LexisNexis
Questions and Answers

Banking Law in Australia

2nd edition

Robin Edwards
LLM, PhD (Monash)
Adjunct Professor
Department of Business Law and Taxation
Monash University

LexisNexis Butterworths
Australia
2012

Chapter 10

Credit Cards, EFTPOS, Smart Cards and Internet Banking

Key Issues

10-1 The obvious characteristic of the credit card is that the cardholder is extended credit by the card issuer. The system as originally set up in 1974 worked with paper: see A L Tyree, *Banking Law in Australia*, 7th ed, LexisNexis Butterworths, Sydney, 2011, [9.7].

Security with a signature credit card is protected because of the need for the cardholder to sign the authorisation slip at the point of sale. If the card is properly swiped by the merchant then the signed authorisation triggers payment from the card issuer to the merchant.

Typically with a credit card, there is a three-part agreement:

1. there is an agreement between the consumer and the card issuer setting out the terms and conditions for use of the credit card;
2. there is an agreement between the merchant and the card issuer detailing the merchant's responsibilities in terms of obtaining payment from the card issuer;
3. there is the agreement between the consumer and the merchant for the purchase of goods and services with the credit card.

Despite considerable legal doubts about the interpretation of theses agreements, the lack of cases is perhaps a testimony to the practical efficacy of credit cards.

There are also now PIN (personal identification number) credit cards, where the consumer keys in a personal identity number. Such PIN credit cards are governed by the Electronic Funds Transfer Code of Conduct (EFT Code), in particular in regard to allocation of fraud loss, whereas the signature credit card fraud loss allocation is governed by the terms of the contract between the cardholder and the issuer.

Both PIN and signature credit cards are subject to chargeback rights for the cardholder, set out in the Code of Banking Practice (the Banking Code). Basically, the chargeback process is initiated by the cardholder, whose bank contacts the merchant's bank with the reason for the

complaint, and the card payment to the merchant is reversed. The onus is then on the merchant to combat this by showing that the complaint and the reversal are not justified.

Chargeback rights may be able to be utilised by the credit card holder for:

- unauthorised transactions;
- non-delivery of goods or services; and
- disputes about goods and services.

EFTPOS (Electronic Funds Transfer at Point of Sale) is one of the fastest-developing forms of payment to the retailer. The customer of the issuing institution is provided with a card and a PIN. The card is 'swiped' and the consumer uses a keypad to enter his or her PIN. The consumer's account at the issuing institution is accessed online. EFTPOS cards are usually debit cards, so that the amount is taken from the customer's account. They can also involve a line of credit to the customer with a credit card. With the debit cards, the amount taken from the customer's account is transferred to the retailer, who is also online. Most of the complaints relating to debit cards revolve around the issue of PIN confidentiality: see Tyree, 2011, [9.6.2].

One of the recent developments in the story of EFT transfers is the development of the 'smart card', which has an embedded microprocessor chip that is capable of storing a great deal of information. Current cards like those used at EFTPOS and ATMs (automated teller machines) have a magnetic stripe on them and communication with a host computer is necessary to obtain authorisation (although many of these now also use microprocessor chips). Smart cards, on the other hand, can work at terminals without a link up and the account records and other information can be kept in the card itself. The smart card has been graphically described as an electronic purse. Typically, such cards can be recharged with value at an ATM or even over the Internet.

There have been a number of versions of the EFT Code; one in 1989 and another in 2002 (this is the current code of conduct). There is a review of it underway that was commenced in 2007, and a new version of the EFT Code is scheduled for introduction mid-2012: see Tyree, 2011, [10.6.3].

The current EFT Code covers remote access to accounts; for example, telephone transfers, email and Internet transfers, and transfers using television etc. It does not cover things such as electronic bills of exchange, electronic letters of credit and electronic applications for loans. It also does not cover transfers to and from accounts primarily used for business purposes: see EFT Code cl 1.3.

The term 'access method' has a wide definition in the EFT Code. It thus encompasses plastic cards used with a PIN, but goes beyond this. The EFT Code defines 'access method' in a very broad way so that it covers, for example, magnetic strip cards, biometric identifiers (for example, iris

readers), cards with chips, digital signatures, passwords and the like. The Code does not, however, cover manual signatures where this is the principal intended means of authenticating a user's authority to give the instruction; for example, when a person signs a credit account voucher when using a credit card. The EFT Code defines 'access method' in cl 1.5.

Loss allocation is probably the most important part of the EFT Code and provides for relatively clear rules for allocation of loss. The choice is usually between the consumer and the financial institution, as the rogue responsible for the loss will usually not be able to be found. These rules apply where a credit card is used with a PIN or to any other EFT application; for example, an unauthorised ATM transaction, an unauthorised debit transaction, or unauthorised use of credit card numbers over the telephone or Internet.

Broadly speaking, the current EFT Code provides that a consumer will only be liable in three situations under cl 5 (the same test is envisaged for the future revised code):

1. Where the bank can affirmatively prove the user's fraud or breach of the security requirements in regard to the user's secret code and that this contributed to the loss.

   The reference to security requirements above means that the user cannot:

   a) voluntarily disclose one or more of the codes to anyone;
   b) indicate one or more of the codes on the outside of the access device, or keep a record of one or more of the codes (without making any reasonable attempt to protect the security of the code records) so that they are liable to loss or theft simultaneously. Likewise, where there is no access device;
   c) after the adoption of the current EFT Code select a code that represents the user's birth date or part of the user's name having been warned by the bank not to select such a code;
   d) act with extreme carelessness in failing to protect the code/s;

   [see cl 5.6.]
2. where the bank can affirmatively prove the user delayed notifying of loss or theft or breach of security requirements; and
3. where a secret code (typically the PIN) is required and neither 1 nor 2 above apply, the user is liable for no more than $150.

The EFT Code was seen initially as an alternative to legislation, the path followed by the United States. Although it is described as a 'code' and as being voluntary, those financial institutions that decide to follow must reproduce its terms in the contract between the card issuer and the cardholder and, moreover, they must warrant that they have incorporated the Code's key features. Failure to comply with this warranty would signify the institution's breach of s 12DB(i) of the Australian Securities and Investments Commission Act 2001 (Cth) and the institution would be liable for a penalty as well as having civil liability.

Content not included.