Peter Mulligan

Solicitor and Head of Banking & Insolvency
Commonwealth Bank of Australia
Sydney

Self Regulation

A well established trend in financial services delivery is so called "self regulation" via the use of industry codes of practice. There has been a proliferation of these codes over the last decade, one of the earliest being the EFT Code of Conduct (EFT Code) which came into effect in January 1991. But we also have the Code of Banking Practice (CBP), the Small Business Principles, the Privacy Code, the Franchising Code, the Life Insurance Code of Practice and the General Insurance Code of Practice. I'm not even going to talk about the Consumer Credit Code (CCC) since that is, after all, simply legislation, not self regulation. Other Codes have come and gone along the way.

As well as the Privacy Code which was developed to explain the Privacy Commissioner's views on what is meant by the labyrinthine provisions of Part IIIA of the Privacy Act which regulates privacy issues regarding provision of consumer credit, we now have the National Privacy Principles which came into operation in December last year.

We are waiting for Australian Prudential Regulation Authority (APRA) to finalise its principles on outsourcing arrangements for Financial Institutions (FI) (expected in July).

The Minister for Financial Services also in May 2000 issued guidelines for development of standards for doing business online.' (Building Consumer Sovereignty in Electronic Commerce — A best practice model for business.)

The point about this self regulation from the legal perspective is that the Codes impose legal obligations on industry participants. They do this via the "two way liability " approach. The Codes contain a provision requiring the participant to warrant in its contracts with customers that it will comply with the Code. They also have a mechanism whereby the participant will make a public announcement that it adopts the Code. If the participant includes the warranty in its contracts then of course it is contractually bound to its customers. If it neglects to include that warranty in its contracts then it is guilty of misleading conduct under Trade Practices Act and in practical terms the result is the same as if it had given the warranty. So, once an FI has "voluntarily" adopted a Code, it has taken on a whole new set of obligations

which are for practical purposes as binding on it as if they were enshrined in legislation. These obligations are treated very seriously by FIs and they take a large amount of resources in ensuring compliance with what are often overlapping requirements of these codes. This is of course, a problem which applies generally to all modes of delivery of financial services but there are some particular examples which apply to online delivery.

Electronic Notices

The EFT Code, which in its revised form became fully operational in April 2002, contains Clause 22 which enables an FI and its customer to agree that information, which the Code requires to be provided to the customer, may be provided electronically instead of by paper. The customer's agreement must be by "specific positive election" and the customer can at any time opt out and revert to paper notification. If sufficient numbers of customers give their specific positive election to this innovation, there is a potentiality for great savings for FIs giving bulk notifications. This will particularly be so once the revised CBP comes into force. The present draft contains a similar provision to that which appears in the EFT Code. The scope of the CBP is much greater than the EFT Code in the range of customers it will apply to (includes small business as well as individuals) and also the range of information which banks and their subsidiaries are to provide. There is also the potentiality for these arrangements to apply to communications required to be given under the CCC.

These electronic communications may be given either by email to the customer's nominated email address or by leaving a "you've got mail" notice at that address which enables the customer to link to the FI's secure website and read the message there. Now I notice a number of statements on the Privacy Commissioner's website about the "technical realities" of email use. I quote from Guidelines on Workplace Email:-
"**Most e-mail is insecure**. It should be regarded as insecure unless it has been encoded or encrypted. E-mail is often compared to a postcard in that anyone who receives it can read it". These messages are likely to contain personal and confidential information eg account statements, particulars of amounts of credit, interest rates etc.

I would take it therefore that the Commissioner's office might have some feelings of unease (one might almost say insecurity) about arrangements under EFT Code and CBP which allowed for the straight email option. At least if that option is to be used, I would expect that the full explanation which has to be given to the customer before they make their specific positive election to accept email notification, should draw attention to this shortcoming.

The FSR Act also contains provisions permitting electronic communication of required notifications (eg Statements of Advice, Product Disclosure Statements and Confirmations.) There is no requirement for a "specific positive election" by the customer but the provision of an email address would probably be some indication that a customer was prepared to receive communications in that way. Nevertheless, I would suggest it would be prudent to use the "you've got mail" technique for any communication containing confidential information.

Where's The Evidence?

Another essential matter to cover off when entering into contracts online is to maintain historical replicas of the screens. It is one thing to capture all the data and retain it, but it is also essential that the complete context in which the data was input by the customer can be shown. Most acceptances of terms and conditions online are effected by a mouse click. But if there ever arose a dispute as to what terms a customer accepted, of how they presented on the screen in terms of layout, font, bolding etc, or even to show that a customer could not have made a transaction without stepping through the screen containing the terms and conditions then the FI will have to be able to reproduce the web pages exactly as they appeared at the relevant time, which could be years previously.

Liability For Unauthorised Transactions

The revised EFT Code contains substantially changed rules (in Clause 5) about liability for unauthorized transactions. The basic proposition is in 5.4 – The accountholder has no liability for losses arising from unauthorized transactions where it is clear that the user has not contributed to such losses. This is analogous with the position which applies to forged signatures on cheques established by such cases as NAB v Hokit[1]. That case, as we know, confirms that customers only have to report forgeries they are actually aware of and are under no obligation to check their statements to detect unauthorized drawings.

With the EFT Code an exception is made in the case of a user contributing to losses eg by failing to keep devices secure or failing to report them lost or stolen when they should reasonably have become aware of the loss or theft. This gives rise to an anomaly in the case of misuse or theft of "identifiers" which are not "devices". An example would be account details taken off a credit or debit card. These could be misused by the thief to make telephone orders. The account holder has no obligation to report the misuse of an identifier on a "should reasonably have become aware" basis – ie no obligation to check their account statements and report misuses to their FI. The EFT Code precludes the FI from imposing any

[1] *National Australia Bank Limited v Hokit Pty Limited & Ors* (1996) 39 NSW LR 377

such obligation on the customer since that would alter their liability from that which the Code provides. By contrast, an obligation could be imposed for paper based transactions since these are not covered by EFT Code.

The EFT Code recognises the possibility that chargeback claims might be made for unauthorised transactions, so as to recoup some of the losses from the merchant's bank (which will usually in turn claim them from the merchant). There are time limits for chargeback claims to be made, and the cardholder's bank must allow credit to the cardholder for amounts which it could have claimed on a chargeback but failed to do so. However, with these unauthorised telephone transactions there is no corresponding obligation imposed on cardholders to check their statements in sufficient time to enable a chargeback claim to be made.

FIs can get some protection by imposing floor limits on telephone orders, but apart from that I think they will be restricted to sending words of advice and encouragement to customers to "please check your statements" without being able to insist that they do so (see clause 5.8(b)).

Peter Mulligan
Solicitor, Commonwealth Bank of Australia