongly over recent years.

---

[25] These include direct credit (where the payer initiates the transaction directly from their bank account) and direct debit (where the receiver initiates the transaction from the payer's bank account with the pre-arranged authority of the payer). Electronic bill payment, which is a form of direct credit payment, is discussed separately below.
[26] PSB Annual Report 2006, at pp. 6–7.
[27] PSB Annual Report 2006, at p. 6.
[28] According to the ANZ survey, usage of direct debit increased from 50% of respondents in 2002 to 60% in 2005.
[29] PSB Annual Report 2006, at pp. 6–7.
[30] See footnote above.

2.13 During the 1990s it was thought that growth of internet transacting would stimulate the development of new forms of electronic currency (often known as 'e-money' or 'digital cash') based on microprocessor chip technology or personal computers, specifically for use in the online environment.

2.14 Despite a number of trials, this type of product has not been successfully commercialised in Australia (or, generally, elsewhere) to date as far as we are aware. Instead, as we have seen, largely existing payment methods have been adapted to the online environment.

Online payment facilitators/intermediaries

2.15 One somewhat new development in the online payments context has been the emergence of entities that facilitate secure consumer payments in the online environment. Examples include the PayPal, Paymate and Technocash systems.

2.16 PayPal[31] in particular has grown significantly in Australia in the last few years, primarily as a payment method for use in the eBay online market. Industry surveys indicate that PayPal now has more than 2 million customers in Australia.[32] Like similar schemes, the PayPal system is not a stand-alone scheme; rather it utilises the existing payments infrastructure of credit cards and bank accounts.

Other payment products

2.17 A range of entities apart from financial institutions issue limited use or closed system electronic payment facilities. These include familiar single payee phone and transport cards and the like, which have been in use for many years.

2.18 More recently, electronic gift cards issued by retailers, shopping centre operators and other businesses are increasingly replacing the traditional gift voucher. Some cards can be used widely. For example, the Coles Myer Card can be used in most retail outlets within the Coles Myer group, while the Westfield Card can be used in participating outlets at most Westfield shopping centres. Generally, gift cards are not re-loadable.

2.19 Another product to have emerged is the re-loadable prepaid card designed for convenience purchases of small items, such as food and drink. An example is the Starbucks Card. Other types of limited use retail payment

[31] http://www.paypal.com.au/au.
[32] Neilsen //NetRatings survey 2006.

mechanisms include toll road electronic tags (or e-tags), mobile phone third party billing services, and university cards with a purse function.[33]

2.20 At the time of the last review, it was assumed that the functions performed by many of these facilities would be undertaken increasingly on smart cards and other devices utilising microprocessor chip technology. By and large this has not proved to be the case to date.[34]

2.21 Rather than controlling the record of value using software in the user's card or other device, most payment systems rely on remote access communication with a central server to authorise payment. As discussed in Section 8, this has implications for the scope of Part B of the EFT Code (intended to provide a regulatory regime for these facilities, among others).

Emerging trends

2.22 Cash continues to dominate the low value/micro payments area, and alternative general use electronic payments products have yet to become established in Australia.[35] In some international markets, by contrast, there has been considerable development of open system facilities, providing a partial substitute for cash for lower value transactions. These include facilities that use contactless technology.

Non-contact payment cards

2.23 For example, internationally there has been some development in the area of contactless payment devices designed to facilitate instantaneous payments in the mass transit context. Examples include Hong Kong's Octopus card,[36] Singapore's EZ-Link card,[37] and London's Oyster card.[38]

2.24 These cards have an embedded microprocessor chip that stores customer details and maintains a record of available value. Using radio frequency technology, this information can be accessed and adjusted when the card is brought near a terminal capable of reading the information stored on the card.

---

[33] Some universities have developed staff and student identity (library etc) cards that can also be used to pay for goods and services purchased from retailers on and around the campus.
[34] This issue is discussed in detail in Section 8.
[35] A recent report to the Department of Communications, Information Technology and the Arts, which highlights the economic benefits associated with greater use of electronic payments channels and products, identifies the absence of cash-replacement electronic products as a key gap in the payments system in Australia. See *Exploration of Future Electronic Payments Markets (June 2006)*, prepared by Centre for International Economics and Edgar, Dunn & Company, at pp. 100–107.
[36] http://en.wikipedia.org/wiki/Octopus_card.
[37] http://en.wikipedia.org/wiki/EZ-Link.
[38] http://en.wikipedia.org/wiki/Oyster_card.

2.25 While initially designed to facilitate transit payments, such facilities have subsequently been adapted for making payments to other participating retailers, utilities and service providers within, and beyond, the transit corridor. Currently, a number of state transit authorities are developing and/or trialing smart transit ticketing systems using similar technology to that deployed internationally. Examples include NSW Transport Administration's 'T Card'[39] and the Victorian Transport Ticketing Authority smart card system.[40] The evolution of smart ticketing internationally suggests a possible development path for an open system electronic alternative to cash in Australia.

2.26 American Express, Visa and Mastercard have also developed cards with contactless functionality, and at least one Australian financial institution is currently trialling a credit card based on the Mastercard Paypass system.[41] These cards would appear to be gaining in acceptance internationally, notwithstanding that some concerns have been expressed about security issues.[42]

Mobile payments

2.27 Microchip and radio frequency technologies have also been utilised internationally to allow specially equipped mobile phones to be adapted as non-contact payment devices. This development appears to have been most successful to date in Japan and South Korea, where such mobile payments now have a significant level of acceptance.

2.28 According to a recent DCITA report, this technology has also captured the attention of business in Australia, and its potential is recognised. However, 'there are still many issues and challenges to be addressed' and products are 'still at a research stage, with a wait of five or more years before they are introduced into the mainstream market'.[43]

Prepaid cards issued by financial institutions

2.29 While prepaid payment cards issued by financial institutions have been a feature of the payments market in the United States and other countries for several years, they have only recently started to appear in Australia. Examples are Westpac's Mastercard Gift Card, ANZ's VISA Gift

[39] http://www.tcard.com.au/tcardweb/.
[40] http://www.doi.vic.gov.au/doi/internet/planningprojects.nsf/headingpagesdisplay/smartcard+ticketing+for+public+transport.
[41] 'Commonwealth to trial new credit card' *Sydney Morning Herald*, 05/04/06.
[42] See, for example, 'Contactless Payments Have Unique Security Risks' *Principia*, 09/08/05 and 'Switching Off may Reduce Contactless Card Fraud', *CIO Insight*, 16/09/05, accessed via epaynews.com.
[43] See *Exploration of Future Electronic Payments Markets (June 2006)*, footnote 35.

Card, and the VISA bopo card issued by CUSCAL and distributed and managed by Bill Express.[44]

Signature-capture payment terminals

2.30 Retailers using paper receipt signatures for card payments must store these against the possibility that they will need to be produced as evidence when a liability dispute with the customer arises. Technologies are now being implemented in the US and elsewhere that allow retailers to avoid this. Instead of signing a paper receipt, the user signs a pad that captures their signature electronically. Together with receipt details, the signature information is then stored on an in-store server or external database, and can be retrieved if required to resolve the chargeback dispute.[45] We understand there has been some limited trialling of this technology in Australia as well.

Electronic payments and fraud

2.31 With the growth of electronic payments, there has been a marked by increase in the range and extent of fraud-related activities in recent years. Sensitive financial/banking data able to be used to perpetuate fraud may be captured in a number of ways. Techniques employed include: hacking into the systems of financial institutions, merchants and third party service providers;[46] wire tapping; and criminal infiltration of organisations where large amounts of data can be accessed.

2.32 Other forms of fraud focus on the consumer interface. For example, increasing use of the internet as a transaction channel (discussed previously) has stimulated an accompanying growth in fraud directed at online users and their PCs and other equipment. As online fraud raises significant issues for this review, it is considered in greater detail in the next section.

2.33 The 'skimming' of credit and debit cards has also emerged as a key fraud challenge. Industry sources indicate that the use of counterfeit cards created from information skimmed from magnetic stripe cards at retail outlets and ATM machines is now the single biggest source of 'card present' fraud against both issuer and acquirer institutions in Australia. This growth has prompted calls for enhanced card security, in particular for industry wide adoption of Chip + PIN in card payment systems in Australia.

---

[44] See further at www.bopo.com.au.

[45] A company producing this technology is the US-based VeriFone (verifone.com).

[46] The most notable case to date involving Australian account holders was the Card Systems breach in the US in June 2005.

Chip + PIN

2.34 Most payment cards issued in Australia still rely on magnetic stripe technology, and card present credit card transactions are still authorised by signature rather than PIN authorisation.

2.35 The international card schemes have developed the EMV (Europay, Mastercard and Visa) standard for chip use in financial transactions, and they are currently driving a worldwide process (including in the Asia Pacific region) to convert terminals and cards for chip-based transactions. As indicated, this is primarily motivated by concern about rising card fraud based on skimming—while criminals are readily able to skim the information contained on a magnetic stripe card, counterfeiting a chip-enabled card is very much harder.

2.36 Apart from fraud considerations, chip technology allows a lot more information to be held on the card and has various other benefits (for instance, it can be adapted for non-contact use, as discussed above). The schemes are also pushing institutions to adopt PIN authorisation, also regarded as more secure than the current signature-based process.

2.37 Although EMV chip migration is well advanced in a number of countries, in particular the UK, progress in this direction in Australia has been relatively slow—largely, it would seem, because card fraud levels have been kept relatively low and most institutions have not yet been satisfied about the business case for migration. Our understanding, however, is that migration is regarded as inevitable and is likely to occur in the next few years.[47]

2.38 As regards upgrading to PIN authorisation, according to the Payments System Board, 'By the end of 2008, it seems likely that cardholders will have the option of authorising credit card transactions at the point of sale with a PIN.'[48] This has important implications for the EFT Code and its administration as it will bring these 'card present' credit card transactions within its scope. (Currently, they are excluded, as noted above, by the manual signature authorisation exemption.)[49]

Your feedback

[47] To encourage migration, since 1 January 2006, a liability shift has been introduced under the card schemes' rules. As the PSB Annual Report notes: "Prior to this change issuing banks bore the cost of most fraud in the credit card system. The new arrangements mean that if an issuer has converted its cards to chip, but the terminal where the card is used has not been converted, the liability for fraud lies with the merchant's acquirer. This is encouraging both issuers and acquirers to speed up conversion in order to avoid liability for fraud."

[48] PSB Annual Report 2006, at p. 24.

[49] See cl 1.5, read together with the definition of 'EFT transaction' at cl 1.1.

Q1 What do you see as the emerging trends or developments in the consumer payments marketplace in Australia over the next few years?

Q2 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?

Q3 What are the issues associated with the emergence of 'non-contact' payment facilities?

Section 3: Growth in online fraud

This section summarises developments in online fraud and the implementation of fraud countermeasures. Consumer responses to the growth in online fraud are also considered.

This material is intended to provide a context for the discussion of online fraud and liability allocation under the EFT Code in Section 7.

Online fraud techniques[50]

3.1 The techniques used to perpetrate online fraud are often known collectively as 'phishing'. Phishing has been described as 'a form of online identity theft that employs both *social engineering* and *technical subterfuge* to steal consumers' personal identity data and financial account credentials'.[51]

3.2 Experts on online fraud emphasise the sophistication and rapid evolution of the techniques employed in its perpetuation. As one commentator notes:

> *Phishers are technically innovative, and can afford to invest in technology. It is a common misconception that phishers are amateurs. This is not the case for the most dangerous phishing attacks, which are carried out as professional organised crime. As financial institutions have increased their online presence, the economic value of compromising account information has increased dramatically. Criminals such as phishers can afford an investment in technology commensurate with the illegal benefits gained by their crimes.*[52]

Deception-based phishing

3.3 In a typical phishing scheme, criminals who want to obtain personal data from people online first create a replica or 'spoof' website and emails of a financial institution, e-retailer, credit card company or other organisation that deals with financial information.

3.4 Phishers typically then send the spoofed emails to as many people as possible in an attempt to lure them into the scheme. These spam emails

---

[50] For a detailed recent summary of online fraud techniques, see *Report on Phishing* (October 2006) to Minister of Public Safety and Emergency Preparedness Canada and Attorney General of United States, available at www.usdoj.gov

[51] See homepage of Anti-Phishing Working Group at http://www.antiphishing.org/index.html

[52] Identity Theft Technology Council (ITTC) Report, *Online identity Fraud Technology and Countermeasures* (3 October 2005), available via APWG site. The ITTC is a US-based public-private partnership between the US Dept of Homeland Security, SRI International, the APWG and private industry.

redirect recipients to a spoofed website where they are asked to enter their account details and other sensitive data. While most recipients will not have an account or existing relationship with the business or government entity being spoofed, a proportion will. In these cases recipients of the spoofed emails and websites are more likely to be deceived.

3.5 Phishers typically rely on recipients' familiarity with and trust of the trade names, logos and other markers of the legitimate businesses or government organisations they spoof—as well as ignorance of how easily these markers of trust can be replicated. Typically, they also create a sense of urgency and the need for immediate action by warning victims that failure to comply with instructions will lead to account termination or other negative consequences. In addition, they exploit the fact that online users generally lack the tools and technical knowledge to be able to authenticate the messages they receive.

3.6 In recent years, criminals have further refined their attacks by incorporating additional or variant techniques. In some cases, for example, phishers use other illegal means to obtain personal information about a group of people. They then target that specific group with emails that appear to come from a trusted source because they include the illegally-obtained information. This technique is sometimes referred to as 'spear phishing' because of its highly targeted character.

3.7 Another technique is voice phishing or 'vishing'. This has been described as follows:

> *Vishing can work in two different ways. In one version of the scam, the consumer receives an email designed in the same way as a phishing email, usually indicating that there is a problem with the account. Instead of providing a fraudulent link to click on, the email provides a customer service number that the client must call and is then prompted to log in using account numbers and passwords. The other version of the scam is to call the consumers directly and tell them they must call the fraudulent customer service number immediately in order to protect their account. …*[53]

Use of technical subterfuge

3.8 Technical attacks do not depend primarily on tricking users into divulging their sensitive information. Rather, certain forms of malicious computer code ('malware' or 'crimeware') that can capture and transmit sensitive information directly are installed on targeted users' computers and other equipment. Various strategies are used to spread this malicious code, and the forms of attack are constantly evolving.

---

[53] See *Report on Phishing*, footnote 50 above, at p.10

3.9 One type of scheme involves the use of key-logging software. Through a range of techniques, phishers cause internet users to unknowingly download code that includes key-logging software. This software is typically set to operate when the user uses their internet browser to access an online financial account. The user's keystrokes are recorded during log-in, and the data is then forwarded to a phishing server. It can then be used to reproduce the user's username and password and, ultimately, to access their account and withdraw funds.

3.10 Redirectors are another form of technical subterfuge. Ordinarily when an internet user types the address of their financial institution (or other business) into their internet browser, the computer directs the user to the correct site. In a redirection scheme, however, malicious code introduced by the phisher changes the code inside the user's computer causing the user to be unknowingly redirected to a phishing website resembling the site the user had intended to access. After the user's access credentials have been obtained by this phisher-controlled proxy, the user may then be redirected to the legitimate site to complete the transaction.

Extent and cost of online fraud in Australia

3.11 There is an absence of public data on the extent of internet banking fraud in Australia. Industry estimates of net losses have been in the vicinity of $25 million per year in recent years; however, it is acknowledged that this is only a round figure and that the total costs (including costs associated with investigating fraud claims) may be higher. It is generally accepted that levels of internet fraud remain considerably lower than other forms of fraud, such as cheque fraud and credit card fraud.

3.12 In November 2006, the Australian Payments Clearing Association released data covering all financial institutions for cheque, debit card, credit card and charge card fraud for the period July 2005 to June 2006.[54] In the case of debit card fraud, the *Other* category (which includes fraud based on identity takeovers and false applications) accounted for around 20% of total debit card fraud by number and 19% by value, where a PIN was used; and around 12% by number and 10% by value where a PIN was not used. The total value of *Other* losses is given as less than $2.5 million.[55] In the case of credit card fraud, Card Not Present (CNP) fraud constituted around 37.5% by number and around 27.2% by value of total credit and charge card fraud.

---

[54] *New data to help fight fraud*, Media release 10/11/06, available at www.apca.com.au. This was the first time such data had been released. The data is not broken down by payments channel.

[55] Ibid. See Payment Fraud Statistics, Debit Card Fraud Perpetrated in Australia (1 July 2005 – 30 June 2006), p.4. The last figure combines total value figures for PIN used and PIN not used.

The total value of losses due to CNP fraud is given as a little over $23.8 million.[56]

3.13 Internationally, there is evidence of substantial growth in the extent and cost of online fraud in recent years.[57]

Fraud countermeasures

User authentication

3.14 An effective system for authenticating the identity of the person undertaking a banking session or transaction is regarded as central to online fraud prevention. Until recently, institutions and their consumer customers have generally relied on user ID and password as the sole means of authenticating the user in the online environment.[58]

3.15 Increasingly, however, because of the online threat, this method is being viewed as inadequate by itself, particularly in situations involving the transfer of funds to third parties. Many financial institutions are therefore looking at how user authentication can be enhanced as part of their broader anti-fraud strategy, using methodologies that are frequently described as involving one or more of three basic 'factors': see Table 4.[59]

Table 4: Factors in user authentication

Something the user *knows*	Apart from passwords and PINs, other methods based on shared secrets have also been developed: • For example, before a session starts, a customer may be required to answer specific questions about their recent transactions, minimum monthly repayments or similar details. • Another technique is to require the customer to identify or select an image (chosen in advance by arrangement with the institution) at the start of each banking session.
Something the user *has*	Various types of device or 'token' in possession of the user, combined with the user's password or PIN, have been developed to enhance the

[56] Ibid. See Payment Fraud Statistics, Credit Card and Charge Card Fraud Perpetrated in Australia and Overseas on Australian-issued Cards (1 July 2005 – 30 June 2006), p.5.
[57] See *Report on Phishing*, footnote 50 above, at p. 5 (*The scope of phishing*) for a summary of recent international surveys and reports
[58] Additional authentication has been common in business banking context for a number of years.
[59] The summary that follows draws on the US FFIEC agencies' *Authentication in an Internet Banking Environment* (12 October 2005). This sets out the expectations of US regulators regarding security measures to reliably authenticate customers remotely accessing their internet-based financial services. Available at www.ffiec.gov

	level of security: • A USB token is one example. The user plugs the token into the USB port of a computer with internet access, and is then prompted to enter a PIN or password linked to the device to start the session. • Another type of token generates unique one-time passwords (OTP) displayed on a small screen at very regular intervals (e.g. every 30 or 60 seconds). This additional code must be entered for each login or transaction in addition to the user's normal password or PIN. (The scratch card is a low-tech version of the OTP generating token.) • Another example is a smart card inserted into a compatible reader attached to the user's computer. If the smart card is recognised as valid, the customer is then prompted to enter their PIN or password.
Something the user *is*	Biometric technologies can also be used to identify or authenticate the identity of the user based on previously scanned characteristics such as: • physiological characteristics (e.g. fingerprints, iris configuration, and facial structure); or • physical characteristics (e.g. the rate and flow of movements, such as the pattern of data entry on a computer keyboard). Before a session commences, the user interacts with the live-scan process of the biometric technology; the results of this process are compared with the previously captured and registered data; assuming a match, access is granted.

3.16 The use of two or more factors of authentication—such as a combination of something the user knows (a password) with either something the user has (a token), or something the user is (a biometric indicator)—is generally regarded as providing a significantly higher level of security than single factor authentication. On the other hand, using additional single factor authentication, such as requiring the user to enter more than one piece of secret information before the transaction can proceed will also enhance online security.

3.17 A multifactor authentication methodology may also include out-of-band authentication, when the identity of an individual is verified through a different channel from the one being used to undertake the transaction. For example, a phone call, email or text message might be sent to the user seeking out-of-band confirmation of a requested transaction.

Implementation of enhanced user authentication by Australian institutions

3.18 Some Australian institutions have taken steps towards implementing two-factor authentication of consumer users, although the extent this has occurred to date would appear to be relatively limited.

3.19 We are aware of the following developments:

(a) Introduction of token-based scheme by Bendigo Bank.

(b) NAB scheme that allows internet banking customers to authenticate their logon by means of their normal password plus a unique session code sent by SMS to a pre-arranged phone number.

(c) A number of institutions have also implemented processes requiring users to answer additional questions before third party transactions can proceed.

3.20 The ABA has produced online user authentication guidelines linking recommended levels of authentication to risk levels associated with different transactions and services. (The guidelines are recommendatory only and have not been made public on the basis of security concerns.)[60]

3.21 It appears that the willingness of institutions to invest in online fraud countermeasures has been limited to some extent by the relatively low losses to date (see above), and the associated difficulties of making a business case for higher levels of investment in countermeasure technology. Institutions are also concerned about negative consumer reaction to more onerous or elaborate access control processes.

Other security measures adopted

3.22 It is important to acknowledge that, while financial institutions are grappling with the issue of how to enhance user authentication for their consumer customers, this is only one aspect of their response to the online fraud threat. Table 5 sets out some other measures adopted.

Table 5: Other security measures for dealing with fraud

Encryption	As far as we are aware, all institutions that subscribe to the EFT Code fully encrypt customer information communicated to their systems. We understand that 128-bit SSL is the encryption technology currently used by most. Institutions also utilise 'firewall' technology to protect their internal systems and customer information against intrusion from the internet.
Consumer awareness	Most online banking sites contain material warning customers about security issues and outlining good online practices (although the level and prominence given to this material varies). Institutions also seek to inform their customers through brochures, messages on account statements and in other ways.

[60] In addition, on 4 December 2006 the ABA released a consultation draft *Guiding Principles for Accessible Authentication*, designed to promote accessible authentication systems. Submissions are due by 2 February 2007. Available at www.bankers.asn.au

[61] http://www.staysmartonline.gov.au/

	Industry associations have also produced materials and undertaken media campaigns. More recently, the industry has supported the Australian Government's National E-Security Awareness Week, which included the launch of *StaySmartOnline* site.[61] Another initiative is the recently-launched *Protect your financial identity* site developed jointly by the ABA, the Australian High Tech Crime Centre and ASIC.[62]
Consistent communication policies	Security experts emphasise the importance of institutions having clear email and website practices consistent with their security guidelines for users, such as: • never asking for personal/account information in an email, • never providing a clickable link in an email, • not using websites with unusual or unpredictable names. The first constraint appears now to be universally accepted. We seek more information on whether institutions engage in other practices arguably similar to those employed by phishers, such as sending emails to customers containing hyperlinks. (We note that some institutions specifically affirm that they do not.)
Monitoring activity	A major focus of Australian institutions' response to the online fraud challenge to date has been in the areas of early detection and loss minimisation. A number of institutions now use sophisticated monitoring software to monitor online banking transactions for evidence of unusual (and potentially fraudulent) patterns of transaction. In 2005, ANZ announced that it had implemented a one-day delay in processing 'pay anyone' transfers so that suspicious transfers could be picked up over night using its detection software. (We assume that other institutions may have done likewise.) However, not all subscribing institutions are using monitoring software, with cost being a factor in particular for some smaller institutions. We understand that integrating disparate fraud detection systems remains a major challenge for many institutions.
Early warning from customers	Many institutions encourage their customers to forward hoax emails and provide a designated email address for this purpose.
Transaction limits	Limiting the amount that can be taken by a fraudster in one day is another mitigation strategy. There appears to have been a significant—although not universal—tightening up of daily transaction limits in recent years, with institutions introducing limits on channels where they had not previously existed and/or reducing daily limits (or making the availability of a higher limit conditional upon the account user's participation in multifactor authentication processes).

[62] www.protectfinancialid.org.au

Staffing and training	We understand that most institutions have introduced enhanced security training for staff, as well as employing more dedicated security staff, and conducting regular security audits.
Cooperation with law enforcement	There is close cooperation between industry and law enforcement agencies (including the Australian Federal Police and the Australian High Tech Crime Centre[63]) to close down internet fraud scams as soon as possible. This includes industry secondments to AHTCC. We understand that this cooperation has been a significant factor in limiting unrecovered losses resulting from such scams.
Customised measures and technologies	Apart from the general measures, various institutions have adopted specific measures and technologies. One example is the dynamic on-screen pin pad used by institutions including ING bank, Citibank, Westpac and Credit Union Australia. This is a technology for countering the use of keystroke logger software to harvest users' account numbers and access codes. It consists of an on-screen pin pad on which the customer's PIN is entered using the computer's mouse rather than the keyboard.

Consumer awareness and response

Impact of internet fraud on online user confidence

3.23 Research commissioned by the Department of Communications Information Technology and the Arts (DCITA) and referred to in *Trust and Growth in the Online Environment (November 2005)*[64] indicates that, while the majority of Australian internet users transact online, 54% of active and 55% of passive online users rank general security of the internet as their number one concern.[65]

3.24 Other concerns included the potential for fraud (23% active users and 17% passive users), privacy (20% and 17%), misuse of personal information (9% and 14%), and provision of personal information (13% and 9%).[66]

[63] ATHCC provides a national coordinated approach to combating serious, complex and/or multi-jurisdictional high tech crimes. It is hosted by the Australian Federal Police and includes representatives of all Australian state and territory police forces.

[64] The research was a 'weighted' survey of 1500 respondents aged 14 years and over conducted by Sensis. Available at: http://www.dcita.gov.au/communications_for_business/industry_development/statistical_benchmarking/trustandgrowth

[65] Report at pp. 23–25. The report defines 'passive' internet users as survey respondents who did not engage in online ordering or booking, did not make online payments, did not do banking online, and did not provide personal information online. 'Active' users engaged in one or more of these activities.

[66] See footnote above.

3.25 As the DCITA report notes, the extent of concerns about security and possible misuse of personal information is in itself unsurprising; previous research suggests that such concerns are long-standing and persistent.[67] 'What is lacking in the Australian context (and presumably for other countries) is any substantial proof that the situation has changed over time.'[68]

3.26 However, the report also refers to a US banking industry survey (conducted by IPSOS Insights in August 2005) suggesting that concerns about personal information, identity theft and services were having a 'stalling' or 'flattening' effect on online banking growth.[69] More recent international studies would appear to support the view that fear of fraud may be hampering online banking growth.[70]

Protective measures adopted by online users

3.27 Despite having concerns about online fraud, most people making transactions online appear not to take adequate steps to secure their equipment against technical subterfuge. The research commissioned by DCITA referred to in the previous sub-section, found that 'Australians transacting online generally adopted a minimalist approach to securing online transactions.'[71]

3.28 Specifically, the DCITA report found only:

(a) 32% of active internet users reported regularly updating virus or worm protection software;

(b) 18% looked for websites with 'trustmarks';

(c) 15% only dealt with well known service providers; and

(d) 14% used a firewall service.

---

[67] Similarly, the majority of respondents to the *ANZ Financial Literacy Survey 2005*, footnote 13 above, (78%) also thought there were risks associated with banking on the internet. Key logging by hackers (59%) was identified as the biggest risk, followed by unsecured sites (27%) and credit card fraud (19%): see pp. 122–123 of the survey.

[68] See footnote above, p. 25.

[69] Available at: http://www.ipsos-na.com/news/pressrelease.cfm?id=2765. This report found that, after years of dramatic growth in online banking penetration, the percentage of Americans who conduct banking online remained unchanged (at 39%) during the 12 months to August 2005.

[70] For example, in media release of 23 January 2006, *Banks encouraged to engage consumers in tackling online fraud*, the UK Financial Services Authority referred to research it had commissioned indicating that "consumer confidence in internet banking is fragile. Half of active internet users said they were 'extremely' or 'very' concerned about the potential fraud risk of making an online transaction". The release goes on to quote an FSA spokesperson as saying: "If consumers were asked to foot the bill for internet fraud losses, our research shows that they would stop using the tool." http://www.fsa.gov.uk/pages/Library/Communication/PR/2006/005.shtml

[71] *Trust and Growth in the Online Environment*, footnote 60 above, at p.2

3.29 In total, only 35% of active internet users adopted multiple measures to secure online transactions (with 49% adopting a single measure, 7% doing nothing and 9% not knowing). However, the level of protective measures adopted increased significantly for users with multiple transaction services.

User capacity to reduce online threats

3.30 The failure to adopt adequate security may be, in part, a capacity issue. The *ANZ Financial Literacy Survey 2005* found that two-thirds of respondents who see risks associated with internet banking said that they were aware of ways to minimise those risks. However, this varied depending on overall level of financial literacy as measured by the survey. Thus, 77% of those in the top Quintile for financial literacy said they were aware of risk-minimisation measures, whereas for those in the lowest Quintile and those with only a Year 10 level of education the figures were, respectively, only 48% and 47%.[72]

3.31 We are not aware of Australian research that attempts to objectively assess online users' knowledge of and ability to implement measures to reduce the risks of online fraud (i.e., independently of users' self-perceptions). Nor are we aware of research on the extent to which Australian online users are duped by deception-based phishing attacks.

3.32 On the last issue, US surveys suggest that around 5% of adult American internet users are successfully targeted by phishing attacks each year (i.e., persuaded to release sensitive personal or financial information) at a cost of around $2.4 billion per year.[73] However, one recent study suggests that these self-assessment surveys may underestimate the real cost and number of victims and that as much as 11% of trick messages might be getting responses.[74]

---

[72] *ANZ Financial Literacy Survey 2005*, footnote 13 above, at pp. 123–125. Four methods were most commonly cited to minimise internet banking risks: using a firewall (32%), keeping anti-virus software up to date (27%), changing passwords regularly (23%) and ensuring the bank has secure website/good security measures in place (19%).

[73] Litan, A, *Phishing attack victims likely targets for identity theft*, FT-22-8873, Gartner Research (2004)

[74] Jakobsson, M and Ratkiewicz, J, *Designing Ethical Phishing Experiments: A study of (ROT13) rOnl query features* (23-26 May 2006, Indiana University). For a link to the study see *Survey: More phishing suckers out there than we thought*, Network World, 18/10/06, at http://www.networkworld.com/news/2006/101906-phishing.html. The study relied on simulated phishing attacks on eBay customers rather than self-assessment surveys. The authors speculate that the latter may understate the number of successful targets because people won't admit to being duped.

Your feedback

Q4 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?

Q5 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?

Q6 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.)

Q7 What information can you provide to the Working Group about the online fraud mitigation skills of Australian online users?

Section 4: Regulatory developments

There have been a number of significant regulatory developments impacting the consumer payments system since the last review of the EFT Code.

Corporations Act regulation

4.1 The *Financial Services Reform Act 2001* (FSR Act) amended the *Corporations Act 2001* (Corporations Act), inserting a new regime (Chapter 7) regulating financial services and markets.[75] Chapter 7 establishes broadly uniform regulation of most financial services and financial products. The regime is administered by ASIC.

4.2 Elements of the regime include licensing of financial services providers, conduct requirements, financial services disclosure requirements, and financial product disclosure requirements. Financial services regulated include giving advice about regulated products and issuing regulated products.

4.3 Regulated financial products include (relevantly to this review) deposit-taking facilities and non-cash payment facilities. These terms are defined as follows:

(a) A '*deposit-taking facility*' is 'made available by an authorised deposit-taking institution (within the meaning of the Banking Act) in the course of its banking business (within the meaning of the Banking Act) other than a Retirement Savings Account'.[76]

(b) A '*non-cash payment facility*' is a facility through which, or through the acquisition of which, a person makes non-cash payments (NCPs).[77] NCPs are defined broadly as payments made 'other than by the physical delivery of Australian or foreign currency in the form of notes and/or coins'.[78]

As we discuss in Sections 6 and 9, there is considerable overlap between the scope of these last-mentioned products and both an 'EFT account' as defined in Part A of the Code and a 'consumer stored value facility' as defined in Part B of the Code.

---

[75] For more information on this process see http://www.treasury.gov.au/content/financial_services.asp?ContentID=328&titl=Financial%20Services.

[76] Section 764A(1)(i), Corporations Act: 'RSA' refers to a retirement savings account within the meaning of the *Retirement Savings Accounts Act 1997*. See s764A(1)(h)).

[77] Section 763A(1). Financial products under the Corporations Act also include facilities through which, or through the acquisition of which a person 'makes a financial investment' or 'manages a financial risk'.

[78] Section 763D(1) (s763D(2) lists exceptions).

Disclosure regulation and deposit products

4.4 Under the Corporations Act regime, retail clients to whom a regulated financial product is recommended, issued or sold must generally be given a product disclosure statement (PDS) setting out the main features of the product.[79] There are also requirements to provide a supplementary PDS in certain circumstances.[80] In addition, clients must be given additional information on request,[81] and in certain circumstances advised of 'significant changes and material events'.[82]

4.5 However, as a result of amendments to the Corporations Act in 2005, these requirements no longer apply to basic deposit products (BDP) and related NCP facilities, subject to certain limited information disclosures being made in some form.[83] A BDP is defined to include at call deposit facilities as well as some term deposits.[84]

4.6 The Government saw this revised approach to disclosure for basic deposit products as appropriate given the relatively low risk and generally well-understood nature of these products. It also noted the role played by industry codes in regulating disclosure in the consumer banking context.[85]

Disclosure regulation and non-cash payment facilities

4.7 As a result of both legislative exemptions and ASIC class order relief, the application of the disclosure and related requirements of the Corporations Act to NCP facilities is also quite limited. In particular:

(a) Single payee NCP facilities[86] are legislatively exempt from the regime, as are electronic facilities when there is no standing arrangement between issuer and payer (such as international money transfers and telegraphic transfers).[87]

---

[79] Part 7.9, Div 2, Corporations Act generally; s1013D sets out main content requirements of PDS
[80] Part 7.9, Div 2, Subdivision D, Corporations Act
[81] Section 1017A, Corporations Act
[82] Section s1017B, Corporations Act
[83] Regulation 7.9.07FA inserted by *Corporations Amendment Regulations 2005 (No. 5*)
[84] Section 761A, Definitions, Corporations Act ('basic deposit product').
[85] Explanatory Statement, Select Legislative Instrument 2005 No. 324, *Corporations Amendment Regulations 2005 (No. 5)*, Item 8 of which states in part: "Further, issuers of BDPs are subject to industry codes such as the Code of Banking Practice and the Credit Union Code of Practice. These codes contain requirements and standard practice for disclosure in the banking industry".
[86] Section 763D(2)(a)(i), Corporations Act
[87] Regulation 7.1.07G, Corporations Regulations

(b) Under ASIC Policy Statement 185 *Non-cash payment facilities*, released in November 2005,[88] we have given class order relief for a number of types of NCP facility. These include loyalty schemes, electronic road toll devices, prepaid mobile phone accounts, gift cards and vouchers, and low value non-cash payment facilities, each as defined.[89] In the case of low value facilities, the class order imposes alternative disclosure and transaction confirmation obligations. Otherwise, the facilities in question are either determined not to be regulated financial products at all, or unconditional relief from the Corporations Act's disclosure requirements is granted.

4.8 The Government is currently also considering a proposal to make the disclosure requirements for stand-alone NCP facilities under the Corporations Act consistent with the requirements for basic deposit products (discussed above).[90]

Banking industry codes

Code of Banking Practice

4.9 The Code of Banking Practice (CBP)[91] was first released in August 2003 and most recently revised in May 2004. It sets out the banking industry's key commitments and obligations to customers on standards of practice, disclosure and principles of conduct for their banking services. Nearly all banks providing services to retail customers subscribe to the CBP, which applies to small business as well as personal bank customers. When there is an inconsistency between the CBP and the EFT Code, the EFT Code will apply (section 39.2, CBP).

4.10 The CBP includes detailed provisions regarding, among other things, the provision of information about banking services, disclosure of terms and conditions, disclosure when changing terms and conditions, the provision of statements of account, dispute resolution and the provision of information electronically—areas also addressed in the EFT Code.

4.11 The CBP also sets out other obligations relevant to the payments' area, including a requirement to promptly process direct debit cancellations on request, as well as provisions relating to the card schemes' chargeback regime. Some issues of alignment between the

[88] Available at: http://www.asic.gov.au/asic/asic_polprac.nsf/byheadline/Policy+fsr+?openDocument

[89] See, respectively, ASIC Class Orders [CO 05/737], [CO 05/739], [CO 05/740], [CO 05/738] and [CO 05/736].

[90] This proposal was put in Corporate and Financial Services Regulation Review Proposals Paper (November 2006), 1.5 Non-cash payment facilities, at pp. 28-31

[91] Available at http://www.bankers.asn.au/Default.aspx?ArticleID=446.

disclosure and notification requirements of the CBP and those of the EFT Code are raised in Section 6.

Other financial industry codes

4.12 The Credit Union Code of Practice (released in July1994) has been adopted by credit union members of Abacus–Australian Mutuals, the Association of Building Societies and Credit Unions. Abacus is considering a range of amendments and improvements to this code, following an independent review conducted some years ago.[92] The Building Societies' Code of Practice was abolished in 2003.

Other regulatory developments

Reform of card payment systems

4.13 In recent years, the Reserve Bank of Australia (RBA) has implemented major reforms to Australia's credit and debit card systems, using its powers under the *Payment Systems (Regulation) Act 1998* (PSR Act). The primary objective of the PSR Act is to increase competition and improve efficiency in the payments system, while preserving its integrity, security and fairness.[93] Details of the RBA reforms are set out in the *Payments System Board Annual Report 2006*.[94]

Prudential supervision of holders of prepaid value

4.14 The Australian Prudential Regulatory Authority (APRA) and the RBA share regulatory responsibility for prudential supervision of holders of value in prepaid or stored value facilities, called purchased payment facilities (PPFs).[95] Since 2000, PPFs issued on a wide basis and that allow value to be redeemed for cash, have been regulated by APRA.[96] In 2005, APRA released a regulatory framework for PPFs subject to its

[92] More information is available at http://www.abacus.org.au/credit_unions/codeofpractice.htm.
[93] Payment Systems (Regulation) Bill 1998, Explanatory Memorandum, para. 1.2
[94] Available at: http://www.rba.gov.au/PublicationsAndResearch/PSBAnnualReports/index.html.
[95] A PPF is a facility for making payments (up to an available limit) that a user purchases from a provider of the facility or a person acting under an arrangement with the provider (in both cases called 'the holder of the stored value'). Under a PPF, it is the holder of the stored value, rather than the user, that makes the payment when the facility is used: s9, PSR Act.
[96] See RBA and APRA Joint Media Release 15 June 2000 *Regulation of Purchased Payment Facilities*

jurisdiction.[97] Pay Pal Australia has since been authorised by APRA to carry on a banking business confined to the provision of PPFs.[98]

4.15 Holders of value in more limited facilities must be either authorised or exempt from authorisation by the RBA, under the PSR Act.[99] The RBA may also declare that the PSR Act does not apply to a limited-use facility or class of facilities if it considers this appropriate.[100]

Anti money laundering reforms

4.16 The recently-enacted anti money laundering (AML) legislative package,[101] to be administered by AUSTRAC, covers a broad range of designated services, including services provided by the financial sector. We do not expect the obligations created by this suite of reforms to overlap with the requirements of the EFT Code. However, we appreciate that businesses are considering their obligations under the new AML regime at the same time as they are participating in this review. (The 3-month period for comments on this consultation paper partly reflects our awareness of this.)

Your feedback

Q8 Are there developments in the regulatory environment that the Review Working Group should particularly consider? What are the implications of those developments for the EFT Code?

---

[97] See APRA Media release, 29 November 2005, for links to Australian Prudential Standard (APS 610) and *Guidelines on Authorisation of Providers of Purchased Payment Facilities.*

[98] Copy of authorisation is available at: http://www.apra.gov.au/ADI/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=12672

[99] Section 22 of the PSR Act (Holder of stored value must be an ADI or be authorised or exempted under this Part) read in conjunction with s23 (Authority to be the holder of the stored value) and s25 (Exemptions).

[100] Section 9(3), PSR Act This power has been used to declare that the PSR Act does not apply to a number of classes of facility to date. These include:

(a) Declaration No. 1, 2006 regarding Purchased Payment Facilities (covers gift cards, loyalty schemes, electronic road toll devices, pre-paid mobile phone accounts).

(b) Declaration No. 2, 2006 regarding Purchased Payment Facilities (covers certain limited value facilities).

[101] The *Anti-Money Laundering and Counter Terrorism Financing Act 2006* (AML/CTF Act), the *Anti-Money Laundering and Counter Terrorism Financing (Transitional Provisions and Consequential Amendments) Act 2006* (the Consequential Amendments Act) and the Rules to the AML/CTF Act make up the suite of anti-money laundering and counter terrorism financing reforms. The Acts received Royal Assent on 12 December 2006.

Section 5: EFT Code, Part A (Scope and interpretation)

This section outlines issues about the scope of Part A of the EFT Code, which applies to 'EFT transactions'.[102] The requirements imposed on subscribers by Part A are considered in Sections 6 and 7.

How the scope of Part A is defined (cl 1.1, 1.2, 1.5)

5.1 Part A applies to 'EFT transactions'.[103] 'EFT transactions' is defined exhaustively using a number of related terms, which are also defined—namely, 'funds transfers', 'electronic equipment', 'access method', 'account institution' and 'EFT account'. In turn, the definitions of all of these subsidiary terms (except 'electronic equipment') refer to other of the subsidiary terms, and all (again except 'electronic equipment') include additional terms that are also defined. In addition, there are nine Endnotes that comment on or give examples of the various terms used, some of which are quite detailed.

Issue/options

5.2 The definition of EFT transactions has been criticised on the grounds that it is overly complex and somewhat circular. A simpler approach to defining the scope of Part A may help to make the EFT Code more accessible to account institution staff, consumers and others. How the scope of Part A of the Code is defined is likely to be affected by any changes made to the scope of Part B of the Code: see Section 8.

Your feedback

Q9 Do you have any suggestions 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?

[102] 'EFT transactions' are defined as 'funds transfers initiated by giving an instruction, through electronic equipment and using an access method, to an account institution (directly or indirectly) to debit or credit an EFT account maintained by the account institution': cl 1.1(a).

[103] 'EFT transactions' are defined as 'funds transfers initiated by giving an instruction, through electronic equipment and using an access method, to an account institution (directly or indirectly) to debit or credit an EFT account maintained by the account institution': cl 1.1(a).

Biller accounts exclusion (cl 1.4, 1.5)

5.3 Many businesses (e.g. utility suppliers and department stores) maintain internal customer accounts the sole purpose of which is to record amounts owing and paid by the customer for goods or services provided by the business. These accounts are defined as 'biller accounts' under the EFT Code if the customer is able to initiate an EFT transaction from or to the account (cl 1.5). Most EFT transactions involving biller accounts are excluded from regulation under Part A (cl 1.4).

Table 6: Biller accounts

When the Code does not apply	Example
Part A does not apply at all to user-initiated transactions that *debit* a biller account, if the purpose of these transactions is to pay for goods or services (apart from financial services) supplied by the business with whom the account is maintained (cl 1.4(b)).[104] Only cl 7 of Part A (dealing with deposits to accounts) applies to user-initiated transactions that *credit* a biller account (cl 1.4(a)).	When funds are transferred from a customer's prepaid mobile phone account to pay for telephony services provided by the mobile phone operator, the transfer is not regulated under cl 1.4(b). If customers can use their mobile account to pay third parties for goods or services (e.g. for mobile content services or goods or services provided in the physical world), the transfer of funds to pay the third party is regulated under the EFT Code.[105]

5.4 Following representations by businesses that maintain internal customer accounts, the biller accounts were excluded in the EFT Code when its scope was broadened after the 1999–2001 review.[106] The Working Group for that review stated in its *Second Draft Expanded EFT Code of Conduct and Commentary (2000)* at p. 24:

> *Given that the inclusion of payments to billers from prepaid biller accounts would significantly broaden the scope of the Code, the Working Group chose not to include them at this time. At this stage, there is not evidence of significant problems with the debiting of most prepaid biller accounts, e.g., for electricity, gas or telephone services, although some problems have been noted in the case of prepaid ISP customer accounts. Because the use of prepaid biller accounts in Internet commerce is likely to increase, the Working Group recommends that the issue of user-initiated funds transfers to billers from prepaid biller accounts be revisited on the next review of the Code.*

[104] An exception to the exclusion for transactions to pay for financial services was included 'to maintain competitive neutrality with financial institutions': Endnote 3, second dot point.
[105] See Endnote 3, third dot point.
[106] See Section 1 of this paper

Issues/options

5.5 The biller accounts exception has been criticised from the perspective of the overall conceptual coherence of the regime.[107] It has also been noted in preliminary consultations that no organisations that provide payment services to third parties, as well as biller accounts, currently subscribe to the EFT Code.

5.6 Specific problems have been identified with the way the exception is explained and applied. In particular, Endnote 3 (first dot point) appears to suggest that, because of the operation of cl 1.4(a), the EFT Code does not apply to the receipt by a biller of funds transferred as a result of a BPAY transaction (the example given).

5.7 As has been noted, however, a BPAY transaction does not directly credit a *biller account.*[108] Rather it credits the biller's account with its financial institution—and is no different in this respect to any other EFT transaction from one person's account to another's. The biller will normally subsequently adjust the balance of its customer's internal account (the biller account) to reflect the payment received.

5.8 However, this is a separate process, and it is not one that is initiated by the account user through electronic equipment using an access method—in other words, it is not an *EFT transaction* as defined by Part A.

5.9 Unfortunately, the inclusion of the BPAY example in the Endnotes appears to have led to some confusion as to whether BPAY transactions come within the scope of the EFT Code (they clearly do, in our view). More generally, as the BPAY case illustrates, 'credits' to biller accounts will normally simply be book entries made by the business maintaining the account to reflect payments made through the ordinary banking system. As such, they are not regulated by the Code. Arguably, this casts doubt on the efficacy of having a carve-out for user-initiated EFT payments that directly credit a biller account (i.e. cl 1.4(a)).[109]

Your feedback

Q10 Should biller accounts continue to be excluded or should cl 1.4 be modified or, alternatively, removed altogether?

[107] In *Banking Law in Australia*, (4th edition, LexisNexis Butterworths, 2002), A.L.Tyree, the author states at p.347: 'If an account institution permits user-initiated account transactions, then it is hard to see why the [EFT] Code should not apply in the usual way'.
[108] See footnote above.
[109] Similarly, the continuing application of cl 7 to cl 1.4(a) transactions assumes that users themselves directly credit biller accounts.

Small business exclusion (cl 1.3, 11.1)

Issues/options

5.10 The issue of whether the EFT Code should apply to small business transactions was raised at the last review, and has again been identified as a matter for consideration in the current review.

5.11 Part A does not cover a funds transfer (or part of a transfer) that debits or credits an account designed primarily for a business and established primarily for business purposes (cl 1.3). Similarly, Part B does not apply to any use of an SVF designed primarily for use by a business and acquired primarily for business purposes (cl 11.1). As they raise similar issues, both these exclusions are considered together here.

Arguments for extending coverage

5.12 Proponents of extending coverage argue that small business entities suffer from much the same information asymmetries and power imbalances that disadvantage householders/consumers.[110] Indeed, small businesses (variously defined) already enjoy consumer-like protections under, among other instruments, the *Trade Practices Act 1974*, ASIC Act, Corporations Act, and the CBP. In addition, a number of external dispute resolution (EDR) schemes (including schemes such as the Banking and Financial Services Ombudsman and the Credit Union Dispute Resolution Centre that adjudicate disputes under the EFT Code) cover small business disputes.

5.13 Another argument for including small business in the scope of the EFT Code notes that those who (for a range of reasons) process business-related transactions through their personal accounts appear to already be covered by the EFT Code.[111] This puts small business people who use business banking accounts to do their business-related transactions at a disadvantage because they are not protected under the current EFT Code.

Arguments against extending coverage

5.14 Some industry representatives have questioned the need for any extension of coverage of the EFT Code to include small business. They argue that aspects of the Part A regime (in particular, the provisions relating to liability allocation) are not appropriate to the small business context.

---

[110] For example, Tyree, footnote 107 above, states at p. 346: 'The business account exclusion is unremarkable even though regrettable. Many small businesses are operated by individuals who are as unsophisticated about banking practice and procedures as any other consumer. They have as little bargaining power as the normal consumer, and as little financial power to resolve disputes with financial institutions. They are, in short, in need of the same protection which gave rise to the EFT Code in the first place.'

[111] As long as the account in question is not 'designed primarily for use by a business and established primarily for business purposes' such transactions would appear to fall outside the cl 1.3 exclusion and thus to be covered by the EFT Code.

They note that small businesses must be given incentives to maintain and improve their systems and procedures, particularly to meet the threat of online fraud. They go on to suggest that a regime allowing loss to be allocated to the institution in most situations would not provide appropriate incentives.

5.15 The volume and value of transactions to and from business accounts will on average be much larger than for consumer accounts. This would expose institutions to significantly greater potential losses as a result of fraud if the EFT Code regulated these accounts. Risk of high potential losses could impact on the cost and availability of the payment services institutions offer to small business.

5.16 Arguably, extending the EFT Code to cover small business may also prompt subscribers to demand a reduction in the overall level of protection in the liability allocation area, and perhaps other areas, to the detriment of consumer stakeholders.

Partial coverage

5.17 Another possibility is that some, but not all, the obligations under the EFT Code might be extended to cover small business transactions and facilities. For example, disclosure, transaction confirmation and dispute resolution requirements might apply, while the liability allocation regime might not. (Alternatively, the regime might apply in full but with a higher 'no fault' threshold than the $150 applying to consumer account holders.)

5.18 Some accounts operated by small businesses are no longer subject to the product disclosure statement requirements of the Corporations Act (as they come within the definition of a *basic deposit product* under that Act).[112] Under the limited coverage model, the EFT Code would provide an alternative voluntary disclosure regime for these products.

Threshold issue

5.19 Before an analysis of the costs and benefits of extending EFT Code regulation to small business transactions and facilities is considered, the extent of problems small business users of banking services experience has to be examined. In other words, is there a problem that needs regulatory intervention? We seek the views of small businesses and their representative organisations, as well as other stakeholders, on this issue.

[112] See Section 4 under *Disclosure regulation and deposit products*

Your feedback

Q11 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?

Section 6: EFT Code, Part A (Requirements)

This section outlines issues about the requirements of Part A of the EFT Code, apart from issues about liability under cl 5 and 6. Because of their complexity, those issues are dealt with separately in the next section.

Notifying changes to fees (cl 3)

6.1 Clause 3 sets out how subscribing institutions should notify fee increases and other changes.

6.2 Under cl 3.1(a), an account institution must give an account holder a written notice at least 20 days before:

(a) a charge for an access method (e.g. an internet banking fee) is imposed or increased;

(b) the account holder's liability for losses is increased (subject to EFT Code limits); or

(c) a daily or other transaction limit is imposed, removed or adjusted.

Issues/options

6.3 Industry representatives have raised concerns about the costs of the current notification requirements, in particular as they apply to notification of increases in fees and charges. They suggest that the costs outweigh the benefits to account holders. A range of approaches is taken to notification of increases in fees and charges in other regulatory regimes: see Table 7.

Table 7: Comparison of notification requirements

Corporations Act	Issuers must notify retail clients of material changes to regulated products, in writing, electronically or by other means specified in the regulations. Thirty days advance notice is required for a change that is an increase in a fee or charge.[113] (Note, however, that these and other disclosure requirements of the Act no longer apply to basic deposit products.)[114]
Uniform Consumer Credit Code	Notification of the amount, frequency or time for payment of a credit fee or charge (including a new credit fee or charge) must be given no later than 20 days before the change takes effect. This notification can be given by publishing a notice in a newspaper circulating throughout the jurisdiction. However, if this is done, the account holder must be given particulars of the change before or when their next account statement is sent.[115]

[113] Section 1017B(5), Corporations Act.
[114] See Section 4 under *Disclosure Regulation and Deposit Products*
[115] Section 61(1) and (2), Consumer Credit Code.

Code of Banking Practice	Some changes to terms and conditions (including the introduction of a new fee or charge by the bank) require advance notice in writing of at least 30 days. With variations in standard fees and charges, however, banks have the option of notifying their customers in the national or local media on the day on which the change takes effect, as an alternative to written notification.[116]

6.4 Industry representatives have suggested that the EFT Code's approach to notification of fee variations could be brought into alignment with that of the CBP. Apart from cost considerations, it is argued that having different notification requirements for fee variations specifically related to the use of an electronic access method is anomalous.

6.5 On the other hand, consumer representatives have expressed reservations about the efficacy of newspaper advertisements as a notification method. It has also been suggested that mandatory notices can be included with/on cardholder account statements and that this should limit the additional costs associated with this method of notification.

Your feedback

Q12 Should the requirement in cl 3.1 to provide written notification in advance of an increase in a fee or charge be replaced by another process? For example, should the notice appear in the national or local media on the day on which the increase starts?

Issuing transaction receipts (cl 4.1)

6.6 Two issues have been raised about the wording of the preamble to cl 4.1(a), which states:

> *Except where paragraph (b) applies, at the time of an EFT transaction and unless a user specifically elects otherwise, the account institution will ensure a receipt is issued containing all of the following information …*

6.7 First, some account institutions have developed systems in which the account user is given the opportunity to receive a receipt, but must 'opt-in' to do so. Arguably, this does not comply strictly with the 'opt-out' wording of the EFT Code ('unless a user specifically elects otherwise').

6.8 In our view, however, as long as the user is required to *consider* whether they want a receipt or not, it does not matter particularly from a consumer protection perspective whether they have to 'opt-in' to receive one or 'opt-out' to avoid receiving one. Subject to your views, we would therefore propose amending the wording of the EFT Code to put beyond

[116] Sections 18.1 and 18.3, CBP.

doubt the compliance of opt-in systems as long as those systems require the user to choose. (So, under this proposal, any default option must be the opt-in option. However, users would be given the alternative of positively electing to opt-out each time they transact.)

6.9 Secondly, the requirement that an account institution must generally 'ensure a receipt is issued' has been criticised on the basis that it does not make any concessions to technical difficulties—in particular, to the situation when an ATM or other transaction-processing machine (e.g. an EFTPOS machine) runs out of paper and a receipt *cannot* be issued.

6.10 In such cases, the account institution will arguably be in breach of the EFT Code even if it has taken all reasonable steps to ensure that its ATMs are supplied with paper and other supplies.

6.11 Arguably, a more flexible approach is needed. Currently, the general requirement is relaxed in situations when the user does not conduct a transaction using the account institution's own equipment or systems (cl 4.1(d)). In these circumstances the account institution is merely required to use its 'best endeavours' to provide a receipt. One suggested option would be to extend this 'best endeavours' standard more generally.

6.12 An alternative approach would be for the EFT Code to codify the now common practice of account institutions advising ATM users that technical difficulties will prevent a paper receipt from being issued before the transaction is processed. This gives users the option of proceeding/not proceeding with the transaction. Under this proposal, if the account institution gave this advice, it would be considered not to be in breach of the EFT Code obligation to ensure that a receipt was issued.

6.13 Arguably, this approach would give greater flexibility in the context of the real-world problem of ATMs running out of paper, without diminishing an important aspect of protection under the EFT Code. (There would be no inconsistency with the Corporations Act regime.[117])

Your feedback

Q13 Should cl 4.1(a) be revised to allow users to 'opt-in' to receive a receipt?

Q14 Should cl 4.1(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?

[117] Under the Corporations Act, amounts debited or credited to a basic deposit product need not be confirmed if a periodic statement is provided within 6 months: *see Consistency between Part A and Corporations Act* (cl 2-4) below.

Merchant identification on transaction receipts (cl 4.1)

6.14 Certain information must be included on the transaction receipt for transactions conducted by voice communications (cl 4.1(a) and (b)). In the case of payments to a merchant, cl 4.1(a)(vii) and cl 4.1(b)(v) require that the *name* of the merchant be stated on the receipt or as part of the process of confirming the voice communication transaction.

6.15 We understand that, with payment transactions undertaken by phone, the BPAY system (and possibly other bill payment services) records the biller's identifying number but not the biller's name (at least in the case of most billers).[118] For such transactions, strict compliance with cl 4.1(b)(v) by subscribers therefore has not been possible.

Issues/options

6.16 This issue was first raised with ASIC in 2002. On 18 March 2002, ASIC wrote to subscriber industry associations expressing the view that:

> *While identification by merchant name is preferable for the purposes of Clause 4.1(b)(v) compliance, identification by biller identification number is also sufficient for compliance, subject to one condition. The condition is that the merchant must ensure that the merchant's invoice to the customer account user clearly sets out both the merchant's name and the biller identification number …*

6.17 We adopted this approach on the basis that:

> *The policy objective underlying Clause 4.1(b)(v) is clearly to ensure that the user is able to confirm the identity of the organisation to which payment is made. This objective will continue to be achieved where identification is by way of biller identification number rather than merchant name, as long as both the merchant's name and the biller identification number are provided on the invoice to which the user may make reference when paying the account.*

6.18 This approach could be reflected explicitly in the wording of the EFT Code. For example, the phrase 'or biller identification number' might be included following 'name' in cl 4.1(b)(v).[119]

Your feedback

Q15 Should cl 4.1(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?

[118] This problem does not arise where payment is made online.

[119] We understand that merchants offering BPAY facilities must provide their biller number on all invoices, and assume that a similar requirement is imposed on merchant participants by other bill payment services.

When a transaction receipt should disclose remaining balance (cl 4.1)

6.19 Clause 4.1(a)(viii) obliges the account institution to state on the receipt the balance remaining after the transaction when possible, and when 'this is not likely to compromise the privacy or security of the user or the account holder'. Endnote 12 suggests, by way of example, that 'privacy and security concerns may preclude providing balance information at EFTPOS terminals but not at ATMs'.

Issues/options

6.20 Some industry representatives have indicated that additional guidance is needed about disclosing remaining balances.

Your feedback

Q16 Should the EFT Code give more guidance on cl 4.1(a)(viii) regarding balance disclosure on receipts? If so, what guidance should be added?

Consistency between Part A and Corporations Act (cl 2–4)

6.21 Industry representatives have previously raised issues of duplication and inconsistency between the EFT Code and the product disclosure and related requirements of *Chapter 7—Financial Services and Markets* of the Corporations Act: see Table 8.

6.22 The primary role of financial services sector codes is to raise standards and complement existing legislative requirements. In ASIC's view, an effective code should do at least one of the following:

(a) address specific industry issues and consumer problems not covered by legislation;

(b) elaborate upon legislation to deliver additional benefits to consumers; and/or

(c) clarify what needs to be done from the perspective of a particular industry or practice or product to comply with legislation.[120]

[120] See Policy Statement 183 *Approval of financial services codes of conduct* at [PS 183.5]. We believe these principles are generally applicable, not just for codes approved under [PS 183]. (The EFT Code is not an approved code under [PS 183].)

Table 8: Product disclosure and related obligations under the Corporations Act

Initial disclosure[121]	Retail clients to whom a financial product is recommended, issued or sold must generally be given a product disclosure statement (PDS) setting out the main features of the product.
Ongoing/ additional disclosure[122]	Supplementary PDS requirements apply in certain circumstances (e.g. to update or add to information in the PDS). There are also obligations to give the client additional information on request, and in certain circumstances to notify the holder of 'significant changes and material events'.
Transaction confirmation[123]	Retail clients must generally be provided with confirmation of their transactions. This must 'give the holder the information that the responsible person believes the holder needs (having regard to the information the holder has received before the transaction) to understand the nature of the transaction'. The confirmation must include the identities of the parties, the date, a description of the transaction, any amount paid or payable by the holder, and other matters. However, amounts debited or credited to a basic deposit product need not be confirmed if a periodic statement (see next point) is provided within 6 months.
Provision of periodic statements[124]	Retail client holders of financial products that have an investment component (including deposit products) must also generally be given periodic statements at least every 12 months. Statements must give the holder 'the information that the issuer reasonably believes the holder needs to understand his or her investment in the financial product'. Statements must also include specific prescribed information (e.g. opening and closing balances, details of transactions) to the extent relevant.

Is there unnecessary duplication between the EFT Code and Corporations Act?

6.23 There is a degree of overlap between the coverage of the Corporations Act and the EFT Code. The Code *both*:

(a) regulates facilities that are also regulated under the law. Thus, unless they are credit facilities (such as credit card accounts), Part A *EFT accounts* will generally fall within the definitions (referred to in paragraph 4.3 above) of a deposit-taking facility and a NCP

[121] Part 7.9, Div 2, Corporations Act generally; s1013D sets out main content requirements of PDS

[122] Part 7.9, Div. 2, Subdiv D, Corporations Act.

[123] Section 1017F (Confirming transaction), s1017F(7) and (8), Corporations Act; and reg 7.9.61D–7.9.63I, 7.9.62(3)(c) and (d), Regulations. For definition of 'basic deposit product', see s761A, Corporations Act.

[124] Section 1017D (Periodic statements for retail clients for financial products that have an investment component) and s1017D(4) and (5), Corporations Act. See also reg 7.9.71–7.9.75D and 7.9.60B, Regulations.

facility under the Act,[125] while Part B *stored value facilities* will generally fall within the definition of a NCP; *and*

(b) includes product disclosure and related requirements broadly similar to those prescribed under the Act—namely, the provisions of the EFT Code covering availability and disclosure of terms and conditions,[126] changing terms and conditions,[127] records of transactions/available balance[128] and the provision of periodic statements.[129]

6.24 This raises the question of whether these EFT Code requirements constitute unnecessary duplication given the existence of the legal framework. This question is addressed in Section 9 in connection with Part B facilities.

6.25 As far as Part A is concerned, as a result of recent amendments to the Act discussed in paragraphs 4.5 – 4.6 above, the product disclosure statement requirements (referred to in Table 8) no longer apply to *basic deposit products* (BDP) and related NCP facilities, subject to certain limited information disclosures being made in some form.[130]

6.26 Given this development, it would seem that duplication under the EFT Code about disclosing terms and conditions and changes to terms and conditions for these products is no longer an issue. Any potential question of overlapping regulatory requirements would seem to arise only in the limited circumstances when a transaction credits or debits an EFT account under the Code that is not also a BDP under the Corporations Act.

6.27 Further, the EFT Code gives a higher level of protection than the Corporations Act in the areas of transaction confirmation and periodic statements. Under the Act, issuers are exempt from confirming transactions

---

[125] Credit facilities are not a financial product under the Corporations Act: s765A(1)(h). Primary responsibility for credit regulation lies with the States and Territories. The Uniform Consumer Credit Code is the primary legislative instrument regulating consumer credit: see at www.creditcode.gov.au.

[126] Clause 2 (Availability and disclosure of terms and conditions applicable to EFT transactions); cl 12 (Availability and disclosure of information and terms and conditions applicable to stored value facilities)

[127] Clause 3 (Changing terms and conditions of use); cl 13 (Changing the terms and conditions of use)

[128] Clause 4A (Records of EFT transactions and notices of surcharges—Receipts); cl 14 (Record of available balance)

[129] Clause 4B (Records of EFT transactions and notices of surcharges—Periodic statements)

[130] Regulation 7.9.07FA, inserted by *Corporations Amendment Regulations 2005 (No 5*) The amendments also remove also remove supplementary PDS requirements (s1016E) and some other related obligations, including the obligation to give additional advice on request (s1017A) and the obligation to notify the client of material changes and significant events (s1017B).

for amounts debited or credited to a BDP if they give periodic statements at least every 6 months.[131] However, under the EFT Code:

(a) receipts must be given for all regulated EFT transactions;[132] and

(b) in the case of periodic statements (except for passport accounts), a record of account activity must be given at least every 6 months (not every 12 months, as under the Act).

6.28 In other words, in these respects the EFT Code goes beyond and does not merely duplicate the Corporations Act.

Are there aspects of the EFT Code that are inconsistent with the legal framework?

6.29 As noted, issues of consistency have also been raised, although not in any very specific way. In general, ASIC takes the following approach to consistency between industry codes and the law:

> *While a code must do more than restate the law (and should offer consumers benefits that exist beyond the protection afforded by the law), it must not be inconsistent with the Act or other relevant Commonwealth law for which ASIC is responsible. For example, where compliance with a code provision would make it impossible to comply with the law, then we will generally take the view that the code provision is inconsistent with the law.*
>
> *In some cases, a code may provide for a higher standard of conduct or practice than that required by legislation. For example, a code provision may specify a longer cooling off period, a shorter response time, or more prescriptive pre-contractual disclosure than is otherwise provided for in the legislation. As long as compliance with the code provision would not make it impossible to comply with the law, then we will generally take the view that there is no inconsistency.*[133]

6.30 Our preliminary assessment is that none of the Part A requirements of the EFT Code is inconsistent with the law, in the sense set out in the previous paragraph. The fact that the EFT Code may impose obligations on the subscriber additional to what the law requires (e.g. the transaction receipt and periodic statement requirements) is not in itself problematic. Indeed, it is unclear what value a code that merely replicated the law would have.

[131] Regulation 7.9.62(3) (c) and (d), Regulations.
[132] Clauses 4.1 and 4.2 of the EFT Code.
[133] See Policy Statement 183 *Approval of financial services codes of conduct* [PS 183) at [PS 183.28]–[PS 183.29]. As noted earlier, we believe these principles are generally applicable, not just for codes approved under [PS 183].

6.31 However, we are interested in any examples of inconsistency or incompatibility of which you are aware.[134]

Your feedback

Q17 Is there duplication or inconsistency between Part A of the EFT Code and the requirements of the Corporations Act that should be reviewed? How should any such issues be dealt with?

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

6.32 The question has been raised as to whether the EFT Code should, by analogy with s1013D(1)(c) of the Corporations Act,[135] impose an obligation on subscribers under cl 2.3 to provide information about significant risks associated with an access method before the access method is used for the first time.

6.33 It is suggested that a minimum level of information about online fraud risks (discussed in Section 3) might be made compulsory.

Your feedback

Q18 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?

Obligation to advise account holder of discrepancies (cl 7)

6.34 Clause 7.1 imposes an obligation on account institutions to tell account holders of discrepancies between amounts recorded by electronic equipment or an access method as having been deposited to an account and amounts recorded as received.

Issues/options

6.35 Clause 7.1 has been criticised for the minimalist character of the obligations it imposes. It has been suggested that, '[s]ince the account institution generally is responsible for the provision of the access method

[134] The law would, of course, prevail over the EFT Code to the extent of any inconsistency; however, it is obviously desirable to avoid inconsistency where possible.
[135] Under s1013D(1)(c), a product disclosure statement must include such 'information about any significant risks associated with holding the product' as a person would reasonably require for the purpose of making a decision as a retail client, whether to acquire the product.

and for the equipment, there should be some obligation for [the account institution] to identify the source of the error and to correct it'.[136]

6.36 The provision has also been criticised for its use of 'the language of "deposits"'. It is suggested that the term 'deposit', while of uncertain scope, 'is probably limited to something like indebtedness through a current or term account'.[137] Given this, it is not clear whether, for example, a transfer initiated by a third party to the user's account would be covered.

6.37 Clause 7.1 might be amended to clarify these issues as follows. (Substantive changes to the wording are underlined):

> *Where, in relation to an EFT transaction that is a transfer for the credit of an account, there is a discrepancy between the amount recorded by the electronic equipment or access method as having been transferred and the amount recorded by the account institution as having been received, the account institution will:*
>
> *(a) notify the account holder of the disparity as soon as possible,*
>
> *(b) advise the account holder of the amount that has been credited to the nominated account, and*
>
> *(c) take action to identify the source of the error and to correct it.*

Your feedback

Q19 Should cl 7 be revised to specifically require subscribing institutions to identify and correct discrepancies between amounts recorded on the user's electronic equipment or access method as transferred, and amounts recorded by the institution as received? What are your views on the suggested redrafting?

What is a 'complaint'? (cl 10)

6.38 The EFT Code monitoring processes (discussed in Section 11 below) require that subscribers report on the number of complaints they receive.

6.39 The term 'complaint' is not currently defined in the EFT Code itself.[138] Clause 10.3 implies that an issue/enquiry/concern raised by an

[136] Tyree, footnote 107 above, at p. 354

[137] See footnote above. 'Indebtedness' here refers to indebtedness of the financial institution to its customer.

[138] However, it is defined in AS4269–1995, the standard for complaints handling to which EFT Code subscribers are committed. See further below in this section.

account user may be a complaint even though it is 'immediately settled to the satisfaction of both user and account institution'.

Issues/options

6.40 It has been queried whether this is true for all such communications. For example, industry representatives have queried whether a request for further information about a transaction the user is unsure of should automatically qualify as a complaint for the purposes of the EFT Code.

6.41 Another example given is when an account institution identifies a possible electronic fraud and advises the account holder of its concerns. The account holder confirms that the transaction is unauthorised, and the account institution adjusts the account. There has been no complaint or disagreement, as ordinarily understood, between the parties. Should this interaction count as a complaint for the purposes of the EFT Code?

6.42 Clause 10.1 obliges subscribing account institutions to 'establish internal complaint handling procedures which comply with Australian Standard AS 4269–1995 or any other industry dispute resolution standard or guideline which ASIC declares to apply to this clause'.[139]

6.43 AS 4269–1995 defines a complaint as 'any expression of dissatisfaction with a product or service offered or provided'.[140] AS 4269–1995 was superseded by AS ISO 10002–2006 (published 5 April 2006).[141] AS ISO 10002–2006 defines a complaint as an 'expression of dissatisfaction made to an organisation, related to its products, or the complaints-handling process itself, where a response or resolution is explicitly or implicitly expected'.[142]

6.44 The EFT Code could include a definition of a complaint replicating, or based on, the AS ISO 10002–2006 definition (see also the next sub-section in this context.) A further option might be to include some commentary or examples in the Endnotes.

---

[139] *Australian Standard—Complaints Handing (AS 4269–1995)*; Available from the Standards Australia website: www.standards.org.au.
[140] See footnote above, Section 1—Definitions, p. 4.
[141] *Australian Standard— Customer satisfaction—guidelines for complaints handling in organizations* (ISO 10002:2006, MOD); Available from the Standards Australia website: www.standards.org.au.
[142] See footnote above, 3—Terms and definitions, p. 2.

Your feedback

Q20 Should the EFT Code include a definition of the term 'complaint' under cl 10? If so, should it adopt the definition in AS ISO 10002–2006? 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?

Standard for internal complaint handling

6.45 As noted before, a new Australian Standard (AS ISO 10002–2006) recently superseded AS4269–1995, the current complaints handling standard required by the EFT Code. It is proposed that this new standard should replace AS4269–1995 as the required standard for internal complaint handling under the EFT Code.

Your feedback

Q21 Should AS ISO 10002—2006 become the required standard for internal complaint handling under the EFT Code?

Meaning of 'immediately settled' complaint (cl 10.3)

6.46 Clause 10.3 requires account institutions to give written advice about how they investigate and handle a complaint unless the complaint is 'immediately settled to the satisfaction of both user and account institution'.[143]

Issues/options

6.47 Industry representatives have queried the meaning of 'immediately settled'. They have suggested that the clause should be changed to allow for a brief time in which the account institution can look into the complaint before any advice on complaint handling procedures must be sent. If the matter was settled to the satisfaction of the parties within the permitted brief period, the information would not need to be sent.

Your feedback

Q22 Should account institutions be given a brief period within which to investigate a complaint before they must give the complainant written

[143] See also final paragraph of cl 10.9. There is a typographical error in this paragraph: 'receives' should read 'resolves'.

advice on how they investigate and handle complaints (as required under cl 10.3)? If so, what is an appropriate period?

Timeframes for resolving complaints (cl 10.5)

6.48 Clause 10.5 specifies 45 days from the date of receipt as the maximum time within which a complaint should be investigated, unless there are 'exceptional circumstances'. Endnote 23 gives 'delays caused by foreign account institutions or foreign merchants being involved in resolving the complaint' as examples of possible exceptional circumstances for the purposes of cl 10.5.

Issues/options

6.49 Some industry representatives have suggested that 45 days will often be too short a time for resolving complaints given, in particular, that most complaints will involve more than one account institution. We are advised that, in these circumstances, it may take some weeks for the institution investigating its customer's complaint to obtain information about the transaction from the merchant's account institution, which in turn may need to obtain information from the merchant. This situation is exacerbated when the transaction involves an overseas account institution. (However, this last point is at least partly addressed by Endnote 23).

6.50 Against this, consumer representatives, and individual consumers who have contacted ASIC, have noted that delays in resolving EFT complaints can mean embarrassment and/or financial hardship for the account user/holder. It has been suggested that, rather than not long enough, up to 45 days is too long in general for the consumer to have to wait for their complaint to be resolved.

6.51 In this context, comparisons are made with the card scheme chargeback rules which largely avoid disadvantaging consumers by charging back disputed amounts while the cardholder's claim is investigated. It is also noted that the 21-day/45-day timeframes are well established. They are adopted, for example, by both the Code of Banking Practice[144] and ASIC Policy Statement 165 *Licensing: Internal and external dispute resolution* [PS 165].[145]

---

[144] Clause 35 of the CBP.

[145] The Schedule to [PS 165] includes this guidance under *Responsiveness* at p. 26:

> *As a general rule, you should aim to respond to a complaint as soon as possible, and where the complaint is not resolved at the time of complaint, you should acknowledge the complaint promptly. ASIC considers that you should substantially respond to a complaint within a maximum of 45 days, but in a shorter period if possible. If you cannot respond to the complainant within 45 days, you should inform the complainant of the reasons for the delay and of their right to refer the matter to the relevant EDR scheme.*

6.52 One option for addressing the competing interests associated with this issue might be not to change the current timeframe, but to amend the EFT Code to require subscribers to respond as far as possible within a specified time to requests for information made by a complainant's authorising institution. (An appropriate time would need to be decided.) Arguably, this could assist the account institution to which the complaint was made to respond within the time limit.

Your feedback

Q23 Should any changes be made to the timeframe for resolving complaints under cl 10 of the EFT Code?

Internal complaints handling

6.53 Consumer representatives have expressed ongoing concerns about what they see as variable levels of compliance with cl 10 among subscribers. The most recent compliance report[146] on the EFT Code also identifies compliance breaches by some account institutions including:

(a) failing to tell complainants about the 45-day timeframe under cl 10.6;

(b) failing to suspend the account holder's obligation to pay under cl 10.7(c)(ii); and

(c) failing to tell complainants of their right to refer a complaint to the member's EDR scheme within 5 days of that right becoming available to them under cl 10.8.[147]

6.54 The regime set out in cl 10.12, introduced after the last review of the EFT Code, was intended to address compliance concerns by giving 'an incentive to institutions to implement good investigation and decision making procedures in accordance with the Code and to compensate account holders for the effects of prejudicial decisions or delays'.[148]

Your feedback

Q24 Do you have information or views about the level of compliance with cl 10?

[146] See *Compliance with EFT Code of Conduct for the period April 2003–March 2004, ASIC Report*, December 2005. Follow links from review website at www.asic.gov.au/eftreview

[147] See footnote above, pp. 13–14.

[148] See Endnote 24 to the EFT Code.

Q25 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?

Investigating complaints and availability of records

Issues/options

6.55 Dispute resolution bodies sometimes find it difficult to get from account institutions the transaction records and other information they need to decide an EFT dispute.

6.56 Sometimes subscribers are unable to supply a record relating to a dispute covered by the EFT Code within a defined time (or alternatively, within a 'reasonable period'). It has been suggested that when this happens the Code should allow a dispute resolution body to resolve a factual issue to which the record relates on the basis of the evidence available to it (including evidence provided by the complainant).

Your feedback

Q26 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 a dispute resolution body is entitled to resolve a factual issue to which a record relates on the basis of the evidence available to it?

Time limit on resolution of complaints under the EFT Code

Issues/options

6.57 Currently, account institutions are prohibited from seeking 'to restrict or deny account holders their rights to make claims or to attempt to impose time limits on users to detect errors or unauthorised transactions' (cl 4.4).

6.58 Some industry representatives have suggested that the EFT Code should permit subscribing institutions to limit the period of time during which they would be required to resolve unauthorised transaction and other disputes on the basis set out in the Code.[149] On this view, as we understand it, the Code would specify a minimum period during which disputes would have to be determined in accordance with its requirements. After this, the subscribing institution would be free to

[149] Liability in cases of unauthorised transactions is discussed in Section 7.

allocate liability contractually (i.e. in its terms and conditions) on a different basis if it chose to do so.

6.59 Periodic statements must be provided at least every 6 months under the EFT Code (cl 4.2(a)). Presumably, as disputed transactions are often not identified until the account holder receives their statements, any minimum period of Code coverage under this proposal would need at least to be longer than 6 months.

6.60 More generally, from a consumer perspective the proposal would significantly reduce the protection account holders currently get under the EFT Code. It would also add considerably to the complexity of the Code and its administration by allowing multiple regimes governing liability allocation top develop.

Your feedback

Q27 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?

Section 7: EFT Code, Part A (Liability; mistaken payments)

The detailed regime for allocating liability for alleged unauthorised transactions set out in cl 5 has been central to the EFT Code's regulatory role since it first came into force. The regime has always been a scrutinised area of the Code, and it continues to be so.

In particular, the question has arisen of whether the regime should be adjusted in light of the growth of online fraud directed at individual users and their equipment. This and other issues about liability allocation are considered in this section. This section also covers cl 6.

In addition, the section deals with the issue of whether mistaken payments should be regulated under the EFT Code.

Current liabilities for unauthorised transactions (cl 5)

7.1 An unauthorised transaction profits the fraudster and leaves a loss (that often cannot be recovered) to be distributed between generally innocent parties—the account institution, the user, and perhaps other parties to the payment system or network. In these circumstances, who should pay? Under the cl 5 regime, unauthorised transaction losses are allocated to either the account holder or the account institution depending on the circumstances. The regime establishes three liability scenarios.

Liability scenario 1: Account holder has no liability

7.2 In this scenario, the account holder has no liability. It is borne in full by the account institution. These circumstances are set out in cl 5.2–5.4. In summary, there is no account holder liability for losses:

(a) caused by the fraudulent or negligent conduct of employees or agents of the institution, another party in the payments network, or a merchant;

(b) relating to any component of an access method that is 'forged, faulty, expired or cancelled';

(c) occurring before the user's receipt of the access method;

(d) caused by the same transaction being incorrectly debited more than once to the same account;

(e) occurring after the account institution has been notified of the compromise of the access method or misuse, loss or theft of the device; or

(f) in any other circumstances, where 'it is clear that the user has not contributed to such losses'.

Liability scenario 2: Account holder is liable

7.3 A second scenario is when the account holder is liable for the losses. These circumstances are set out in cl 5.5 and 5.6. Liability will occur when the account institution can prove, on the balance of probability, that the account user:

(a) acted fraudulently;

(b) contravened one or more of the requirements in cl 5.6 about the handling of access codes; or[150]

(c) unreasonably delayed notifying the loss or theft of the user's device or breach of security codes.

7.4 The account user's action or failure to notify must contribute to the loss. However, the account holder's liability in these circumstances cannot be more than daily or other periodic transaction limits on the account, or the account balance (including any available credit). In addition, the account holder is not liable for any amount accessed using an access method not agreed to by the parties.

Liability scenario 3: Other circumstances

7.5 The third scenario applies in all other circumstances. In such circumstances (e.g. when it cannot be proved that the account user breached code security requirements), liability is allocated on a 'no fault' basis, with up to $150 of the loss being allocated to the account user,[151] and the rest to the account institution.

7.6 Clause 5 also deals with:

(a) notification facilities by the account institution (cl 5.9);

(b) procedures for acknowledging the notification of loss, theft or unauthorised use (cl 5.10);

(c) the relation between the EFT Code's unauthorised transaction regime and the card schemes' chargeback rules (cl 5.11); and

(d) account institutions' and external dispute resolution bodies' discretion to reduce account holder liability for losses in the absence of reasonable daily or other periodic transaction limits protection (cl 5.12).

---

[150] This means the account holder is liable if they:
(a) voluntarily disclosed an access code to a third party;
(b) recorded an undisguised code on a card or other device, recorded an undisguised code on other articles liable to loss or theft in certain circumstances;
(c) used certain easily guessed alphanumeric codes despite being warned not to do so; or
(d) acted 'with extreme carelessness in failing to protect the security of all the codes'.

[151] More specifically, the account holder will be liable for the least of:
(a) $150 (or such lower figure as may be determined by the account institution);
(b) the balance of the defrauded account(s), including any pre-arranged credit; or
(c) the actual loss at the time the account institution is notified (where relevant): cl 5.5(c).

Historical and comparative perspective

7.7 The cl 5 regime controls the capacity of subscribing financial institutions to allocate liability for unauthorised transactions contractually (i.e. through the terms and conditions for the facility or service).

7.8 This has been the essential approach of the EFT Code since its predecessor was released in 1986. *Discussion Paper on an expanded EFT Code of Conduct*, released by ASIC's EFT Working Group in 1999, includes a valuable historical overview of the development of the regime, explaining why this approach was adopted.[152]

7.9 The approach taken in Australia is not unique. Appendix A summarises the equivalent regimes (whether established as laws or industry codes or a combination) in comparable jurisdictions. As this material indicates, there is a general assumption that intervention to prescribe the way liability is allocated is appropriate, although the degree of prescription varies.

Policy considerations

7.10 Two guiding principles were seen as providing the policy rationale for changes made to the unauthorised transaction regime at the last review. The first of these principles, based in economic efficiency considerations, was a 'least cost avoider' principle. This was described as follows in the Review Discussion Paper (July 1999):[153]

> *…[B]oth users and account institutions can take action to reduce losses—the user by reasonably safeguarding the access method for accessing the account, and the account institution by maintaining and improving the reliability and the security of the access method to reduce the scope for unauthorised transactions to occur.*
>
> *An economically efficient loss allocation rule would therefore assign liability:*
>
> - *To the [account holder] where there has been a failure by the user to reasonably safeguard the access method. (The precise terms of this liability will take account of the nature, strengths and weaknesses of the access method approved by the account institution.) This will encourage users to safeguard the access method; and*
> - *In other cases, to the account institution to encourage it to improve the security of the access method and EFT system over time.*

[152] See *Historical perspective on fair allocation of unauthorised transaction losses* at pp. 26–30. To access this paper, follow links from review website at www.asic.gov.au/eftreview
[153] Ibid at p.28-29

7.11 The second principle relied on in the context of the last review was a principle of simplicity—that liability allocation rules should be simple, clear and decisive so as to minimise the costs of administering them. In relation to this principle, the Review Discussion Paper stated:[154]

This principle suggests that:

- *A no-fault allocation system is better than one that requires the evaluation of fault; and*
- *If a fault-based system is used, the obligations on parties should be clear and specific so that a breach of those obligations can be easily determined with little cost. This suggests that broad standards such as 'the user takes all reasonable steps to keep the access method safe' are less appropriate than specific standards. They are less appropriate because broad standards involve significant judgment and argument as to their interpretation in particular cases. This is expensive and time consuming.*

7.12 We consider these principles to be of ongoing relevance for the current review, and make further reference to them below.

Online fraud and liability allocation

7.13 Section 3, *Growth in online fraud*, is an overview of online fraud techniques, as well as measures that have been and are being developed to counter the online fraud threat. Familiarity with the material in Section 3 is assumed in the comments that follow.

7.14 At the time of the last review, neither the involvement of sophisticated criminal networks in online fraud, nor the specific techniques used to perpetuate it, had emerged to any extent. Nonetheless, the drafters of the current EFT Code were well aware of the relative insecurity of the internet as a payments channel, and the associated potential for fraud; and they structured the current liability allocation regime with this in mind.

7.15 As the summary above indicates, the current regime imposes the main burden of liability on the account institution, unless fraud or one of a limited number of types of carelessness with access codes can be established. This approach was favoured on the basis, principally, that an account institution rather than its customers collectively is generally better placed to reduce system insecurity at the lowest cost overall if it chooses to do so—in other words, it is generally the 'least cost avoider', referred to in the previous sub-section.

[154] ibid

7.16 While the regime imposes the main regulatory burden on the account institution, it nonetheless also gives account users an incentive to take reasonable steps to protect the security of their codes in circumstances other than those set out in cl 5.6, including in the online environment—namely, the potential loss of the 'no fault' threshold amount up to $150.

7.17 Despite this some industry representatives want to re-examine how liability for unauthorised transactions is allocated in cl 5 in light of the growth of fraud in the online environment. In general, they argue that:

(a) account users need to do more to reduce the risks and losses associated with online fraud, and

(b) the EFT Code's liability allocation regime should be adjusted to increase the regulatory incentives on users to do so.

Their views, and responses to them, are discussed in this section.

7.18 The questions of liability for losses resulting from the vulnerability of users' equipment to malicious code, and liability for losses resulting from deceptive phishing attacks are distinct. Therefore they are considered separately.

Liability for losses resulting from vulnerability of user's equipment

Proposal to extend account holder liability for equipment

7.19 It is generally agreed that the insecurity of end-user equipment is a major source of vulnerability to malicious software installation, and that a properly secured PC or other equipment is one of the best defences currently available against malicious code installation. Nonetheless, research suggests that many online transactors do not adequately protect their equipment.[155]

7.20 Given this, some industry representatives have proposed that users could potentially be made liable under the EFT Code for the full amount of losses from malicious code compromises of account access data unless they have 'minimum' (or sometimes 'adequate') equipment security.

Issues/options

7.21 This proposal raises a number of significant issues about the relative benefits and costs of extending account holder liability for losses resulting from user equipment insecurity: see Table 9.

[155] This issue is discussed in Section 3, under *Protective measures adopted by online users* (paragraphs 3.27 – 3.29)

Table 9: Implications of extending account holder liability for equipment

Potential impact on consumer confidence	It is generally agreed that, despite accelerating levels of take-up in recent years, users' confidence in the online environment is relatively fragile, with security concerns growing as the threat from (and publicity given to) online fraud exploits has grown.[156] A shifting of liability to the consumer may impact negatively on confidence in, and with this use of, the online channel.
Potential impact on development of other fraud countermeasures	Arguably, the only effective long-term solution to malicious code-related fraud is to make the online channel more secure independently of end users. However, implementing enhanced online security measures such as two-factor authentication (and other measures of the kind outlined in Section 3) involves account institutions in significant costs. Arguably, a shifting of liability as proposed may reduce the incentives for institutions to make necessary investments in security by effectively allowing them to externalise the risks associated with unauthorised transaction losses (including the risk of large-scale losses). As noted in paragraph 7.10, this was the key policy consideration behind the approach of the current regime.
Complexity/cost of administration	A rule making account holders liable for losses resulting from breaches of equipment security standards would add considerably to the complexity and cost of the regime. Again, this was a key consideration behind the current approach (see paragraph 7.11 above). For example, before an unauthorised transaction loss could be attributed to user equipment insecurity, certain technical and causal issues would need to be resolved by the determining entity (whether account institution staff, IDR process, or EDR process). These include deciding: • whether the user's security was in fact below the mandated standard; whether a compromise of the user's access code(s) occurred as a result of the sub-standard security (rather than some other security failing for which the user was not responsible); and • whether this compromise contributed to the unauthorised transfer.
Potential for misattribution of cause of loss	Given this last-mentioned complexity, there would be potential for unauthorised transaction losses to be misattributed to the insecurity of the end user's equipment, as distinct from some other security failing for which the user was not responsible. In most circumstances, users would not be in a position to challenge the legitimacy of an attribution themselves. They would either simply have to accept the explanation they were given by their account institution on

[156] This issue is discussed in Section 3, under *Impact of internet fraud on online user confidence* (paragraphs 3.23 – 3.26)

	trust, or attempt to have it assessed by an EDR scheme or other external adjudicator (which, in turn, would require the capacity to assess the causal issues under consideration).
Potential for harsh/unfair outcomes for account holders	Allocation of liability for losses to the account holder may produce harsh or unfair outcomes for account holders in circumstances when the account user either did not know about, or lacked the skills to implement and maintain, the minimum required security standards. As noted earlier, there is evidence suggesting that the ability of many online transactors to deal with security threats is currently quite limited.[157] There is also a question of cost to users to the extent that they are required to pay for anti-fraud software themselves. At a more general level, the fairness of shifting of liability to the account holder has also been questioned in the context of the active promotion of the internet as a transaction channel in recent years. In other words, through their fee structures and in other ways, institutions have sought to encourage their customers to do their banking on the internet, rather than over the counter; and they have reaped considerable benefits from the increasing use of this low cost distribution channel as a result. Consumer representatives and others have asked whether, given this, it is fair that industry should now be able to shift risks/costs associated with that strategy to the customer.
Response may be premature	Malicious software attacks are still a relatively recent phenomenon. Arguably, consumer understanding of the threat they represent, and what needs to be done in terms of security to reduce its impact, takes time to develop across the community as a whole. Given this, it has been suggested that, although a regulatory response may be appropriate at some point in the future, such a response is premature at this stage.

Your feedback

Q28 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 issues would have to be addressed?

[157] This issue is discussed in Section 3 under *User capacity to reduce online threats* (paragraphs 3.30 – 3.31)

Liability for losses resulting from deceptive phishing attacks

Proposal to extend account holder liability for phishing

7.22 Deceptive phishing attacks have been a ubiquitous feature of the online environment for the last few years. Despite the increasing publicity they have received and efforts by business, government and other stakeholders to warn online users against responding to phishers' calls to action, people continue to do so in significant numbers.

Issues/options

7.23 Some industry representatives have suggested that, as with the malicious software situation, this situation could be addressed in part through the regulatory structure of the EFT Code. It is contended that, if account holders were potentially exposed to the full amount of losses resulting from a successful deception-based attack, at least some users would be induced not to respond to criminals' lures.

7.24 A particular concern appears to be with users who respond on more than one occasion. According to industry representatives, some users (how many is not clear) continue to give their account details in response to deception-based attacks, despite specific warnings after an initial attack. It is unfair and unreasonable, it is argued, for the account institution to absorb losses resulting from these subsequent attacks, in particular.

7.25 On this specific point, we note the following:

(a) The account institution always has the option of discontinuing the user's right to access their account online.

(b) In some cases of this kind, the user's conduct could be characterised as a contravention of cl 5.6(e). Under this provision, the account holder is liable where 'the user acts with extreme carelessness in failing to protect the security of all the codes'. However, the circumstances of each particular case would need to be considered.

7.26 Most of the issues raised in connection with liability for losses resulting from vulnerability of user's equipment (see earlier issue) would also appear to be relevant in the deceptive phishing attack context.

7.27 Whether the potential impact on consumer confidence of a shift in liability would be as significant an issue may be open to doubt—arguably, many users would be more confident of their ability to refrain from responding to phishing lures than of their ability to install and maintain online security software.

7.28 A fundamental question, however, is whether imposing increased regulatory responsibility on account holders would be effective in modifying conduct (as opposed to merely shifting liability).

Well-resourced criminals know how to manipulate people's anxieties, including their habits of deference to (apparent) authority, and they are frequently able to create convincing copies of legitimate websites.

7.29 As noted above, research suggests that large numbers of consumer continue to be taken in. Given the essentially non-voluntary character of the user's response to a deception-based attack (i.e. the user is tricked), would a regulatory incentive in fact work in modifying conduct?

7.30 Other issues would also need to be addressed in the context of any proposal to extend account holder liability in deceptive phishing cases. One of these is subscribing institutions' own online communication practices. Clearly, for example, it is no longer acceptable for institutions to ask their customers to provide account number or PIN or password details in unsolicited emails (and, neither, arguably, is the inclusion of hyperlinks in emails). Indeed, we understand that some in the IT security community consider that email itself is now so compromised as an institution-to-customer communication channel that it should no longer be used.

7.31 Another issue that would need to be addressed is the extent and effectiveness of account institutions' efforts to warn users about online phishing.

Your feedback

Q29 Should an additional example be included in cl 5.6(e) specifically referring to the situation when an account user acts with extreme carelessness in responding to a deceptive *phishing* attack?

Q30 Apart from this possible clarification, should account holders be exposed to any additional liability under cl 5 for unauthorised transaction 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?

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

Experience of cl 5.6(d) contravention

7.32 Clause 5.6(d) creates a restriction on the user self-selecting codes based on their name or birth date. It was introduced after the last review of the EFT Code in response to industry concern that the use of easily guessed codes assisted criminal activity.

7.33 At the time, there was some doubt about how the provision would operate from a consumer perspective. We are interested in receiving

information on the extent to which account institutions have relied on this provision, and consumer representatives' experience of its operation.

Your feedback

Q31 To what extent has the restriction on using a user's name or birth date under cl 5.6(d), been relied on?

Scope and certainty of cl 5.6(e)

7.34 Clause 5.6(e) makes the account holder liable if they 'act[s] with extreme carelessness in failing to protect the security of all the codes'. This clause was inserted after the last review. The Working Group commented as follows on the decision to include the provision:

> *In order to avoid a protracted and probably unfruitful debate on additional specific content in sub-clause 5.6, the Working Group has adopted [sub-clause 5.6(e)]. It is recognised that introducing a general standard of 'extreme carelessness' introduces scope for interpretation and argument and therefore raises transaction costs. However, given that agreement among stakeholders of additional specific prohibitions in sub-clause 5.6 is very unlikely, the Working Group considered that paragraph (e) provides a reasonable balance of the interests of account institutions and users by providing a flexible catch all for the future. Account institutions are given the flexibility to prove user contribution to unauthorised transaction losses in different ways in the future but users are given the comfort that account institution's assessment of their conduct will be measured by external review agencies against a standard of 'extreme carelessness'.*[158]

Issues/options

7.35 Your views are sought on whether this approach should be reviewed in light of marketplace and consumer experience since the last review.

7.36 For example, the possibility of the EFT Code including additional examples (apart from that given in Endnote 17) has been raised. It has also been suggested that consideration be given to extending the circumstances in which 'extreme carelessness' by the user would trigger a liability shift (i.e. apart from extreme carelessness in 'failing to protect the security of all codes').

[158] *Second Draft Expanded EFT Code of Conduct and Commentary (January 2000)* at p. 30. To access this paper, follow links from review website at www.asic.gov.au/eftreview

Your feedback

Q32 Should the restriction on users acting 'with extreme carelessness in failing to protect the security of all the codes' under cl 5.6(e) be further elaborated or extended in some way? Should additional examples of extreme carelessness be given?

Situation where card is left in ATM

7.37 Currently, the EFT Code does not specifically address the situation (which arises in practice) when a user leaves their card in an ATM machine and, before automatic shut down of access occurs, somebody undertakes a further (unauthorised) transaction using the user's card.

Issues/options

7.38 It has been suggested that this is the kind of situation when the EFT Code might specifically allocate liability to the account holder, subject to the ATM meeting acceptable minimum standards in terms of the time taken before automatic shut down (these would need to be defined).

7.39 We understand that this is now the approach generally taken by internal and external dispute resolution processes—so in effect the proposed change would largely codify the existing approach.

7.40 This approach is arguably justified on the basis that the ATM user is in the best position to mitigate loss by being careful.

Your feedback

Q33 Should the EFT Code specifically address the situation when an unauthorised transaction occurs after a user inadvertently leaves their card in an ATM machine?

Unreasonable delay in notification (cl 5.5(b))

'Card not present' transactions on the internet

7.41 Clause 5.5(b) sets out account holders' liability when they contribute to losses because they have unreasonably delayed telling the account institution after becoming aware:

(a) 'of the misuse, loss or theft of a device forming part of the access method'; or

(b) 'that the security of all the codes forming part of the access method has been breached'.

7.42 Unless one of these circumstances applies, there is no account holder liability for unreasonable delay in notification.

Issues/options

7.43 In the case of internet-based credit or scheme debit card transactions, however, it is doubtful whether either of the above-mentioned circumstances would ever apply. This is because the access method for internet-based card transactions is generally, simply, the keying-in of card number and expiry date identifiers (and possibly an additional second factor identifier) at a computer terminal. Arguably, this does not involve either:

(a) the use of a physical device (e.g. a card), in contrast to an ATM or EFTPOS transaction—in which case, the first cl 5.5(b) circumstance does not apply; or

(b) the use of (secret) codes, as distinct from (non-secret) identifiers—in which case, the second circumstance does not apply.

7.44 Arguably, account holder liability could be extended to include the situation when an account user unreasonably delays notifying the account institution of an online security breach of which the user has become aware.

A specific timeframe instead of 'unreasonable delay'

Issues/options

7.45 The question has also been raised of whether the standard of 'unreasonably delaying notification' under cl 5.5(b) might be replaced by a specific time limit. Thus, after the expiry of the proposed time limit, the account holder would be liable for any losses that could have been avoided by notification.

7.46 Because it does not involve issues of interpretation, this approach might be regarded as simpler and more cost-effective from an administrative perspective.

7.47 On the other hand, a specific time limit might be see as inappropriate given the range of circumstances that lead consumers to delay notifying their account institution of a security compromise. Such circumstances include:

(a) the frequency of use of the device;

(b) the frequency of receipt of account statements;

(c) how certain the user is that their device has been lost or security has been breached; and

(d) the fees and other costs associated with replacement.

7.48 Account holders often only become aware of a security breach after they receive their periodic account statement and discover an unauthorised transaction on the statement. Under the EFT Code, periodic statements must be provided at least every 6 months (cl 4.2(a)). Presumably, a specific time limit for unreasonable delay (if one were to be introduced) would need to be set by reference to this requirement.

Your feedback

Q34 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.)

Q35 Should the circumstances when the 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?

Q36 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?

'No fault' liability limit (cl 5.5(c))

7.49 Clause 5.5(c)(i) currently sets a threshold limit on account holder liability without proof of fault of the least of: $150 (or such lower figure as the account institution decides); the balance of the account (including any prearranged credit); *or*, the actual loss at the time of notification.

7.50 This figure was set after the last review, having regard to 'no fault' thresholds of laws and EFT industry codes in other jurisdictions.[159] The amount represented a significant increase on the previous no fault liability limit of $50, and was opposed by consumer representatives. However, the Working Group took the view that the increase was justified, particularly in the context of the clarification of the onus of proof under cl 5.5 and 5.6 in the amended EFT Code.

[159] See Appendix A below.

Issues/options

7.51 Industry representatives have suggested that the current 'no fault' threshold should again be increased, given the growth in EFT transactions and the efforts of account institutions to educate their customers about their obligations under the EFT Code.

7.52 Increasing the threshold has also been proposed as an alternative way of addressing the issues of risky online conduct and inadequate online user equipment security, discussed earlier in this section. In other words, instead of dealing with these issues by expanding the range of fault-based liability situations, it is suggested that increased regulatory pressure might be put on users to improve equipment security and avoid phishing lures via a higher 'no fault' penalty.

7.53 If the extent of any increase was limited, it is argued, the implications for consumer confidence may be less acute than if account holders were potentially liable for the full amount of unauthorised transaction losses as a result of online fraud. A no fault approach would also be significantly simpler (and therefore less costly) to administer.

7.54 From a consumer and welfare perspective any significant increase in the 'no fault' liability threshold is likely to be strenuously opposed on the basis that a 'no fault' impost operates regressively, hitting low income and disadvantaged consumers disproportionately hard.

7.55 As well as seeking your views on these issues, we are interested in learning more about how account institutions apply the current 'no fault' provision. Our understanding is that current practices vary widely as far as deducting the amount is concerned. We also understand that many institutions regard the customer-relations costs of deducting the amount as generally outweighing the benefits of doing so. (Individual institutions may prefer to give us this information on a confidential basis.)

7.56 Any increase in the amount of 'no fault' liability would arguably need to be balanced with other possible changes to the liability regime.

Your feedback

Q37 To what extent do subscribing institutions currently use the other 'no fault' liability provision in cl 5.5(c)?

Q38 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?

Liability allocation and 'book up'

7.57 'Book up' involves traders, such as general stores and taxi drivers, offering small amounts of short-term credit to customers, typically 'secured' by custody of a debit/credit card, together with being told their PIN. The trader is then able to recover the funds advanced from periodic payments to the customer's account, such as social security payments or wages. The practice of 'book up' is widespread in, but not confined to, remote Aboriginal communities.[160]

Issues/options

7.58 On occasions, customer's trust in a trader is abused, and more funds are deducted from their accounts than was advanced to them. However, because they voluntarily revealed their PIN, contrary to cl 5.6, liability for the unauthorised transaction (and therefore the burden of seeking to recover the funds from the trader) falls to the customer, not the account institution.

7.59 It has been suggested that consideration be given to including a provision in the EFT Code requiring subscribers to prohibit in their merchant agreements the practice of taking a customer's PIN or other access code as part of a 'book up' arrangement. Such a prohibition might be subject to specific exceptions covering, for example, people with disabilities.

Your feedback

Q39 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?

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

6.61 Clause 6.1 makes account institutions liable for losses arising from system malfunction when this causes the failure of a transaction that had been accepted by the system in accordance with the user's instructions. Clause 6.2 deals with consequential damage.

Issues/options

7.60 It has been suggested that the scope of cl 6.1 is unclear and, depending on how it is interpreted, potentially too restrictive.

7.61 This concern arises from the fact that the obligation is only imposed for loss caused by the failure of an 'institution system' or

[160] For more information on 'book up', see ASIC's *Dealing with book up*, available at: http://www.fido.asic.gov.au/fido/fido.nsf/byheadline/Indigenous?openDocument#3.

'institution equipment'. The EFT Code defines institution system as 'an electronic system, communications system or software controlled or provided *by or on behalf of* an account institution to facilitate EFT transactions'.[161] Institution equipment is defined as 'electronic equipment controlled or provided *by or on behalf of* an account institution to facilitate EFT transactions'.[162]

7.62 The concern raised goes to whether these definitions are sufficiently broad to cover systems and equipment owned or controlled by a third party (e.g. a 'foreign' ATM).

7.63 It is suggested that any doubt about scope could be rectified simply by making the account institution liable for any failure resulting from equipment used when they have agreed to accept instructions through that equipment.[163]

7.64 Our understanding is that the drafters' intention was always to cover third party equipment. The fact that the definitions refer to systems and equipment 'provided … on behalf of' the institution supports this.

7.65 The approach as clarified is clearly the preferable one, in our view. As between the institution and the account user, the former will generally be better placed both to decide how a malfunction occurred, and to seek an adjustment from a third party (that may not be a EFT Code subscriber) in appropriate cases.

Your feedback

Q40 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?

Mistaken payments

Issues/options

7.66 An effective consumer code of conduct needs to be responsive to identified and emerging consumer issues.

7.67 The issue of mistaken internet payments was identified in preliminary consultations as one that might potentially be dealt with under Part A of the EFT Code. At present, the EFT Code does not cover mistaken payments.

[161] These terms are defined in cl 1.5, *Interpretation*.
[162] Clause 1.5, emphasis added.
[163] Tyree, footnote 107 above, at p. 353–4

7.68 Contemporary internet banking permits 'pay anyone' direct credit payments to be made by account users. The payer is required to enter the intended recipient's account number on their account institution's internet banking screen. In most cases, the system also requires or permits entry of the payee's name. However, there is no process at either the payer account institution or receiver account institution end for checking the number against the name, nor are there other means of confirming the user has entered the right account number.

7.69 On occasions users mistakenly key in the wrong account number. This may happen when, for example, the payer inadvertently reverses two numbers, or enters the wrong number entirely (perhaps confusing two payees to whom they make payments). The funds are then transferred on the basis of the account number entered alone.

7.70 When the mistake comes to light (e.g. after the intended payee tells the payer that payment has not been received), there may be problems recovering the transferred funds from the unintended recipient. The payer may be told that, for reasons of confidentiality, the identity of the recipient cannot be revealed by the recipient bank.

7.71 In some cases, the recipient may resist repaying the money on the basis of the legal defence of change of position in good faith. This defence is available when the recipient incurs unusual expenses or liabilities when relying on the payment they believed they were entitled to.[164] In other cases the recipient may simply fail to cooperate. Ultimately, the funds may not be recovered at all, or only after a delay and negotiation.

7.72 The legal question of where to allocate liability for unrecovered loss after a mistaken internet payment is contentious. The Banking and Financial Services Ombudsman (BFSO) has taken the view that if the name entered on the screen forms part of the payment instructions to the receiving account institution (as it normally will), a disparity between name and account number can mean in effect that the account institution does not have a clear mandate to transfer the funds and therefore that the funds should be re-credited by the account institution.[165]

7.73 However, to avoid this, the account institution can make it clear that the account name does *not* form part of the payment instructions by:

---

[164] See *David Securities v Commonwealth Bank of Australia* (1992) 175 CLR 353. See also Banking and Financial Services Ombudsman, Bulletin 52, December 2006 at p. 6-7 (*Misunderstandings about mistaken deposits into an account*)

[165] The BFSO considered the issue in Bulletin No. 35 (September 2002), and again in Special Bulletin of September 2003 following a forum on *Emerging Issues in Electronic Banking Dispute Resolution* held by the Ombudsman. See also Tyree, AL, 'Mistaken internet payments' (2003) 14(2) JBFLP 113.

(a) clearly stating as much in its account terms and conditions, and

(b) including a clear warning on the internet banking screen that the name will be disregarded in making the payment and that the bank will rely solely on the account number.

7.74 We understand that general industry practice, while assisting customers to try to recover funds that have been transferred by mistake, is not to accept liability for mistaken payments in any circumstances (unless an entry or other error has been made by the bank's officer).

7.75 The EFT Code might address the issue of mistaken payments in a number of ways. Various options have been proposed, some of which are set out in Table 10.[166] It is appreciated that many of these measures could not be implemented without system changes, and that an agreed implementation timeframe would need to be established.

Your feedback

Q41 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.

Table 10: Possible regulatory responses for mistaken payments

Reduce mistakes	Users may be less likely to make a mistake when entering account numbers if the number entry boxes are formatted in groups of four rather than being a single continuous string.[167] The BFSO regards this kind of formatting as good industry practice and this could be specified in the EFT Code.
Warn users	A warning to users could be included, to take care when entering account numbers immediately next to the account entry boxes. Users could be advised that wrongly entered numbers may result in funds being transferred to someone other than the intended recipient. Many institutions currently adopt this measure, although the prominence and effectiveness of warnings varies.
Configure for double entry	Account institution's systems could be required to be configured for double entry of the account number, with the transfer only being approved when the numbers match. This would address the situation when, for instance, digits were reversed inadvertently when being entered.
Clarify ambiguity	Recipient institutions that are EFT Code subscribers could be required to seek clarification of any ambiguity in the payment instructions. This might be required, for example, when because of the mistake the payment cannot be made without

[166] Some of these suggestions are similar to BFSO good practice guidance. See BFSO Bulletin September 2003 at p.7–8.

[167] Tyree, 'Mistaken internet payments', footnote 165 above.

	alteration of the BSB or the account number.
Notify unintended recipient	Measures could be codified to reduce the possibility that the unintended recipient of the funds will pay away the money in their account in the mistaken belief that they are entitled to it. These might include an obligation on the account institution to immediately notify the recipient account institution when advised of an error. Recipient institutions that are EFT Code subscribers could then have a corresponding obligation to immediately notify the recipient that an error had been asserted, and seek the recipient's consent to its reversal. When the recipient of the payment asserts that they are entitled to it, the subscribing recipient institution would also be obliged to seek the recipient's consent to the disclosure of the recipient's name and details to the payee's account institution and payee.
Require recipient AI to identify funds recipient	The recipient account institution, if a Code subscriber, could be required to identify the recipient of the funds allegedly paid under a mistake to the payer AI. This would facilitate recovery, but privacy issues would need to be addressed.
Implement chargeback regime	A form of chargeback might be adopted allowing the payer AI to reverse the disputed transaction unless the recipient was able to show he or she was entitled to payment.
Codify clear mandate/liability for payer AI	The EFT Code might incorporate the BFSO approach as described above.

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

Part B was added to the EFT Code following the last review.[168] It aims to provide an alternative 'lighter touch' regulatory scheme for newer/alternative types of payment products (particularly prepaid), including both limited use and cash-substitute facilities issued by entities in a range of sectors of the economy.[169]

However, the regulatory framework provided by Part B has had little impact, because providers of payment facilities outside the financial services sector have not subscribed to the EFT Code.[170]

This review is an opportunity to consider both the scope of Part B and the obligations it imposes to see what can be done to make the EFT Code a more viable and effective regulatory instrument. This section, considers the scope of Part B, while the substantive requirements are considered in Section 9.

The central issue discussed here is whether the scope of Part B needs to be defined in a broader, more technology neutral way than is currently the case.

Payment facilities to which Part B applies

8.1 Part B applies to 'stored value facilities' (SVF) and 'stored value transactions' (cl 11.1). A stored value facility is 'a facility (e.g. software) that:

(a) is designed to control:

  (i) the storage of stored value, and

  (ii) the release of that stored value from the facility in the course of making a payment using that stored value;

(b) is intended to be in the possession and control of the user; and

(c) contains a value control record.' (cl 11.2)

The terms 'stored value' and 'value control record' are also defined (cl 11.2).

8.2 A stored value facility (SVF) may take the form of an 'electronic purse' in which records of available value are stored on a card or other device[171], or 'digital cash' in which records are maintained on computer software.

---

[168] See Section 1, *1999-2001 Review*

[169] See Section 2, under *Other payments products*

[170] See Section 1, *Who subscribes to the Code*

[171] For example, a chip-enabled mobile phone (see Section 2)

8.3 In the first case, the device is used at a specially-adapted public access terminals, such as a point-of-sale terminal. A microprocessor chip on the device holds and adjusts the record of value available for use by the cardholder. When the card is presented as a means of payment, the terminal reads the balance information on the card to see if sufficient value is available to pay for the goods or services being purchased. Assuming this, the payment is processed, with the balance recorded on the card chip being debited from the cardholder's account and credited to the merchant on software located on the merchant terminal.

8.4 Digital cash operates via a personal computer or other equipment to which the consumer has proprietary access. Digital representations of value are transferred electronically from one computer to another to effect an online payment. It would appear that there have been no successful commercial applications of this electronic payment instrument in Australia to date, and that there is currently little interest in it as a payment mechanism.

8.5 SVFs are commonly contrasted with electronic access products, such as an EFTPOS card. In the latter case, the value record is not adjusted on the device or equipment but at a central facility where the user's account is accessed remotely each time the card is used.

8.6 Under the EFT Code, an aspect of the use of a Part B SVF can fall within the regulation of Part A. If a stored value card can be 'topped up' by transferring funds from a deposit or credit card account, that transfer (being from an EFT account) falls within the scope of Part A. However, the use of the topped-up card to make payments is regulated under Part B.

Background to development of Part B regime

8.7 Part B aims to be a general regulatory scheme for prepaid and other limited use payment products because arguably many of these products would not be appropriately regulated within the Part A framework.

8.8 Part A had its genesis in regulating electronic transactions to and from traditional deposit accounts issued by banks and other financial institutions. Most prepaid facilities are quite differently conceived (although the extent of variation varies), and consumer expectations about these facilities may also be different.

8.9 The separate, tailored Part B regime takes account of the relatively recent emergence of these facilities and generally applies a 'lighter touch' to their regulation. The generally more limited obligations imposed under Part B are discussed in the next sub-section.

Part A and Part B obligations compared

8.10 Part B regulates some of the same areas as Part A, including disclosure and changing of terms and conditions (cl 12 and 13), liability for system or equipment malfunction (cl 17), and complaint investigation and resolution (cl 19).

8.11 However, there are important differences between the two regimes: see Table 11. These reflect the different types of product they were designed to regulate.

Table 11: Comparison of obligations in Parts A and B

Transaction confirmation and account statements	Part A requires detailed information to be given in receipts, and account statements to be sent to account holders at least every 6 months (cl 4). Part B requires only a reasonably available mechanism for checking the available balance (cl 14). There are no separate transaction confirmation or account statement requirements.
Liability for unauthorised transaction losses	Part A imposes liability on subscribing institutions in a wide range of circumstances both before and after notification of loss or theft (cl 5). Part B limits stored value operator liability in two ways. First, liability is limited to situations when the stored value operator and other system participants can create a reliable record of the amount of stored value controlled by the facility, and can prevent any further transfer of value from the facility (cl 16(a) and (b)). Secondly, responsibility only applies to losses following notification (cl 16(d)). Generally, Part B reflects general marketplace practice outside financial services without seeking to set higher standards of consumer protection.
Right to exchange/refund and expiry of value	Part B gives users rights to exchange and refund the stored value in certain circumstances (cl 15 and 16).[172] It also imposes disclosure requirements specifically about these rights.[173] Another matter that must be disclosed is 'the period or date (if any and if determinable at the time of issue) after which the stored value facility or the stored value controlled by the facility will not be usable to make a payment'.[174] There are no equivalent provisions in Part A. This is because issues relating to the right to exchange and refund, and the 'expiry' of value, do not normally arise with traditional deposit account facilities (in respect of which funds are deposited on an 'on demand' basis).

[172] These clauses are considered in Section 9 of this paper.
[173] Clause 12.3(b)–(e)
[174] Clause 12.3(c)

Does the scope of Part B need to be redefined?

8.12 At the time of the last review it was assumed that most emerging payment facilities would take the form of electronic stored value payment instruments and Part B facilities were defined in terms of such instruments. Since that review, however, there has been only limited use of 'smart' technologies to authorise payments (although recent developments, particularly in the mass transit area, suggest that use of these technologies is likely to increase[175]).

Facilities not covered by Part B

8.13 The majority of newer limited-use payment products available rely primarily on remote access authorisation, sometimes utilising legacy infrastructure, rather than on stored value technologies. This includes, in our understanding, most prepaid cards, gift cards, toll devices, and mobile payment services. *Given the way these facilities work, they are not captured by the Part B regime*.

Facilities covered by Part A

8.14 In some cases, transactions involving such facilities come within the definition of an EFT transaction under Part A. This broad definition effectively encompasses virtually any transaction when an instruction to transfer funds is given electronically to a subscribing entity by a user to debit or credit the user's account with that entity.[176] An example would be an instruction given by an e-tag to debit a tollway customer's account when their vehicle passes through the toll booth.

Facilities not covered by Part A or Part B

8.15 On the other hand, the definition of an EFT transaction under Part A is limited to transfers to or from an account held with an identified account holder of the subscribing entity.[177] Thus, if there is no identified account holder an electronic funds transfer will not be an EFT transaction under Part A. However, the facility through which payment is made will not come within the Part B definition of a stored value facility either, if the payment is authorised remotely rather than by adjusting a value record on the facility.

8.16 This will be the case, for example, with most gift and similar prepaid cards issued by retailers. In general, these cards are not

---

[175] See Section 2, *Other payments products*

[176] See definitions of 'EFT transaction' and related terms, including 'EFT account' at cl 1.5 of the EFT Code.

[177] This follows from the definition of 'EFT account' in cl 1.5 of Part A.

personalised, there is no identified account holder—rather, they are issued as cash substitutes on the basis that ownership may and frequently will be transferred to someone other than the purchaser. At the same time, they do not generally use microchip technology (most are conventional magnetic stripe cards), and payment is authorised remotely.

Issues/options

8.17 In summary, there is a range of alternative payment facilities that might have been regulated within the Part B framework (or something similar to it), but that fall outside its scope. Either they come within the more intensive regulatory regime of Part A, or they fall outside the EFT Code altogether.

8.18 Arguably, then, given the way prepaid products have developed in recent years, the scope of Part B has been defined in too narrow and technologically specific a way in the current EFT Code. If this is accepted, how might the scope of Part B be appropriately broadened?

Alternative approach to defining Part B scope

Focus on products rather than payment authorisation

8.19 One possible option would be to look to the features of the products themselves and the consumer risks and expectations associated with those features, rather than to focus on the payment authorisation technology (as with the current stored value facility definition). Thus, Part B might be re-conceptualised as a lighter touch regulatory structure for facilities judged to be lower risk and/or not to have the same expectations of protection as those associated with traditional deposit accounts and similar products.

8.20 For example, Part B might be redefined to include some or all of the following facilities—irrespective of whether they use stored value or remote access technology:[178]

(a) facilities that are anonymous in character (i.e. the owner of the SVF does not have to give their name when acquiring the facility);

(b) disposable prepaid facilities, when additional value cannot be loaded post-purchase (these may also be anonymous);

[178] The suggestions following are largely based on the statutory and regulatory exemptions applying to non-cash payment facilities (NCPF) under the Corporations Act regime. The relationship between Part B and the Corporations Act NCPF jurisdiction is discussed in Section 9 (paragraphs 9.3 - 9.6).

(c) facilities provided for one off transactions (e.g. facilities offered by remittance dealers);

(d) single payee facilities;

(e) facilities that can only be used to pay a limited range of payees—eligible payees might be limited by factors such as location (e.g. in and around transit corridor, university campus, retailers at a particular shopping centre etc), whether the entity is a member of a corporate group, whether the entity is one of a limited number of scheme participants;

(f) facilities that can only be used to purchase a limited range of goods and services (e.g. a mobile payment facility for purchasing additional services provided to the user's handset); and/or

(g) prepaid facilities designed for low value transactions—this might be defined by reference to a total amount of prepaid value available at any time, or over a defined period.

8.21 This is a provisional list only, and the scope of some of suggested inclusions would themselves need to be defined. Table 12 sets out our preliminary view of the potential advantages and disadvantages of redefining Part B in this way.

Table 12: Implications of defining scope by products rather than payment authorisation

Advantages	Disadvantages
• Broadened scope would include facilities arguably overregulated under Part A, as well as facilities currently not caught by either part. • Greater alignment of consumer risk and expectation of protection with regulatory burden. • Greater alignment with the approach of the Corporations Act. • No disruption of the settled regulatory framework currently provided under Part A (as long as the scope of Part B was appropriately limited). • No additional costs to existing subscribers. • Potentially more attractive as a voluntary instrument for payment service providers that do not currently subscribe to the Code.	It may be difficult to develop a revised description of Part B scope that is: • sufficiently broad, but not too broad • sufficiently precise, but not unduly complex.[179]

[179] It has been suggested that this issue could be addressed by making Part A the regime for authorised deposit-taking institutions (as defined under the Banking Act) and Part B the regime for other providers of payment facilities. We have not developed this suggestion. Although the approach would allow a clear line to be drawn between the

Should a unitary regulatory model be adopted?

8.22 Our discussion to date has assumed the continuance of a dual (Part A/Part B) regulatory model. Another option might be to seek an appropriate level of differentiation of payment facilities' regulation within a unitary structure (i.e. one set of rules which are differentially applied).

8.23 There has been some support for a unitary model, largely on the basis that the EFT Code would be more conceptually coherent if structured in this way.[180] Further to this, some Australian and international commentators have argued that the concept of 'stored value' is problematic, and that what are called stored value facilities are fundamentally akin to traditional account-based facilities.[181] Rather than being distinct, both types of facility are essentially account-based (involving the debiting and crediting of payers and payees accounts), even though the account keeping process in the SVF case is a more distributed or decentralised one.

8.24 One writer has illustrated this last point as follows:

> *Take for example an anonymous smart card able to process payments offline. Let us assume that the card can be used to effect payments at vending machines and other merchants not continuously linked to the issuer. The vending machine does not need to contact the issuer before accepting each payment. Instead, the vending machine keeps track of transactions made with it and each card keeps a record of transactions which its holder has made. These records are reconciled with the issuer's records periodically. When the card is presented for recharging or when the vending machine operator periodically settles with the issuer (eg monthly). It is in many ways a decentralised form of ledger or account keeping.*[182]

8.25 The passage continues:

> *Does the fact that the issuer doesn't know the balance of each holder at all times, and that the merchant need not confirm a payment with the issuer before accepting it, mean that the transaction is inherently*

---

two regimes, it would be problematic on competitive neutrality grounds. More specifically, in cases where an issuing business did not come within the scope of the Banking Act definition of an authorised deposit-taking institution, that business could provide deposit-like facilities offering lower levels of protection than if it was regulated under Part A. Conversely, the ability of entities regulated under Part A to develop alternative payment models within the Code framework would be heavily circumscribed (if not impossible, given the nature of the requirements of Part A).

[180] See, for example, Tyree, footnote 107 above, at pp. 345 and 356. More generally, see Tyree AL, 'The legal nature of electronic money' (1999) 10(4) JBFLP 273–281 and Bollen R, 'A review of the development and legal nature of payment facilities' (2005) 16 JBFLP 130 at pp. 140–141 and 145–147.

[181] See footnote above. See also international commentators cited in Bollen.

[182] See Bollen at p. 146.

different to a conventional account transaction? No. In both [the credit card and smart card examples given], the system still relies on the maintenance of customer accounts.[183]

8.26 The view that SVFs should be dealt with as part of a unitary structure was in fact put to the Working Group during the Code's last review. At the time, the Working Group commented by way of response:

> *Although there may be considerable merit in conceiving of stored value products as akin to traditional account products, their different functionality would still require considerable differentiation in treatment between the two types of products in a unified set of rules. The early stage of development of stored value products also requires a more flexible and general set of rules than the relatively prescriptive and detailed set of rules in Part A. For both these reasons, the Working Group has decided to retain separate Parts A and B. In future reviews of the Code, as experience with stored value products grows, the issue of unifying Parts A and B should be revisited.*[184]

8.27 Your views are sought on whether this issue should be revisited in the context of the current review.

Your feedback

Q42 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?

Part B scope and interpretation: other aspects

8.28 Apart from the question of whether the scope of Part B should be redefined, some more specific issues have been raised concerning the way the scope of Part B is currently defined. The ongoing relevance of these issues will obviously depend on whether or not a different approach is taken to the scope of Part B following this review.

Definition of a 'payment facilitator'

8.29 The substantive obligations under Part B are imposed on the 'stored value operator', defined as an entity that subscribes to the EFT Code that is either an 'issuer' or a 'payment facilitator' of an SVF, or both (cl 11.2):

[183] See footnote above.

[184] Second Draft Expanded EFT Code of Conduct and Commentary (January 200) at p. 36, accessible via review website at www.asic.gov.au/eftreview.

(a) an 'issuer' is defined as 'an entity, which, in the course of its business, provides an SVF to a user' (cl 11.2);

(b) a 'payment facilitator' is defined as 'an entity, which is contractually bound to a *user* to facilitate the payments the user initiates by using the SVF' (cl 11.2, emphasis added).

8.30 The definition of a 'payment facilitator' has been criticised on the grounds that, typically in a payments scheme, the user will not have a contractual relationship with the ADI or other financial institution responsible for ensuring that payments are processed and participating merchants' accounts credited.[185] Rather, it is the *issuer* that will normally have this contractual relationship (unless, of course, the issuer is itself also the payment facilitator). Given this, the definition of payment facilitator arguably needs to be changed to allow entities acting as facilitators of payments to be EFT Code subscribers (as the drafters intended).

Definition of 'system participant'

8.31 Another term criticised is 'system participant'. A 'system participant' is defined as 'a party to a stored value system and includes issuers, payment facilitators, holders of value received in exchange for stored value, originators of stored value, distributors of stored value, transaction processors, communications service providers and merchants who receive stored value as payment' (cl 11.2).

8.32 The precise meaning of both an 'originator' and a 'distributor' of stored value have been questioned, as has the need for the inclusion of 'system participant' as a defined term given that the only mention of this term in the substantive provisions is in cl 18.[186]

Your feedback

Q43 Assuming the scope of Part B of the EFT Code continues to be defined in terms of the concepts of 'stored value facilities' and 'stored value transactions', what changes, if any, should be made to the definitions and other provisions of cl 11?

[185] Tyree, footnote 107 above, at p. 357

[186] Clause 18 says that the stored value operator cannot avoid obligations under the EFT Code merely because the problem is attributable to another system participant, and cannot require users to raise the problem with another participant. Arguably, the term 'system participant' could be used here without requiring definition.

Section 9: EFT Code, Part B (Requirements)

This section considers issues about the substantive obligations imposed on subscribers under Part B of the Code. Because providers of facilities regulated under Part B have generally not subscribed to the EFT Code to date, there has been only limited feedback from stakeholders on these obligations.

Record of available balance (cl 14)

9.1 Clause 14 is currently limited to requiring stored value operators to ensure 'that an undamaged SVF (either by itself or together with other equipment reasonably available to the user) enables a user to find out the amount of stored value controlled by the SVF, which is available for use'.

Issues/options

9.2 It has been suggested that this is a very minimal requirement and that operators of regulated facilities could also be required to make a transaction history available on request for a specified period (for instance, two months). As has been noted, without access to at least minimum records it is difficult for purchasers of SVFs to identify mistaken and/or unauthorised payments.[187]

Your feedback

Q44 Should any changes or additions be made to cl 14?

Q45 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?

Consistency between Part B and Corporations Act (cl 12–14)

9.3 As discussed in Section 6,[188] there is a degree of overlap between the coverage of the Corporations Act financial services regime and that of the EFT Code. Similar issues are potentially raised when considering the interrelation of Part B of the Code and the Act.

[187] Budnitz M, 'Stored Value Cards and the Consumer: the Need for Regulation' (1997) 46 *American University Law Review* at 1071, discussed in Bollen R, 'A Review of the regulation of payment facilities' (Part 2) (2005) 16 JBFLP 352 at p. 331.
[188] See *Consistency between Part A and Corporations Act (cl 2-4)*, paragraphs 6.21 – 6.24.

Issues/options

9.4 In particular, it might be thought that consistency between the disclosure and record of available balance requirements under Part B (i.e. cl 12–14) and the disclosure and transaction confirmation requirements of the Corporations Act (see Table 8, Section 6) is a possible issue. As we noted in Section 6, 'consumer stored value facilities' as defined by the EFT Code would fall within the definition of a 'non-cash payment facility' under the Act.[189]

9.5 Arguably, however, as with the Part A/Corporations Act interrelation, the issue of regulatory consistency between Part B and the Corporations Act is more apparent than real. This is because, as a result of both legislative exemptions and ASIC Class Order relief, discussed in Section 4 (see paragraphs 4.4 to 4.6), the application of the disclosure and related provisions of the Act to non-cash payment facilities is now heavily circumscribed.

9.6 In short, when any of these carve-outs apply, issues of regulatory duplication between the Corporations Act and the EFT Code do not appear to arise.

Your feedback

Q46 Are any aspects of Part B of the EFT Code incompatible with the requirements of the Corporations Act? How should any incompatibility be addressed?

Right to exchange/replace stored value (cl 15)

9.7 Clause 15.1 gives users a general right to exchange stored value for money (i.e. a cash refund) or replacement stored value, at the user's option.[190] A reasonable fee may be imposed.

9.8 Clause 15.1 and 15.2 together also deal with the situation when an SVF or stored value is unusable for whatever reason—for example, because the facility is damaged or malfunctioning, the amount of stored value remaining is below the minimum needed for a transaction, or the facility or value has 'expired'.[191]

9.9 In these circumstances, the right to exchange for money or replacement stored value also applies as long as the amount of stored

[189] See paragraph 6.23

[190] The right to exchange for money only applies where the stored value is denominated by reference to currency: cl 15.1, Endnote 36.

[191] These are the example given in Endnote 34.

value controlled by the facility can be ascertained by the stored value operator using its own equipment (cl 15.2(a)). However, the terms and conditions may limit exercise of this right to a minimum 12-month period (cl 15.2(b)) and certain other limitations apply (cl 15.3). When the facility or stored value is unusable, no fee may be imposed for refunding or replacing it (cl 15.1).

9.10 Because of this right to exchange for cash, an SVF under Part B may be subject to prudential regulation by APRA as a purchased payment facility in certain circumstances.[192]

Extent of rights to exchange

Issues/options

9.11 It has been suggested that mandating a general right to exchange stored value for money under cl 15.1 is unnecessarily prescriptive and out of step with current marketplace practices.

9.12 In contrast to mainstream deposit accounts, it is argued that these types of payment facility do not inherently involve an implicit promise that the funds paid are a debt due, and that they should be able to be received back again. It is also noted that giving a right to exchange potentially adds to administrative costs associated with the facility, and (particularly in the case of lower value facilities) that these additional potential costs may affect the viability of the facility as a business proposition. Concern has also been expressed about the regulatory implications (specifically, the potential for Code-compliant facilities to be subject to prudential regulation).[193]

9.13 Giving a right to exchange for 'expired' value under cl 15.1 and 15.2 has also been questioned. (Effectively, as noted, a refund or exchange of expired value can be sought for a further 12 months.) Again, it is suggested that this requirement is unnecessarily prescriptive and out of touch with marketplace realities.

9.14 It is noted that the business case for many prepaid facilities turns on the fact that a proportion of prepaid value will 'expire' (i.e. the value will become the issuer's). We understand that this occurs in up to 5% or more of total value purchased, in the case of some widely used cards. It is also contended that the fact that most gift cards and similar products must

---

[192] See paragraph 4.14 above. APRA regulates purchased payment facilities that: (a) are issued on a wide basis, and (b) allow any unused stored value to be redeemed on demand in Australian currency. APRA's regulatory scheme for PPFs is set out in Australian Prudential Standard (APS 610) and *Guidelines on Authorisation of Providers of Purchased Payment Facilities* available at www.apra.gov.au

[193] See previous footnote.

be used within a defined period is widely understood and accepted by the public.

9.15 From a consumer perspective, on the other hand, it is noted that prepaid payment facilities are likely to become the only means of payment for certain services in the future (e.g. mass transit ticketing). In this context, a general right to exchange may be seen as appropriate.

9.16 Consumer representatives have also expressed concern about the promotion of prepaid cards with very short use-by dates (e.g. as little as 3 months).

Possible alternative approach

9.17 A possible alternative approach to regulating this area might be considered. In response to industry concerns, both the general obligation to exchange stored value and the specific requirement to do so when that value has expired might be removed. An obligation to exchange or convert value could be retained in other circumstances (e.g. when the remaining value is below the minimum needed for a transaction, or the facility is malfunctioning).

9.18 However, balancing this from a consumer perspective the EFT Code might also include:

(a) a requirement that all facilities regulated under Part B must have a minimum use time of at least 12 months; and

(b) measures to enhance disclosure of the expiry period for the facility.

9.19 Currently, the EFT Code merely requires that information or a summary including 'the period or date … after which the stored value facility or the stored value controlled by the facility will not be usable for making a payment' must be given to the user before the facility is used.[194]

9.20 In addition, subscribers might be required to prominently display either the use period or date on any physical device (such as a card) used to make payments with the facility.[195]

Your feedback

Q47 Should the rights to exchange stored value under cl 15 be narrowed?

[194] See cl 12.3(b).

[195] These proposals are based on ASIC Class Order relief for gift vouchers or cards [CO 05/738] and low value non-cash payment facilities [CO 05/736].

Q48 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?

Q49 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?

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

9.21 Clause 16 is, in a sense, the Part B counterpart to the Part A unauthorised transaction regime. It only applies to regulated facilities when the operator and relevant system participants can identify specific facilities and the amount remaining on them, and can prevent further transfers of value from the facility: cl 16.1(a) and (b). In such cases, the EFT Code requires the operator to:

(a) tell the user how to notify the loss or theft of the facility (cl 16.1(c)); and

(b) pay the user the amount of any stored value that the operator could have prevented from being transferred from the facility (cl 16.1(d)).

Issues/options

9.22 As with the cl 15 requirements, this requirement has been criticised because it imposes what are seen as unnecessary limits on product design.

9.23 It is suggested that, for example, a low value prepaid facility might be marketed to consumers, and purchased by them, on the basis that whoever has possession of the facility can use it without restriction—in effect, the risk of losing the card is like the risk of losing cash. It is contended that many consumers are willing to purchase low value facilities (in particular) on this basis and that the EFT Code should not impose additional regulatory obligations, and associated costs, on such facilities.

Possible alternative approach

9.24 It has been suggested that a right of the kind set out in cl 16 might be retained but in a modified form. For example, the obligation might only apply to facilities that allowed more than a certain level of prepaid value to be held (the amount would need to be determined).

9.25 Alternatively, and more minimally, the Code could specify that, where facilities allow more than a certain level of value to be held, users must be given the option of PIN security or other access control functionality. In other words, for a facility allowing prepaid value above

a certain level to be EFT Code-compliant it would need to give users a means of protecting themselves against loss or theft (following notification) if they chose to activate it.

9.26 PIN security is already common in the case of facilities that allow higher levels of prepaid value to be held. Arguably, the measure would be consistent with promoting higher standards of consumer protection in the context of a voluntary code.

Your feedback

Q50 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?

Q51 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?

Right to unilaterally vary terms and conditions

9.27 Terms and conditions for payment facilities frequently give the issuer broad rights to unilaterally vary the terms and conditions.

Issues/options

9.28 It has been suggested that applying a unilateral right to vary a prepaid facility in a way that makes it materially different from the facility as purchased is unacceptable from a consumer perspective.

9.29 Currently people must be told if the issuer has a right to unilaterally vary the terms and conditions (under cl 12), or if the conditions are changed. (cl 13) It has been suggested that the EFT Code should go further and exclude unilateral variation clauses if applying them would materially disadvantage the holder of the facility.

9.30 Consumers should not be put in a position, it is argued, when they purchase one thing and end up getting something else as a result of the operation of a standard term unilateral variation clause.

Your feedback

Q52 Should the use of unilateral variation clauses in the terms and conditions for facilities regulated under Part B be restricted?

Complaint investigation/dispute resolution (cl 19)

9.31 This clause applies cl 10 of Part A to disputes about Part B facilities; however, cl 10.11–10.14 inclusive are not applied. Among other things, the excluded clauses:

(a) impose obligations on subscribers to make documents and other evidence available to account holders (cl 10.11(a)), and to advise account holders if any system or equipment malfunction had occurred at the time of the disputed transaction (cl 10.11(b)); and

(b) allow an external dispute resolution body to determine that the account institution is liable to pay part or all of the amount in dispute to the account holder as compensation if it fails to follow the cl 10 procedures (even if it is ultimately determined that the institution is not liable for the loss).

Issues/options

9.32 The more limited Part B requirements were seen as part of the lighter touch regulatory approach to Part adopted by the Working Group at the last review. Nonetheless, it has been commented that, 'There is no explanation as to why these sections (i.e., cl 10.11 – 10.14) do not apply to stored value operators. It seems an undesirable distinction between account institutions and stored value operators.'[196]

Your feedback

Q53 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?

Payment finality

9.33 A key aspect of a payment facility is whether or not its use results in final discharge of payment (or payment finality or non-refutability).[197]

Issues/options

9.34 Arguably, users of facilities regulated under Part B should be able to assume that, when they use the facility as instructed, their payment obligation to the payee will be effectively discharged. It has been suggested that this principle could be reflected in Part B of the EFT Code. (Arguably, general banking law principles would cover most facilities regulated under Part A.)

[196] Tyree, footnote 107 above, at p. 358

[197] See Bollen, footnote 180 above, at p. 331 and authors cited therein.

Your feedback

Q54 Should Part B of the EFT Code address the issue of payment finality?

Part B subscribers to the Code

9.35 This issue is discussed under Membership in Section 12.

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

This section considers the two 'content' areas of Part C of the EFT Code. Administration of the EFT Code is dealt with in the next section.

Privacy obligations (cl 21)

10.1 Privacy obligations are covered in three clauses:

(a) Clause 21.1 commits all EFT Code subscribers to comply with the National Privacy Principles (NPPs) or an approved code under the *Privacy Act 1988* (Cth).

(b) Clause 21.2 sets out certain non-binding 'guidelines' to assist in interpreting and applying the NPPs and any approved privacy code to Part A EFT transactions. These guidelines are about the use of surveillance devices, account access, information disclosed on transaction receipts, and the provision of privacy policies at the account institution's website or other electronic address.

(c) Clause 21.3 clarifies that, for compliance purposes, it is the NPPs not the guidelines that will determine privacy issues.

Privacy guidelines (cl 21.2, 21.3)

10.2 The guidelines in cl 21.2 are unique in being the only non-binding provisions of the EFT Code. They were included on this basis as a compromise at the time of the last review, on the understanding that their status and content would be re-examined during the current review.

Issues/options

10.3 Doubt has been expressed about whether the sub-paragraph on the use of surveillance devices (cl 21.2(a)) is properly described as a 'guideline' to interpreting the NPPs. Arguably, notification about surveillance does not come within the scope of the Privacy Act (although it could be dealt with in a privacy code).

10.4 We seek your views on whether additional provisions relating to privacy should be included in the EFT Code and/or whether provisions relating to privacy should have the same status as other provisions under the Code—in other words, should they be requirements? Clauses 21.1(a), (b) and (d) have been described as no more than expressions of general industry practice. Paragraph 21.1(b) arguably also comes within the account institution's general law duty of confidentiality to its customer.

Your feedback

Q55 Should the provisions about privacy under cl 21 of the EFT Code be modified and/or extended to cover other areas or issues?

Q56 Should the status of the cl 21.2 guidelines be changed to make these provisions contractually binding requirements?

Receipt information—privacy concerns (cl 21.2(c))

Issues/options

10.5 The information disclosed on transaction receipts (dealt with in cl 21.1(c)) has been raised as an issue by consumer and privacy advocates concerned about the inclusion of full account number and/or expiry date details on the EFTPOS receipts issued at some merchant terminals. ASIC and, we understand, the Office of the Privacy Commissioner (OPC) have received complaints about this issue.

10.6 Consumer and privacy representatives are concerned that information disclosed on the receipt could be used in perpetuating payments fraud or other identity theft crime, if it comes into the possession of a dishonest third party. Drawing on overseas legislative models,[198] it has been suggested that:

(a) a truncated version only of the account number should be included on receipts;

(b) the expiry date should not be included; and

(c) the account holder's name or address should never appear on receipts. (We are not aware of these details ever being included on transaction receipts.)

10.7 It is suggested that the EFT Code could mandate these measures, rather than simply include them as recommendations. This may be an appropriate approach given heightened concern about security issues in recent years. It would also be consistent with now widespread industry practice.

10.8 In addition, Principle 4 (Data security) of the NPPs arguably requires consideration of measures such as those proposed. Paragraph 4.1

[198] For example, s1747.09 of the California Civil Code generally prohibits entities that accept credit or debit cards for payment from printing more than the last five digits of the card number, or the expiry date, on any receipt provided to the cardholder. The requirement only applies to receipts that are electronically printed, and does not apply to transactions where the sole means of recording the transaction is by handwriting or an imprint of the card.

of NPP4 states that, 'An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.' Finally, revealing the full account number, name or address of the account holder on a receipt may, it is suggested, constitute a breach of the account institution's general law duty of confidentiality to its customer.[199]

10.9 Views are sought on the above proposals including cost and time for implementation (where the measure has not already been implemented).

Your feedback

Q57 Should the EFT Code require that transaction receipts include only a truncated version of the account number?

Q58 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?

Q59 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 timeframe?

Electronic communications (cl 22)

10.10 Clause 22 allows mandated information under the EFT Code to be supplied by electronic means, subject to a number of requirements designed to safeguard users' interests. Most importantly, users must agree to receive information electronically, and this agreement must be by way of 'a specific positive election after receiving an explanation of the implications of making such an election' (cl 22.1, final para).

10.11 Electronic communications may be made available:

(a) directly to the user's device, electronic equipment or electronic address (cl 22.1(a)); or

(b) at a dedicated website or other electronic address (cl 22.1(b)). In this case:

  (i) the user must be advised electronically that the information is available on each occasion (cl 22.1(b)(i)); and

[199] Tyree, footnote 107 above, at p. 356

(ii) the subscriber must also 'provide the user with the ability to readily retrieve the information by electronic communication' (cl 22.1(b)(ii)). (This requirement is considered below.)

10.12 The user also has the right under cl 22 to terminate the agreement to receive communications electronically, as well as to change their nominated device, equipment or address (cl 22.1, final para). The manner and format of communications is also regulated: they must be clear and readily understandable and must be able to be retained (printed or stored).[200] Finally, the user may require the subscriber to provide 'a paper copy' of any electronic communication if this is requested within a 6-month period (cl 22.3). (This requirement is also considered below.)

Ability to readily retrieve information at a dedicated site (cl 22.1(b)(ii))

10.13 Under cl 22.1(b), as noted, when information is made available for retrieval at the subscriber's website or other electronic address, the subscriber must among other things give the user the ability to 'readily retrieve' the information. The examples given of methods of retrieving information readily are—'by providing an electronic link to the relevant information at the Code subscriber's electronic address or the URL of the Code subscriber's website' (cl 22.1(b)(ii)).

Issues/options

10.14 Arguably, retrieval involving a 'click through' link in the account institution's message are inconsistent with contemporary good practice in internet fraud prevention. As will be appreciated, links in messages sent to users that allow the user to click through to what appears to be a financial institution's website are commonly used in phishing attacks. (When the EFT Code was last reviewed such attacks were far less common than today.) Customers are now warned not to open links in messages that purport to be from their account institution, and there is a general view among fraud experts that practices for legitimate communications should be consistent with such warnings.

10.15 Given this, it has been suggested that the requirement to give the ability to *readily* retrieve mandated information should be amended or deleted. It should be enough, it is argued, for the user to be advised to go to their institution's website to retrieve the information.

[200] This is achieved under the EFT Code through the definition of 'electronic communication' (cl 20.1).

Your feedback

Q60 Should cl 22.1(b)(ii) be deleted, or amended in some way?

Clause 22.2(b)(ii)

10.16 This clause appears to imply that an electronic communication will only be treated as having been supplied for the purposes of the EFT Code if the user:

(a) confirms that they have viewed the communication and have been given an opportunity to retain it, and

(b) understands they will not otherwise be given a copy of the information (subject to cl 22.3).

Issues/options

10.17 Industry representatives have queried whether this is an additional requirement imposed on subscribers that send mandated information electronically by earlier agreement with the user.

10.18 Our understanding is that this was never intended. A requirement that a user (having elected to receive information by electronic communications) must confirm that they have received their periodic statement or other communication on each occasion before the subscriber can be treated as having sent the statement would arguably be onerous and unworkable.

Your feedback

Q61 Should cl 22.2(b)(ii) be deleted, or amended in some way?

Products that only allow electronic communication of information required by the EFT Code

10.19 In drafting the current cl 22, it was assumed that electronic communication of periodic statements and other information would be an option available within the context of products that also communicated by way of paper copies through the post. Thus, for instance, in the situation when a person terminated their election to receive communications electronically, the option of receiving paper communications would be available.

Issues/options

10.20 We understand, however, that some account institutions have considered/are considering introducing banking products for which

periodic statements and other information can *only* be received by electronic means.

10.21 From an account institution's point of view, presenting electronic account statements and other mandatory information has clear cost advantages over posting. Some online consumers may also be attracted to products that rely exclusively on the electronic channel, particularly if some of the cost benefits are passed on in the form of a lower account fees. For some users, electronic information may also be preferred as more convenient and/or secure than postal delivery.

10.22 It is noted, however, that prospective users of such products need to be made fully aware of the implications of only being able to receive their statements and other information by electronic means (e.g. that paper copies will not be available, that the ongoing capacity to receive or access information electronically needs to be ensured, and how long information will remain accessible electronically). Currently, the EFT Code does not deal specifically with these disclosure issues. Views are sought on whether it should do so.

10.23 Views are also sought on whether the current regime under cl 22 imposes any regulatory *impediments* to introducing products that only allow electronic communication of information required by the EFT Code. One issue previously raised with us in this context is the cl 22.3 requirements that subscribers supply a 'paper copy' of any electronic communication if the user requests this within 6 months of receiving the electronic communication.[201] We were previously advised that there may be technical problems generating and posting paper copies of statements (in response to a cl 22.3 request) when systems designed for electronic presentment of information, such as the BPAY system, are used to generate the initial electronically-presented document.

10.24 We would assume, on the other hand, that all account institutions have the capacity to generate hard copy records going back at least 6 years should these be required in litigation or non-court dispute

[201] After receiving a submission from an EFT Code subscriber who was considering introducing a product that would require users to receive account statements and other communications electronically, ASIC wrote to stakeholders on 30 June 2003, under cl 24.1(b), seeking views on proposed guidance for cl 22.3. We sought views on whether the requirement could be satisfied by making the requested copy available to be downloaded and printed from a dedicated website for at least 6 months (subject to certain additional disclosures being made to potential account holders/users). A number of submissions were received in response, most of them positive about this approach. However, concerns were also raised about whether the proposed guidance went beyond our power under cl 24.1(b) to 'interpret' the provisions of the EFT Code. As a result, we decided not to issue the guidance sought, and to await the further consideration of the issue as part of the current review.

resolution or other contexts. (The issue of the availability of records in the context of dispute resolution is considered in Section 6, under *Investigating complaints and availability of records*.)

10.25 Finally, views are sought on whether the Review Working Group should consider the issue of the period of time for which electronic copies of statements are available. Consumer representatives have noted that, for a range of reasons (including lodging tax returns), account holders sometimes require copies of their statements for the previous year or earlier. It is argued that, in the context of the electronic provision of statements, the Code could prescribe a minimum period (for instance, two years) during which statements must be available to be accessed electronically. It is appreciated that current systems do not generally allow access for more than 3 months, and that any change of the kind proposed would require an extended implementation period.

Your feedback

Q62 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?

When the communication 'bounces back'

10.26 What should an account institution do if it sends an email communication to a user at their current electronic address as required under cl 22 and receives a mail delivery failure or 'bounce back'?

Your feedback

Q63 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?

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

This section raises issues related to the administration of the EFT Code.

The administrator's role

11.1 ASIC has been responsible for administering and reviewing the EFT Code since 1998. The statutory basis for this role is provided by s12A(3) of the *Australian Securities and Investments Act 2001* (ASIC Act).[202]

11.2 Our role under the Code is set out in cl 23 and 24:

(a) ASIC must be notified when an entity subscribes to the Code (ASIC maintains a register of subscribing entities) (see cl 23.2).

(b) ASIC is given power to modify the application certain aspects of the EFT Code in consultation with subscribers and other interested parties (see cl 23.3). It may also issue guidelines interpreting the provisions of the Code (see cl 24.1(b)).

(c) ASIC has responsibility for setting Code reporting guidelines and monitoring subscriber compliance with the Code through an annual survey (cl 23.5 and 23.6 require subscribers to report to the Commonwealth annually in accordance with reporting guidelines).

(d) ASIC is required to undertake periodic reviews of the Code, such as the current review (see cl 24.1(a))

11.3 Regulators have played a greater part in administering the EFT Code than has been the case with other financial industry codes, such as the Code of Banking Practice.[203] This is primarily because of the EFT Code's functional character—the fact that it regulates certain types of transactions and facilities across a range of industries rather than being the Code of a particular industry or industry sector (in which case the industry itself would have a clear mandate and responsibility for its administration).[204]

---

[202] Section 12A(3) states: ASIC has the function of monitoring and promoting market integrity and consumer protection in relation to the payments system by:
(a) promoting the adoption of approved industry standards and codes of practice; and
(b) promoting community awareness of payments system issues; and
(c) promoting sound customer-banker relationships, including through:
  (i) monitoring the operation of industry standards and codes of practice; and
  (ii) monitoring compliance with such standards and codes.

[203] More information about this Code is available at the Australian Bankers Association website. See http://www.bankers.asn.au/Default.aspx?ArticleID=446.

[204] ASIC Policy Statement PS 183 *Approval of financial services sector codes of conduct* states (at [PS 183.78]): 'In rare instances, there may be a role for ASIC in administering

11.4 Your views are sought on ASIC's role as EFT Code administrator, including whether (despite the functional character of the Code) there may be other options for its administration in the future. Such options might include establishing a separate administration body.

11.5 In our view, an effective administrative body would need to be:

(a) independent of the industries that subscribe to the EFT Code and able to fund it. One way of achieving this would by having a balance of industry and consumer stakeholders and an independent chair; and

(b) adequately resourced to fulfil its functions.[205]

11.6 There may also be potential for sharing aspects of the administration of the EFT Code among stakeholders and/or service providers, with ASIC continuing to be primarily responsible. We refer to this option later.

Your feedback

Q64 Should ASIC continue to be primarily responsible for administering the EFT Code? Are there other arrangements that should be considered?

Modifying the EFT Code

11.7 ASIC has various powers to modify aspects of the EFT Code:

(a) A subscriber or prospective subscriber can apply to ASIC to modify the application of Part B of the Code for particular products, services or activities of the applicant. We must consider certain matters in deciding whether to grant the modification (see cl 23.3).

(b) Subject to consultation, ASIC can modify the disclosure requirements of the Code to avoid inconsistent operation with, or duplication of, disclosure requirements in legislation (see cl 23.4(a)).

(c) Subject to consultation, ASIC can modify cl 4.6 to ensure consistency with future legislative (*sic*) or industry practices (see cl 23.4(b))

(d) Subject to consultation, ASIC can modify the standards for industry dispute resolution that apply under cl 10.1 (cl 23.4(c)).

11.8 These powers were given to ASIC as a mechanism for addressing specific issues the last Review Working Group thought may arise during the

---

and/or monitoring the code (e.g. where the code is a functional code that covers a range of industries and providers). We will consider this on a case-by-case basis.'

[205] See ASIC Policy Statement PS 183 *Approval of financial services sector codes of conduct*, at [PS 183.73].

operation of the current EFT Code. We have not used these powers since the Code became operational. Nor have we been asked to use any of them.

Issues/options

11.9 Issues about modification powers under the EFT Code include:

(a) whether there should be such powers at all;

(b) if so, what they should cover;

(c) what procedural controls should be in place; and

(d) who should exercise any modification powers.

11.10 We make the following observations on these issues:

(a) The fact that the modification powers have not been used since the revised EFT Code came into operation may be an argument for not including modification powers at all. Alternatively, their inclusion might be seen as a potentially beneficial mechanism for dealing with overlooked or unforseen circumstances, and enhancing the flexibility and responsiveness of the Code to subsequent marketplace and other developments.

(b) If modification powers were retained, there may be a case for replacing the current limited powers with a general power to modify the application of any rule or obligation, subject to a mandated set of criteria being considered and principles of procedural fairness followed. This would have benefits from the point of view of flexibility and responsiveness, given the length of time between reviews of the EFT Code.

(c) Decision-making on the exercise of modification powers could be undertaken by ASIC as at present, or by a new EFT Code administration body if established. Even if a new Code administration body is not established, it may be thought desirable to have decisions about exercising modification powers made by a standing or ad hoc committee of stakeholder representatives established for the purpose.

(d) Similar arrangements might apply to the development and issuing of guidelines interpreting the provisions of the Code under cl 24.1(b).

Your feedback

Q65 Should the EFT Code allow its requirements to be modified between reviews in certain circumstances? If so, what modification powers should be included and how should they be administered?

Monitoring compliance

11.11 Under cl 23, EFT Code subscribers or their representative associations must report to the Commonwealth Government annually on:

(a) compliance (cl 23.5). This must be in accordance with 'the reporting guidelines for the industry sector' (cl 23.6). (This phrase is not explained.)

(b) initiatives in training staff in understanding and implementing the Code (cl 23.7).

11.12 In addition, cl 10 makes specific reference to producing and making available complaints data. Clause 10.14 states:

> *The account institution is to provide for the recording of complaints and their resolution so that aggregate data on the type, frequency and resolution of such complaints can be made available as required in Part C of this Code and so that institutions can identify and address systematic problems.*

EFT Code monitoring survey

11.13 Monitoring is normally undertaken in an annual self-assessment survey which subscribers are required to complete. The survey used to be paper-based and covered, as well as the EFT Code, the Code of Banking Practice, the Credit Union Code of Practice and the (since abolished) Building Society Code of Conduct. However, since 2001–2002 it has been electronic in format; and since 2003–2004 monitoring has been limited to the EFT Code alone.

11.14 The survey is divided into parts:

(a) a checklist of questions (approximately 160 for the 2003–2004 survey) requiring subscribers to report systematically on their compliance with the specific provisions of the EFT Code (Part A); and

(b) a complaints section requiring subscribers to provide statistics on transactions and complaints coming within the jurisdiction of the EFT Code during the monitoring period (Part B).

11.15 After looking at the survey results, ASIC usually publishes an annual report identifying areas of non-compliance and including aggregated transaction and complaints data.

The monitoring survey and the current EFT Code

Issues/options

11.16 There have been considerable difficulties with the survey monitoring process for the current EFT Code, mostly due to data recording issues. As a result, only one Code monitoring report has been published on the current Code (for April 2003–March 2004),[206] and monitoring for 2005–2006 has been cancelled while ASIC reviews the process, including through the current review. The most significant issue is that most subscribers appear not to be able to consistently extract and report transactions and complaints statistics (i.e. Part B of the survey).

11.17 Following implementation of the revised EFT Code, the monitoring survey for April 2002–March 2003 (the first reporting period for the revised Code) included, for the first time, questions on transaction and complaints data broken down across the wider range of channels to which the Code now applies (i.e. ATM, EFTPOS, telephone, internet, WAP and other). In part because subscribers had significant difficulties reporting this information in disaggregated form for the new channels, we decided to withhold the results of the 2002–2003 survey.

11.18 As an interim measure to address this issue, ASIC simplified the 2003–2004 survey so that subscribers only reported aggregated transactions and complaints data across the range of channels—in other words, the data did not need to be broken down by channel. However, subscribing institutions still had major difficulties reporting the data sought, as well as with other aspects of the survey. In consequence, while a report for 2003–2004 was published, a highly qualified view was expressed about the results.

11.19 Following this, ASIC decided that before attempting to redesign the survey further, we needed more information on the barriers preventing subscribers from capturing and/or extracting transactions and complaints data and other information. In late 2004, a roundtable feedback meeting was held with subscriber representatives on this subject, and written feedback was also invited. This was followed in 2005 by a one-off survey, in place of the usual annual survey, specifically focussed on how institutions collect and record EFT Code-related information, particularly about complaints.

11.20 Our consultation found that extracting and reporting transactions and complaints data is the area of most concern to subscribers. Within a single institution, such data may be complied by a number of different business units using multiple, and sometimes incompatible, recording and storage systems. What transactions and complaints are counted, how

[206] See *For more information* at Review web site, www.asic.gov.au/eftcode

they are categorised, the amount of information captured and whether and to what extent it can be retrieved are all part of the problem.

Table 13: Barriers to reporting reliable data[207]

Transactions data	• Some subscribers/business units cannot separate EFT Code-regulated credit card transactions from non-EFT Code regulated transactions.[208] • Some institutions/business units cannot separate consumer and business transactions. • Many subscribers/business units find it impossible to separately report internet and phone banking transactions. • Institutions count over-the-counter use of EFTPOS and PIN in different ways.
Complaints data	• Some institutions cannot separate EFT Code-regulated and non-EFT Code regulated complaints (e.g. signature-authorised credit card complaints and business transaction complaints from within their total complaints data). • Complaints may be categorised other than by channel (e.g. by topic/type). • Complaints data may not clearly distinguish between different channels (e.g. internet/phone banking/ATM/EFTPOS). • Complaints that are immediately resolved may not be counted at all. • Complaints may be double counted if escalated from one business unit to another (e.g. to a more specialised investigation unit).

Possible alternative approaches

11.21 In light of the problems experienced with the current process, we consider that a broad discussion of how the EFT Code should be monitored in the future is warranted.

11.22 Compliance monitoring is an essential feature of an effective code of conduct, in our view.[209] Specifically in relation to the EFT Code, it is important that both industry and ASIC have effective means of monitoring emergent consumer protection issues in the payments area, including issues related to specific payment channels (such as the internet). This objective has driven ASIC's Code compliance monitoring process, and it remains highly relevant in our view.

11.23 However, we accept, given the above-mentioned problems, that this objective may need to be pursued using a different monitoring process from the current one. For instance, one option might be to

[207] As identified by subscribers in the 2005 survey (not a complete list).
[208] When a credit card is used to transact by phone or via the internet, it will be subject to regulation under the EFT Code (assuming it is a consumer transaction) as the manual signature authentication exception (see cl 1.5(c)) does not apply.
[209] This view is expressed, for instance, in ASIC Policy Statement 183 *Approval of financial services codes of conduct* at [PS 183.77].

combine a more limited annual self-reporting survey with other mechanisms. Thus, a revised survey might be limited to soliciting information about breaches. How that information is sought might also be considered, including possible alternatives to the systematic checklist of questions covering all EFT Code requirements set out in Part A of the current survey.

11.24 Other possible compliance monitoring mechanisms might include:

(a) An external body (e.g. a third party service provider or ASIC if it continues in its role as EFT Code administrator) could selectively audit the Code. One or two aspects might be audited each year.

(b) Depending on broader administrative arrangements, a Code Compliance Committee could be established with powers to receive and investigate breach complaints from the public. This model has been adopted by the banking industry for the Code of Banking Practice.

Your feedback

Q66 How should compliance be monitored? What alternatives to the current self-reporting survey should be considered?

Reviewing the EFT Code

11.25 Regular reviews are an accepted feature of administering codes of conduct. Reflecting this, codes approved by us under Policy Statement 183 *Approval of financial services codes of conduct* [PS 183] must be independently reviewed at intervals of at least 3 years.[210]

11.26 Currently, the EFT Code and associated administrative arrangements must be reviewed by ASIC in consultation with a range of stakeholders, with the first review to start 2 years after the Code became binding on subscribers (i.e. on 1 April 2003).[211] This paper initiates the public phase of that review.

Issues/options

11.27 You may have views on how often the EFT Code should reviewed. One option might be to hold full reviews less frequently and

[210] [PS 183.79] explains the rationale for regular reviews: 'Independent code reviews are essential to ensuring that a code remains current and continues to deliver real benefits to consumers and subscribers. Reviews provide an opportunity for stakeholders to provide feedback about how a code has operated in the past and how it might operate in the future'.

[211] See cl 24.1(a) with cl 23.1(a). ASIC initiated this review process, writing to industry associations representing subscribers and consumer representatives seeking preliminary views about issues relevant to the EFT Code. Other stakeholders were also contacted.

implement a process of reviewing and updating aspects of the Code as marketplace and consumer developments require. Other options might include engaging an independent reviewer. This model could be adopted whether or not ASIC continues to be primarily responsible for administering the EFT Code.

Your feedback

Q67 How should the EFT Code be reviewed? What alternatives to the current approach should be considered?

Section 12: Other issues

Membership

Issues/options

12.1 As noted in Section 1 (*who subscribes to the Code*), the range of subscribers to the EFT Code remains, with few exceptions, limited to retail banks, credit unions and building societies. This is despite the fact that the EFT Code's scope was broadened considerably following the last review, with the inclusion of the Part B regime regulating SVFs.[212]

12.2 Newer/non-traditional providers of prepaid facilities that have not subscribed include:

(a) retailers issuing gift and other prepaid payment cards;

(b) mobile phone operators allowing customers to pay for goods and services from third parties using their phones;

(c) electronic toll operators;

(d) university card scheme operators; and

(e) transit authorities.[213]

12.3 Generally, the finance company sector has also failed to subscribe. We have not researched why these issuers/operators of prepaid facilities have not subscribed.[214]

Your feedback

Q68 In your view, why has membership of the EFT Code remained limited generally to providers of generic banking services?

Q69 What steps could/should be taken to broaden EFT Code membership?

Q70 How much of the EFT Code's requirements do non-subscribing entities take into account even though they do not subscribe to it?

[212] See the discussion of the 1999 – 2001 Review in Section 1.

[213] Electronic ticketing systems planned for major Australian cities are generally still at the trialling stage. To date, one authority has contacted ASIC about joining the EFT Code.

[214] Extrinsic factors might include lack of awareness of the EFT Code, lack of history of involvement, no ongoing relationship with ASIC as regulator, concern about compliance costs etc.

Design and presentation of the EFT Code

Issues/options

12.4 Preliminary consultations suggest that more could be done, in terms of language, design and presentation, to enhance the accessibility of the EFT Code to staff of subscriber institutions, consumers, and other stakeholders. External stakeholders and ASIC editorial staff have put forward a range of suggestions:

(a) Adopt a more plain language style throughout.

(b) Address the consumer of regulated services/facilities and use direct speech. For example, the first sentence of cl 2.2 might be rewritten as: '*We will give you a copy of the terms and conditions before or when you first use the access method, and at any other time you or the user asks for a copy.*'[215]

(c) Include other introductory material to give the reader a context for the information in the EFT Code (e.g 'About the EFT Code').

(d) Set out 'What the EFT Code covers, and 'What the EFT Code does not cover' in the introductory section.

(e) Simplify how the scope or coverage issues are explained.[216]

(f) Consolidate definition/interpretation sections of Parts A, B and C.

(g) Move definitions to a 'Glossary' or 'Key terms' section to or towards the back of the EFT Code.

(h) Consider whether similar material in Parts A and B on disclosing and changing terms and conditions, and complaints investigation and dispute resolution could be merged to reduce duplication.

(i) Use footnotes instead of the current Endnotes and state clearly that these are interpretative or explanatory only and do not form part of the EFT Code. Another suggestion was that the Endnotes be retained but renamed 'Explanatory Notes'. The status of notes should be made clear in the introductory section (not in cl 20.3 as at present).

(j) Improve clarity by:

  (i) using consistent terminology to describe clauses and sub-clauses of the EFT Code (currently the terms 'clause' and 'paragraph' are used interchangeably; in this paper we have used Clause or cl to describe any part of the Code); and

---

[215] Currently in the EFT Code, this sentence says:
'Account institutions will provide a copy of the Terms and Conditions:
(a) to the account holder prior to or at the time of initial use of the access method; and
(b) at any other time when requested to do so by a user.'

[216] See Section 5.

(ii) having a consistent approach to capitalising terms (e.g. 'Terms and Conditions' is sometimes capitalised and sometimes not).

Your feedback

Q71 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?

Statement of objectives

Issues/options

12.5 ASIC Policy Statement 183 *Approval of financial services codes of conduct* [PS 183] states that a code should clearly set out its objectives: see [PS 183.57]. A number of industry codes have statements of objectives or key commitments or similar wording near the beginning of the document.[217]

12.6 Is it appropriate for a functional code covering a range of industries and providers (such as the EFT Code) to include a statement of this kind? As well as giving the reader (particularly the first time reader) a context for the EFT Code, a statement of objectives could provide criteria for measuring the ongoing effectiveness and efficiency of the Code.

Your feedback

Q72 Should the EFT Code include a statement of objectives? If so, what should the objectives of the EFT Code be?

Other issues you want to raise

Your feedback

Q73 Are there other issues that are not included in this consultation paper that the review should address?

[217] See, for example, cl 1.17 of the General Insurance Code of Practice; cl 2 (Our key commitments to you) of the Code of banking Practice.

Appendix A: International approaches to allocating liability for unauthorised transactions

United States

In the United States (US), unauthorised transaction liability is addressed in legislation passed in the late 1960s (and now codified). Different regimes apply to debit card and other EFT transactions excluding credit accounts, on the one hand; and credit card transactions on the other.

Electronic Funds Transfer Act and Regulation E

The *Electronic Funds Transfer Act*[218] and Regulation E,[219] which implements it, govern electronic funds transfers, excluding credit accounts. Regulation E covers transfers initiated through an electronic terminal, phone, computer or magnetic tape. It includes authorisation by manual signature.

Under Regulation E (pt. 205.6), consumer liability for unauthorised transactions, including multiple unauthorised transactions, is generally limited to USD 50 (or the lower amount of the loss). However, financial institutions are permitted to impose greater liability in certain circumstances, depending—solely—on the consumer's promptness in notifying the financial institution of the loss, theft or unauthorised use of their card.

In summary:

- The consumer normally has 60 days following the transmission of a statement displaying an unauthorised transaction to notify the card issuer of the loss, theft or unauthorised use of their card. For this period, they will have no liability greater than USD 50 if they are unaware of the loss or theft.
- If the consumer becomes aware of the loss or theft during this 60-day period, they have 2 business days in which to notify the card issuer in order to limit their liability to USD 50. If they advise the card issuer after this, but before the expiration of 60 days, they can be made liable for up to USD 500 in losses (provided that the institution establishes that subsequent transfers would not have

[218] 15 U.S.C. 1693 et seq. (2004)
[219] 12 C.F. R. pt 205 (2004) available at http://www.fdic.gov/regulations/laws/rules/6500-100.html

occurred if the consumer had notified the institution within the two-day period).

- Following the expiration of 60 days from the transmission of the statement displaying the unauthorised transaction, the consumer's liability for subsequent losses is unlimited (again, provided that the institution establishes that subsequent transfers would not have occurred if the consumer had notified the institution within the 60-day period).

Note that, for any liability to be imposed under Regulation E, the issuer must provide some means (e.g., signature or PIN) for those who accept the consumer's card to identify the consumer (205.6(a)). When this does not occur (as with fraudulent phone, mail order and internet transactions), consumers cannot be made to face any liability under the Regulation E regime.

Consumer Credit Protection Act and Regulation Z

Under the *Truth in Lending Act*[220] and the implementing Regulation Z,[221] liability for unauthorised use of a credit card, including multiple instances of unauthorised use, cannot exceed USD 50 (or a lower amount if less than USD 50 is lost prior to notification to the card issuer). In contrast to the EFT transactions regime discussed above, there are no additional regulatory incentives to encourage consumers to report loss or fraud.

"Unauthorised use" is broadly defined by Regulation Z. In addition, the card issuer bears the burden of proving that use of a credit card was in fact authorised.

For any liability to arise under Regulation Z the card issuer must meet certain requirements, including the provision of a means to identify the cardholder or an authorised user of the account. In consequence, no consumer liability can arise from unauthorised card-not-present transactions, as there is no method of identification in these situations.

The provisions under Regulation Z apply to be any natural person to whom the card is issued for any purpose (including business, commercial, or agricultural use).

[220] 15 U.S.C. 1601 et seq. (2004)
[221] 12 C.F.R 226 at pt. 226.12, available at http://www.fdic.gov/regulations/laws/rules/6500-100.html

European Union

A range of approaches is currently taken to unauthorised transaction liability issues among European Union (EU) members.[222] With the objective of creating a single payment market among member states, the EU is currently advancing proposals for a New Legal Framework for Payments.[223] To this end, a draft Directive on payment services in the internal market was published in December 2005.[224] This Directive addresses unauthorised transaction issues in detail,[225] adopting an approach based in part on that taken in an earlier European Commission Recommendation.[226]

Under the draft Directive, the user is liable for all unauthorised transaction losses incurred by them a) acting fraudulently; or b) acting with "gross negligence" in failing to:

1. Comply with the terms governing the issue and use of the payment verification instrument, or
2. Notify loss, theft or misuse without undue delay.[227]

Otherwise, prior to notification, the user's liability is limited to a maximum of EUR 150; and this liability only applies to losses resulting from the use of a lost, stolen or misappropriated payment verification instrument (Article 50.1). Further, following notification the payer is not liable for any financial consequences of the unauthorised use, except when they have acted fraudulently (Article 50.3). There is also no liability prior to notification when the payment service provider fails to provide adequate means of notification, again except in cases of fraud (Article 50.4).

The Directive also addresses issues of burden of proof when the user denies having authorised a transaction. First, the payment service provider must "provide at least evidence that the payment transaction was authenticated, accurately recorded, entered in the accounts and not affected by a technical breakdown or some other deficiency" (Article 48.1). If this evidence is provided, the payment user who wishes to

---

[222] For information on these, see comparative tables "National rules related to liabilities in payment services" and National rules related to burden of proof in payment services" at: http://ec.europa.eu/internal_market/payments/framework/comparison_en.htm
[223] The New Legal Framework homepage is: http://ec.europa.eu/internal_market/payments/framework/index_en.htm
[224] Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52005PC0603:EN:NOT
[225] See Preamble paragraph 21, and Articles 45 - 51
[226] Recommendation 97/489/EC
[227] Directive, Article 50.2, together with Article 46

pursue the dispute is then required to provide "factual information or elements to allow the presumption that he could not have authorised the payment transaction and that he did not act fraudulently or with gross negligence…" (Article 48.2). This presumption will not be rebutted merely because the provider can establish that the payment verification instrument was used in the disputed transaction (Article 48.3).

The Directive applies to a wide range of payment services[228], including electronic money within the meaning of Directive 2000/46/EC.[229] Generally, however, the above liability allocation regime does not apply to electronic money except that the payment user is not liable for unauthorised transaction losses following notification if the provider is "technically in a position to freeze or prevent further spending of the electronic money stored on an electronic device" (Article 51.2).

United Kingdom

The relevant regulatory instruments in the United Kingdom (UK) are:

(a) the voluntary Banking Code[230] (UK Banking Code), which was last revised in March 2005; and

(b) the *Consumer Credit Act 1974* (CCA).

UK Banking Code

The UK Banking Code applies to financial institutions in their dealings with personal customers. It applies to any card used by a customer to pay for goods and services or to withdraw cash (including debit, credit, cheque, guarantee, charge cards and cash cards)[231] and to products provided by branches, over the phone, by post, through interactive TV, on the internet, or by any other method.[232]

Under section 12.11 of the UK Banking Code, a customer's liability is unlimited if the institution is able to show they have acted fraudulently. Customer liability may also apply if "you act without reasonable care and this causes losses".[233] Liability may apply in this situation if either:

---

[228] See Annex "Payment Services" under Article 2(1) to the Directive

[229] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0046:EN:HTML

[230] Available at http://www.apacs.org.uk, see under "Payments Industry"

[231] See glossary definition of 'card'. Electronic purses and store cards are specifically excluded.

[232] See s 1.2 of the UK Banking Code.

[233] At p. 41 of the Guidance for Subscribers (March 2005) on the phrase 'without reasonable care'

- the customer fails to comply with various, detailed card, PIN and password security measures set out in section 12.5 of the Code, or
- the customer fails to keep to the terms and conditions for the account.

The UK Banking Code also provides specific recommendations regarding security measures in relation to online banking.[234] Unlike the PIN security measures, however, failure to comply with these is not specifically cited as a failure to take reasonable care.

If the institution is unable to show fraud, or failure to take reasonable care, liability under the UK Banking Code will be limited (under section 12.12) to:

(a) GBP50 prior to notification of loss or theft of the card, or disclosure of PIN;

(b) nothing, if the card details are used without permission and the card has not been lost or stolen, or if the card details have been used in a card-not-present transaction, or if the card is used prior to receipt by the consumer.

Consumer Credit Act

The *Consumer Credit Act 1974* (CCA) governs liability in relation to credit accounts.[235] The definition of a 'credit-token' under the CCA is broad, and has been interpreted to include the use of a credit card, a debit card on an overdrawn account, or a debit card if the transaction has the effect of overdrawing the account. The CCA will take precedence over both the UK Banking Code and individual account terms and conditions in cases of inconsistency.

Under the CCA, a consumer can be made liable for a maximum of GBP50 for losses arising from unauthorised use of the card and there is no requirement for the consumer to take reasonable care. The CCA does not specify the circumstances in which the use will be considered unauthorised, however the UK Banking Ombudsman has indicated that it will look at the card terms and conditions in each case. Cardholders have no liability under the CCA following notification to the card issuer that the card has been lost or stolen.

---

[234] For example: 'Use up-to-date anti-virus and spyware software and a personal firewall … Treat e-mails you receive with caution and be wary of e-mails or calls asking you to reveal any personal security details.' See section 12.9.

[235] This summary is based on commentary in the UK Financial Services Ombudsman News 46, available at http://www.financial-ombudsman.org.uk/ (follow links under "Publications")

The CCA does not actually impose liability; rather it allows the card issuer to do so. Accordingly, the UK Banking Ombudsman has indicated that liability will still generally be determined by reference to the account terms and conditions.

New Zealand

Members of the New Zealand Bankers' Association (NZBA) observe the New Zealand Code of Banking Practice (NZ Banking Code),[236] as a minimum standard. The NZ Banking Code is currently under review, having last been revised in 2002.

Paragraph 3.9 of the NZ Banking Code deals with "Your liability – cards, pins, and passwords". It defines 'cards' to include any cards that can be used to pay for goods and services, or to access ATM machines or other electronic banking services such as EFTPOS. Credit cards, charge cards, debit cards, cash cards, stored value or smart cards and multi-function cards are specifically listed.[237]

Customer liability is specifically excluded in several situations[238], including before the customer receives their cards, PINs or passwords; or when it is clear that the consumer could not have contributed to the loss. Generally, consumers have no liability for unauthorised transactions following notification of lost or stolen cards or disclosure of PIN or password. Liability prior to notification is otherwise generally limited to NZ$50.

However, this is subject to an extensive and non-definitive list of exceptions when the customer will be liable in full. For instance, the customer is not protected: if they have 'acted fraudulently or negligently'; if they breach the bank's terms and conditions; if they select 'unsuitable pins or passwords' (broadly defined), if they fail to 'reasonably' safeguard cards, if they fail to take 'reasonable' steps to prevent disclosure when keying in PINS or passwords; and in a range of other circumstances.[239]

While there is scope for subscribers to incorporate liability provisions into card terms and conditions,[240] they may not impose terms more onerous than those imposed by the NZ Banking Code.[241] Subscribers are also required to undertake to use their 'best endeavours to make sure that

---

[236] Available at http://www.nzba.org.nz/public.asp
[237] See paragraph 5.1, Glossary, NZ Code of Banking Practice.
[238] See paragraphs 3.9 (a) – (c) and (f), NZ Banking Code, for a full list
[239] See paragraph 3.9 (d), NZ Banking Code
[240] See paragraph 3.9(b), NZ Banking Code.
[241] 'Code of Banking Practice December 2002', Sally Peart, *Lawlink Magazine*, Autumn 2003, Volume 19, Issue 1, available at http://www.lawlink.co.nz/resources/publications.asp#autumn2003.

our banking systems and technology are secure'.[242] The NZ Banking Ombudsman has indicated that this undertaking applies to all banking services, including internet banking.[243]

The NZ Banking Code provides no guidance as to which party carries the burden of proof in determining liability for unauthorised transactions.[244]

Canada

Code of Practice for Consumer Debit Card Services

The Canadian Code of Practice for Consumer Debit Card Services (Canadian Code),[245] which was revised in 2004, requires endorsees to maintain or exceed the Code's consumer protection standards. The Canadian Code only applies to the use of debit cards and PINs to access point-of-service terminals, such as automated banking machines (ABMs), point-of-sale (POS) terminals and debit card terminals in the home.

Section 5 of the Code provides a non-definitive list of circumstances when the consumer will not be liable for losses. Cardholders are not liable for losses resulting from circumstances 'beyond their control', including:

(a) technical problems or system malfunctions;

(b) unauthorised use when the card issuer is responsible for preventing such use (e.g. following notification of the loss or theft of the card or possible PIN disclosure, or following cancellation or expiry of the card);

(c) when the cardholder has unintentionally contributed to the unauthorised use, provided they cooperate in any subsequent investigation.

In all other cases when the cardholder contributes to unauthorised use, they are liable for the resulting loss. The cardholder will contribute to the loss by, for example, disclosing their PIN, writing or poorly disguising their PIN, or by failing to notify the issuer within a reasonable time of the loss or theft of the card, or possible disclosure of the PIN. Choosing a PIN combination from the cardholder's name, address, telephone number, date of birth, or social insurance number (SIN) is considered to

---

[242] See para 1.2(b)(iii) of the NZ Banking Code.

[243] The Office of the Banking Ombudsman Newsletter No. 18, May 2005, available at http://www.bankombudsman.org.nz/documents/May_2005_newsletter.pdf

[244] The NZ Banking Ombudsman has indicated that this aspect requires clarification. See footnote above.

[245] Available at http://www.cba.ca/en/viewdocument.asp?fl=3&sl=65&tl=135&docid=266&pg=1.

be a voluntary disclosure; however, the PIN issuer also has an obligation to advise the cardholder of typical PIN combinations to avoid for security reasons.[246]

The Canadian Code also provides guidance on the interpretation of the liability provisions which indicates that the 'reasonableness of an attempt to disguise a PIN should be assessed from the point of view of the reasonable cardholder, not from the point of view of the thief or the card issuer's official who through experience have become familiar with many types of disguises and their strengths and weaknesses'.[247]

The PIN issuer must show on the balance of probabilities that the cardholder contributed to the unauthorised use before any liability can be imposed on the cardholder. [248] The interpretation of an authorised transaction specifically excludes situations when the cardholder has been the victim of 'trickery, force intimidation or theft'.[249]

[246] See para 2.2(e) and Appendix A, cl 5.4 of the Canadian Code.
[247] See Appendix A, cl 5.6 of the Canadian Code.
[248] See paragraph 6.6 of the Canadian Code.
[249] Appendix A, cl 1 of the Canadian Code

Appendix B: Consolidated list of questions

Section 2: Marketplace developments

Q1 What do you see as the emerging trends or developments in the consumer payments marketplace in Australia over the next few years?

Q2 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?

Q3 What are the issues associated with the emergence of 'non-contact' payment facilities?

Section 3: Growth in online fraud

Q4 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?

Q5 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?

Q6 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.)

Q7 What information can you provide to the Working Group about the online fraud mitigation skills of Australian online users?

Section 4: Regulatory developments

Q8 Are there developments in the regulatory environment that the Review Working Group should particularly consider? What are the implications of those developments for the EFT Code?

Section 5: EFT Code, Part A (Scope and interpretation)

How the scope of Part A is defined	**Q9**	Do you have any suggestions 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?
Biller accounts exclusion (cl 1.4–5)	**Q10**	Should biller accounts continue to be excluded or should cl 1.4 be modified or, alternatively, removed altogether?
Small business account holders	**Q11**	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?

Section 6: EFT Code, Part A (Requirements)

Notifying changes to fees (cl 3)	**Q12**	Should the requirement in cl 3.1 to provide written notification in advance of an increase in a fee or charge be replaced by another process? For example, should the notice appear in the national or local media on the day on which the increase starts?
Issuing transaction receipts (cl 4.1)	**Q13**	Should cl 4.1(a) be revised to allow users to 'opt-in' to receive a receipt?
	Q14	Should cl 4.1(a) be revised to deal with the practical problem of ATMs or other machines running out of paper for receipts? If so, how should it be amended?
Merchant identification on transaction receipts (cl 4.1)	**Q15**	Should cl 4.1(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?
When a transaction receipt should disclose remaining balance (cl 4.1)	**Q16**	Should the EFT Code give more guidance on cl 4.1(a)(viii) regarding balance disclosure on receipts? If so, what guidance should be added?
Consistency between EFT Code and Corporations Act (cl 2–4)	**Q17**	Is there duplication or inconsistency between Part A of the EFT Code and the requirements of the Corporations Act that should be reviewed? How should any such issues be dealt with?
	Q18	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?

Obligation to advise account holder of discrepancies (cl 7)	**Q19**	Should cl 7 be revised to specifically require subscribing institutions to identify and correct discrepancies between amounts recorded on the user's electronic equipment or access method as transferred, and amounts recorded by the institution as received? What are your views on the suggested redrafting?
What is a 'complaint'? (cl 10)	**Q20**	Should the EFT Code include a definition of the term 'complaint' under cl 10? If so, should it adopt the definition in AS ISO 10002–2006? 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?
Standard for internal complaint handling	**Q21**	Should AS ISO 10002—2006 become the required standard for internal complaint handling under the EFT Code?
Meaning of 'immediately settled' complaint (cl 10.3)	**Q22**	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 cl 10.3)? If so, what is an appropriate period?
Timeframes for resolving complaints (cl 10.5)	**Q23**	Should any changes be made to the timeframe for resolving complaints under cl 10 of the EFT Code?
Internal complaints handling	**Q24**	Do you have information or views about the level of compliance with cl 10?
	Q25	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?
Investigating complaints and availability of records	**Q26**	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 a dispute resolution body is entitled to resolve a factual issue to which a record relates on the basis of the evidence available to it?
Time limit on resolution of complaints under the EFT Code	**Q27**	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?

Section 7: EFT Code, Part A (Liability; mistaken payments)

Circumstances when account holder is liable

Q28 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 issues would have to be addressed?

Q29 Should an additional example be included in cl 5.6(e) specifically referring to the situation when an account user acts with extreme carelessness in responding to a deceptive *phishing* attack?

Q30 Apart from this possible clarification, should account holders be exposed to any additional liability under cl 5 for unauthorised transaction 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?

Q31 To what extent has the restriction on using a user's name or birth date under cl 5.6(d) been relied on?

Q32 Should the restriction on users acting 'with extreme carelessness in failing to protect the security of all the codes' under cl 5.6(e) be further elaborated or extended in some way? Should additional examples of extreme carelessness be given?

Q33 Should the EFT Code specifically address the situation when an unauthorised transaction occurs after a user inadvertently leaves their card in an ATM machine?

Unreasonable delay in notification (cl 5.5(b))

Q34 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.)

Q35 Should the circumstances when the 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?

Q36 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?

'No fault' liability limit (cl 5.5(c))	**Q37**	To what extent do subscribing institutions currently use the other 'no fault' liability provision in cl 5.5(c)?
	Q38	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?
Liability allocation and 'book up'	**Q39**	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?
Liability in cases of system or equipment malfunction (cl 6)	**Q40**	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?
Mistaken payments	**Q41**	To what extent, and how, should the EFT 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.

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

Scope of Part B	**Q42**	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?
Other aspects	**Q43**	Assuming the scope of Part B of the EFT Code continues to be defined in terms of the concepts of 'stored value facilities' and 'stored value transactions', what changes, if any, should be made to the definitions and other provisions of cl 11?

Section 9: EFT Code, Part B (Obligations)

Record of available balance (cl 14)	**Q44**	Should any changes or additions be made to cl 14?
	Q45	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?
Consistency between Part B and Corporations Act (cl 12–14)	**Q46**	Are any aspects of Part B of the EFT Code incompatible with the requirements of the Corporations Act? How should any incompatibility be addressed?
Right to exchange/replace stored value (cl 15)	**Q47**	Should the rights to exchange stored value under cl 15 be narrowed?
	Q48	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?
	Q49	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?
Right to refund of lost or stolen stored value (cl 16)	**Q50**	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?
	Q51	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?
Right to unilaterally vary terms and conditions	**Q52**	Should the use of unilateral variation clauses in the terms and conditions for facilities regulated under Part B be restricted?
Complaint investigation/dispute resolution (cl 19)	**Q53**	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?
Payment finality	**Q54**	Should Part B of the EFT Code address the issue of payment finality?

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

Privacy obligations (cl 21)	**Q55**	Should the provisions about privacy under cl 21 be modified and/or extended to cover other areas or issues?
	Q56	Should the status of the cl 21.2 guidelines be changed to make these provisions contractually binding requirements?
	Q57	Should the EFT Code require that transaction receipts include only a truncated version of the account number?
	Q58	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?
	Q59	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 timeframe?
Electronic communications (cl 22)	**Q60**	Should cl 22.1(b)(ii) be deleted or amended in some way?
	Q61	Should cl 22.2(b)(ii) be deleted or amended in some way?
	Q62	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?
	Q63	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?

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

The administrator's role	**Q64**	Should ASIC continue to be primarily responsible for administering the EFT Code? Are there other arrangements that should be considered?
Modifying the EFT Code	**Q65**	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?
Monitoring compliance	**Q66**	How should compliance be monitored? What alternatives to the current self-reporting survey should be considered?
Reviewing the EFT Code	**Q67**	How should the EFT Code be reviewed? What alternatives to the current approach should be considered?

Section 12: Other issues

Q68 In your view, why has membership of the EFT Code remained limited generally to providers of generic banking services?

Q69 What steps could/should be taken to broaden EFT Code membership?

Q70 How much of the EFT Code's requirements do non-subscribing entities take into account even though they do not subscribe to it?

Q71 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?

Q72 Should the EFT Code include a statement of objectives? If so, what should the objectives of the EFT Code be?

Q73 Are there other issues not covered in this consultation paper that the review should address?