

Bankwest Credit Card Account Access

Conditions of Use

1 July 2010

About these Conditions of Use

These Credit Card Account Access Conditions of Use apply to your use of a credit card, Bankwest Online Banking, Phone Banking and Pay AnyBody to access a credit card account in circumstances where we tell you that these Credit Card Account Access Conditions of Use form part of the credit card contract between us.

This document does not contain all of the information we are required to give you before entering into a credit contract. Other information is contained in the Credit Card Schedule and the Credit Card Conditions of Use.

Each of these Services provides you with access to Bankwest credit card accounts which we agree you may nominate.

You must read these Credit Card Account Access Conditions of Use together with the Credit Card Schedule and the Conditions of Use specific to the credit card account. All three documents comprise your credit card contract. If there is an inconsistency between these Credit Card Account Access Conditions of Use, and the Conditions of Use specific to the credit card account, these Credit Card Account Access Conditions of Use prevail in respect of EFT transactions.

Customer enquiries

Please call **13 17 18** or visit **bankwest.com.au**.

Where to report lost or stolen cards or suspected unauthorised transactions (24 hours):

Within Australia **13 17 18** (cost of a local call)

Outside Australia **+61 8 9449 2840**.

Contents

Part 1 – General	1
1.1 Definitions	1
1.2 EFT Code	3
1.3 Changes	3
1.4 Cancellation of electronic access	3
1.5 Additional Cardholders	4
1.6 Access to a nominated cheque or savings account	4
1.7 Privacy	4
Part 2 – Cards Conditions of Use	5
2.1 About this Part	5
2.2 Access to your Card account	5
2.3 How much cash can you get?	5
2.4 Paying bills using your Card	6
2.5 Deposits	6
2.6 Transactions at EFT terminals	6
2.7 Do transactions have to be authorised by us?	7
2.8 Use of Card at Merchants, financial institutions or our agents	7
Part 3 – Phone Banking and Bankwest Online Banking Conditions of Use	8
3.1 About this Part	8
3.2 What is Phone Banking?	8
3.3 What can be done using Phone Banking?	8
3.4 How to use Phone Banking	9
3.5 What is Bankwest Online Banking	9
3.6 What can be done using Bankwest Online Banking?	9
3.7 How to use Bankwest Online Banking	9
3.8 Internet security and privacy	9
3.9 Access and restriction of access to Services	10
3.10 Future payments	11
3.11 Limits	11
3.12 Other matters	11
3.13 Authorised users	11
3.14 BPAY Payments	11
3.15 BPAY View	15
Part 4 – Pay AnyBody Conditions of Use	18
4.1 About this Part	18
4.2 What is Pay AnyBody?	18
4.3 Daily Pay AnyBody transfer limit	18
4.4 Making a Pay AnyBody transfer	18
4.5 Postdated Pay AnyBody transfers	19
4.6 Cancelling a Pay AnyBody transfer	19
4.7 Mistakes as to the amount of a Pay AnyBody transfer	19
4.8 Processing Pay AnyBody transfers	19
4.9 If we make the wrong payment	19

Part 5 – Regular Payments	20
5.1 About this Part	20
5.2 Maintain a record of any Regular Payment Arrangements	20
5.3 Changing Regular Payment Arrangements	20
Part 6 – Security of Access Methods	21
6.1 What do users need to do to safeguard their Access Methods?	21
6.2 Guidelines	21
Part 7 – Loss, Theft or Unauthorised Use of Your Access Method	24
7.1 What users have to do	24
7.2 What is your liability for unauthorised EFT transactions?	24
7.3 What is your liability for other unauthorised transactions?	27
7.4 When the electronic banking system or EFT terminal malfunctions or breaks down	27
Part 8 – Procedures For Handling Errors and Disputed Transactions	28
8.1 How will any errors, mistakes and disputes be handled?	28
8.2 Outcome	30
8.3 If you are not satisfied	31
8.4 If we fail to comply with these procedures	31

Part 1 – General

1.1 Definitions

In addition to the definitions in the Bankwest Credit Card Conditions of Use, the following definitions apply to this document:

Access Method means a method the use of which we authorise and accept as providing authority to us to act on an instruction given through Electronic Equipment.

A reference to an Access Method includes a reference to each of its individual components and includes, but is not limited to, a Card, Card Details, a Security Token, a Secret Code or any combination of these. It does not include a method where a manual signature is the principal means of verifying the authority to give the instructions.

Approved Browser means a browser which can be used to access Bankwest Online Banking and Online Business Banking. A list of these browsers can be accessed at <http://www.bankwest.com.au> – enter ‘browser’ in the search box to find the list.

ATM means an automatic teller machine.

BPAY® Scheme means a Service which allows you to make BPAY payments electronically and receive or access bills electronically via BPAY View. We are a member of the BPAY Scheme. We will tell you if we cease to be a member of the BPAY Scheme.

BPAY Pty Ltd means BPAY Pty Ltd ABN 69 079 137 518, PO Box 3545 Rhodes NSW 2138. Tel: (02) 9646 9222.

BPAY View means an electronic Service offered as part of the BPAY Scheme which allows you to view bills from a nominated Biller electronically.

Card means the credit card issued by us in accordance with the Bankwest Credit Card Conditions of Use.

Card Conditions of Use means the specific Conditions of Use we provide to you together with these Credit Card Account Access Conditions of Use and which we tell you form part of the Card contract.

Card Details means the information printed on a Card and includes, but is not limited to, the Card number and expiry date.

Cardlink Services Ltd means Cardlink Services Ltd ABN 60 003 311 644, Level 4, 3 Rider Boulevard, Rhodes NSW 2138. Tel: (02) 8754 2800.

EFT Code means the Electronic Funds Transfer Code of Conduct.

EFT System means the shared system under which EFT transactions are processed.

EFT Terminal means any terminal connected to the electronic banking system and authorised by us for use with an Access Method to conduct an EFT Transaction, including ATMs and EFTPOS terminals.

EFT Transaction means an electronic funds transfer from or to an account with us initiated by a User through Electronic Equipment using an Access Method.

EFTPOS Terminal means an electronic funds transfer point of sale terminal.

Electronic Equipment includes, but is not limited to, a computer, television, telephone and an EFT Terminal.

Merchant means a supplier of goods or services.

PAN means a personal access number of up to ten characters allocated to a User by us to identify the User for the purposes of accessing Phone Banking and Bankwest Online Banking.

PIN means the personal identification number we allocate a User for use with a Card, as changed by you or us from time to time.

Secret Code means individually and collectively a User's PIN, Token Code, Secure Code and Token PIN.

Secure Code means the Access Method required by users, along with a PAN, to access Phone Banking or Bankwest Online Banking. For Phone Banking the Secure Code is a four digit number. For Bankwest Online Banking the Secure Code is an alphanumeric code of 6 – 10 characters or, for those users with a Security Token, a ten digit code which is a combination of the Token PIN and Token Code.

Security Token means, if we have provided one to a User, the physical device which generates a Token Code.

Service means Phone Banking or Bankwest Online Banking, including the BPAY Scheme or Pay AnyBody service.

Token Code means a random six digit code generated by a Security Token. The security of a Token Code is breached if the Security Token is lost, stolen or allowed to be seen by any person other than the User.

Token PIN means a four digit code which is chosen by users who have been provided with a Security Token.

User means you and/or any Additional Cardholder.

WST means Western Australian Standard Time.

we and **us** means the Bank of Western Australia Ltd ABN 22 050 494 454 AFSL 236872 of 108 St Georges Terrace, Perth Western Australia 6000 and includes its successors and assigns.

Any other grammatical form of the word 'we' has a corresponding meaning.

you means the holder of the Card account. Unless otherwise required by the context, a singular word includes the plural and vice versa.

1.2 EFT Code

We will comply with the requirements of the EFT Code where those requirements apply to your dealings with us.

1.3 Changes

Changes to these Credit Card Account Access Conditions of Use.

We can change these Credit Card Account Access Conditions of Use at any time. We will give you notice by writing to you at least 20 days (or such longer period required by law) before we:

- (a) impose or increase charges relating solely to the use of an Access Method or the issue or use of any additional or replacement Access Method;
- (b) increase your liability for losses relating to EFT transactions;
- (c) impose, remove or adjust a daily or other periodic transaction limit applying to use of an Access Method, your Card account or Electronic Equipment;

except where an immediate change is necessary to restore or maintain the security of the EFT system or a Card account.

Subject to any applicable legislation, we shall notify you of other changes to these Conditions of Use no later than the day that the change takes effect by:

- (a) a notice on or with your Card account statement;
- (b) publishing a press advertisement; or
- (c) notices on EFT terminals or in our Customer Service Centres, except where an immediate change is necessary to restore or maintain the security of the EFT system or a Card account.

1.4 Cancellation of electronic access

We may suspend or deny access to a User to the Services or your Card account at any time without prior notice, in certain circumstances including (but not limited to):

- suspected fraudulent use;
- to comply with anti-money laundering and counter-terrorism financing laws;
- unsatisfactory account operation;
- non-compliance with these Credit Card Account Access Conditions of Use; or
- if we consider a security issue has arisen which requires further investigation.

If in such circumstances we cancel a Card, you may request a replacement Card unless we decide not to provide you with further credit. In the event that electronic access to your Card account is cancelled by you or us, you must, if relevant, halt the use of any Security Token and return it to us undamaged.

The Bank has an obligation under the Code of Banking Practice to act fairly and reasonably towards you in a consistent and ethical manner.

1.5 Additional Cardholders

You agree that you are responsible to ensure that Additional Cardholders comply with these Credit Card Account Access Conditions of Use and to ensure that each Additional Cardholder protects their Access Method in the same way as these Credit Card Account Access Conditions of Use require you to protect your Access Method.

1.6 Access to a nominated cheque or savings account

Account access to a nominated account by a User is not governed by these Conditions of Use but by the Bankwest 'Account Access Conditions of Use'. Users should refer to those Conditions of Use for information about the use of the Card to access a nominated account.

You acknowledge that by linking a nominated account to your Card you increase the risk of loss for which you could be liable if the Card is used without a User's knowledge or consent.

You agree that any User will have authority to operate a nominated account.

1.7 Privacy

- (a) We may collect personal information about you or a User for the purposes of providing our products and services and may use and disclose that information in accordance with our Privacy Policy.
- (b) We may disclose personal and transactional information to others in order to execute instructions given to us (including use of the BPAY Scheme), including:
 - (i) any party nominated to receive a payment;
 - (ii) BPAY Pty Ltd and any agent appointed by it from time to time, including Cardlink Services Ltd who provides the electronic systems to implement the BPAY Scheme; and
 - (iii) agents and contractors we may use in providing any of our Services.
- (c) Users may have access to the personal information we hold about them at any time by asking us.

- (d) You can request access to information held by BPAY Pty Ltd or its agent Cardlink Services Ltd using the contact details supplied in Clause 1.1.

For more details of how we handle your personal information, please refer to our Privacy Policy, available from our website (bankwest.com.au) or by telephoning us.

Part 2 – Cards Conditions of Use

2.1 About this Part

This Part (together with Parts 1, 6, 7 and 8) applies to all transactions involving the use of the Card itself or the Card Details to access your Card account.

2.2 Access to your Card account

(a) Over the counter (including EFTPOS terminals), mail order, telephone and online

Users can use their Visa and MasterCard® in Australia and overseas over the counter at financial institutions and Merchants displaying the appropriate Card symbol. If a Merchant accepts payment with your Card by mail order, telephone or online, users may authorise payment in the manner required by the Merchant by providing the Card Details to the Merchant.

(b) ATMs

Users may use their MasterCard or Visa Card and PIN to obtain cash advances in Australia and overseas at ATMs displaying the appropriate symbol.

2.3 How much cash can you get?

(a) Subject to (b):

The minimum amount a User can obtain each day from our ATMs is \$20 or \$50 (depending on the ATM), otherwise it will be determined by the institution from which the cash advance is obtained. A maximum daily ATM transaction limit also applies. Users will be advised of this limit when their Card is issued. Other financial institutions and our agents may set their own limits.

Cash advances may not be obtained using EFTPOS terminals but are available at our Customer Service Centres up to the amount of available credit. Banks overseas displaying the appropriate Card symbol may arrange a cash advance in local currency from the Card account. This is subject to their own cash advance transaction limit, their own country's exchange control requirements, any fees they may charge and your available credit limit.

- (b) A maximum monthly cash advance limit may apply. The amount of the limit will be at our discretion, may vary monthly and will be determined according to our credit risk assessment of you, the period for which the Card account has operated and your payment history.

2.4 Paying bills using your Card

Users can pay utility accounts such as water, gas and power from the Card account by mail or telephone (if applicable) quoting their Card Details. The transaction will be treated as a purchase by us.

If a User pays such accounts over the counter using their Card at a bank nominated by the utility, the amount will be debited to your Card account as a cash advance (not a purchase) and will immediately be subject to interest charges.

(Utility accounts can also be paid by way of BPAY payment – see Clause 3.14).

2.5 Deposits

You can deposit funds to the Card account with some of our agents and at any of our ATMs with deposit capability. There are limits on the amount of cash you can deposit at our agents. If a cheque is deposited the proceeds of the cheque will not be available until the cheque is cleared.

All deposits made at our ATMs are checked by us. If the amount appearing on the transaction record differs from the amount actually received by us, we will credit your Card account with the amount actually received and notify you as soon as possible. You must not include coins in payment envelopes at our ATMs.

We accept responsibility for the security of deposits received at our ATMs subject to checking of the amount deposited. The amount checked by us is evidence of the amount actually received.

2.6 Transactions at EFT terminals

When a User makes an EFT Transaction at an EFT Terminal you authorise us to act on the instructions given by the User. Users should ensure that the correct transaction details are entered into the terminal before authorising a transaction and also that the completed transaction is in accordance with those instructions. All vouchers and transaction records should be kept to help check statements.

EFT transactions may not be processed to your Card account on the day they are made. Processing may take a number of days. We will process transactions to your Card account as soon as practicable.

Users should observe the guidelines set out in Clause 6.2 to ensure the security of access methods when transacting at an EFT Terminal.

2.7 Do transactions have to be authorised by us?

Transactions on the Card account may need to be authorised by us. We may at our discretion decline a transaction and may do so for security reasons, or if you are in default, your credit limit would be exceeded, or we are unable to authorise the transaction because the system to do so is inoperative and the amount of the transaction exceeds limits we set in the circumstances.

If a User, or the Merchant, does not proceed with a transaction after it has been authorised by us your available credit limit may be reduced for at least three business days.

2.8 Use of Card at merchants, financial institutions or our agents

If a User provides a Merchant with their Card Details:

- (a) to enable the Merchant to complete a transaction in the future (e.g. authorises a hotel for room service or use of the mini-bar); or
- (b) to pay for goods and services in advance even if the User later decides not to take the goods or use the services; the User authorises the Merchant to complete the transaction and when the Merchant completes the transaction the available credit limit will be reduced.

To the extent permitted by law and the EFT Code, we do not accept responsibility for the actions of financial institutions, merchants or our agents:

- (a) in refusing to accept or honour a Card; or
- (b) in imposing limits or conditions on use of a Card.

The User must resolve such issues directly with the financial institution, Merchant or agent.

Card promotional material displayed on any Merchant's premises does not mean that the goods and services on those premises may be purchased using a Card.

Unless required by law we are not responsible for goods or services supplied to a User or for any refund. The User must take up any complaints or concerns directly with the Merchant and any refund is a matter between the User and the Merchant. However, please refer to Clause 7.1 where a 'chargeback' right may be available under the Credit Card scheme rules.

If a Merchant gives the User a refund we can only credit the Card account when we receive correctly completed refund instructions from the Merchant. Refunds credited

to the account will not be treated as monthly payments to the account but will reduce the amount of the most recent outstanding purchases appearing on the next statement following the refund.

Care! If a refund is obtained from an overseas Merchant, there may be a difference in the Australian dollar values due to movements in the foreign exchange rates. You take the risk of currency fluctuations between the date of purchase and the date of refund.

Care! You should obtain proof of refund and should check that the refund appears on your Card account statement.

The hours that a Merchant, financial institution or our agents may be open for business will determine when a terminal at their premises will be available.

Part 3 – Phone Banking and Bankwest Online Banking Conditions Of Use

3.1 About this Part

This Part (together with Parts 1, 6, 7 and 8) applies to use of Phone Banking and Bankwest Online Banking in connection with your Card account.

3.2 What is Phone Banking?

Phone Banking is a Service which enables a User to make enquiries and effect transactions on your Card account using a PAN and Secure Code and tone telephone or mobile phone.

Users must not use an analogue mobile phone as the tone message may be scanned and the PAN and Secure Code may be disclosed.

3.3 What can be done using Phone Banking?

Users can:

- obtain the balance of your Card account;
- transfer funds between accounts;
- enquire about transactions on your Card account;
- make payments to your Card account;
- make bill payments and receive or access bills electronically through the B_{PAY} Scheme;
- postdate funds transfer and bill payments up to 90 days in advance;
- order a statement of interest for taxation purposes; and
- change a Secure Code.

3.4 How to use Phone Banking

To use Phone Banking users must:

- phone us for the cost of a local call Australia wide. Calls from mobile phones and calls made from overseas are charged at the applicable rate;
- enter their PAN and Secure Code using the telephone keypad; and
- follow the instructions given.

3.5 What is Bankwest Online Banking?

Bankwest Online Banking is a Service provided by us which enables a User to make enquiries and effect transactions over the Internet on your Card account using a PAN and Secure Code. Bankwest Online Banking must only be accessed via an Approved Browser.

3.6 What can be done using Bankwest Online Banking?

Users can:

- obtain the balance of your Card account;
- transfer funds between accounts;
- enquire about transactions on your Card account;
- check past statements on your Card account;
- order a printed statement on your Card account;
- make payments to your Card account;
- make bill payments and receive or access bills electronically through the BPAY Scheme;
- postdate funds transfer and bill payments;
- order a statement of interest for taxation purposes;
- change a Secure Code;
- lodge various service and application forms with us; and
- make a Pay AnyBody transfer (see Part 4).

3.7 How to use Bankwest Online Banking

To use Bankwest Online Banking users must have a PAN and Secure Code.

The PAN will be provided separately from any Secure Code or Security Token we provide, and upon receipt, users should visit our website (bankwest.com.au) to get further information and to log on to Bankwest Online Banking.

Users without a Security Token logging onto Bankwest Online Banking for the first time will be required to change their issued Secure Code to an alphanumeric code of 6 – 10 characters with at least one letter and one number. Users with a Security Token logging on for the first time will be required to choose a Token PIN.

3.8 Internet security and privacy

Users of Bankwest Online Banking must ensure that they take all reasonable steps to protect the security of their

Electronic Equipment, any Security Token issued to them and their Secure Code. This includes, but is not limited to:

- ensuring that, if and when the Secure Code is changed, the number and letters which are chosen cannot be easily identified, e.g. it has no obvious pattern (patterns such as 1234A, 1111A, and ABCDEF are too obvious) and has no connection with the User (such as a birthday, telephone number, car registration, postcode or the PIN used with a Card);
- ensuring their computer is free of viruses;
- ensuring their computer is not left unattended while they are logged on to Bankwest Online Banking;
- ensuring their computer is free from any form of password recording program or mechanism;
- ensuring that they shut down all browser windows used to gain access to Bankwest Online Banking and that the 'back' function or similar function cannot be used to trace their activities.

The security guidelines in this subclause provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised transactions. Liability for unauthorised transactions will be determined in accordance with Part 6 of these Credit Card Account Access Conditions of Use and the EFT Code.

3.9 Access and restriction of access to Services

Access to Phone Banking and/or Bankwest Online Banking may not be available from some States, Territories or country telephone exchanges.

We will try (without any legal obligation) to provide the Services on a 24-hour continuous basis. However, circumstances may not always make this possible.

If the Services cannot be accessed at any time, to help us to investigate the reason please advise us by calling us.

We do not guarantee to give effect to any payment instruction received via our Services. We may delay and/or refuse to give effect to any Phone Banking or Bankwest Online Banking instruction without notifying you. Instructions will not be processed:

- when your Card contract prohibits the payment(s);
- when the credit limit of the Card account would be exceeded; or
- when a BPAY payment will cause you to exceed your daily BPAY payment limit.

You should ensure that any transaction instruction you give would not cause your credit limit to be exceeded.

Except for BPAY and Pay AnyBody transactions, transactions made prior to 6.00pm WST on a business day should be processed that day and otherwise should be processed on the next business day. However, payments to credit card accounts will not be available until the day after the next business day.

3.10 Future payments

If a funds transfer, BPAY payment or Pay AnyBody transfer is scheduled for a future stipulated date, it will only be effected on that date by us if the payment will not cause your credit limit to be exceeded by 11.30pm WST on the business day prior to the scheduled payment date and the funds transfer, BPAY payment or Pay AnyBody transfer will not cause you to exceed any limit we impose in accordance with Clause 3.11, your daily BPAY payment limit or your daily Pay AnyBody transfer limit on the date stipulated for the payment to be made.

3.11 Limits

At our discretion we may impose and/or vary minimum and/or maximum limits on the amounts which you may transfer from your Card account using our Services. We will notify you of these limits if and when they apply.

3.12 Other matters

We shall issue a receipt number for each funds transfer or BPAY payment instruction received via our Services. When we have instructions for more than one transfer or BPAY payment from the Card account we may determine the order.

3.13 Authorised users

Each Additional Cardholder will have automatic access to our Services with their own PAN and Secure Code.

3.14 BPAY Payments

- (a) If there is any inconsistency between the provisions of this Clause 3.14 and the Credit Card Account Access Conditions of Use, Clause 3.14 prevails to the extent of that inconsistency.
- (b) When you tell us to make a BPAY payment, you must give us the information specified in paragraph (f) below. We will then debit your Card account with the amount of that BPAY payment.
- (c) All bill payments that are made through our Services are processed through the BPAY Scheme. Bills which may be paid through the scheme display the BPAY logo and biller reference details. The bill will also record the type of accounts the biller will accept payment from (e.g. cheque, savings, or credit card).

- (d) Phone Banking users may nominate a maximum of 12 B_{PAY} billers per PAN on their frequent billers list. Bankwest Online Banking users may nominate a maximum of 500 B_{PAY} billers on their frequent billers list, with the first 12 B_{PAY} billers stored in the frequent billers list also available in Phone Banking. Users will be able to pay other B_{PAY} billers by manually keying in their full details.
- (e) The maximum aggregate amount of B_{PAY} payments you may instruct us to make on any business day is \$5,000.00. This aggregate amount will be your daily B_{PAY} payment limit.
- (f) The following information must be given to us to make a B_{PAY} payment:
- (i) the biller code;
 - (ii) the biller customer reference number;
 - (iii) the amount to pay;
 - (iv) a date if the payment is to be postdated; and
 - (v) the account to be debited for the payment.
- (g) We shall not be obliged to effect a B_{PAY} payment instruction if the information is incomplete and/or inaccurate, the payment would cause the credit limit of the Card account or the daily B_{PAY} payment limit to be exceeded.
- (h) If there is any inconsistency between this Clause 3.14 and any other part of these Credit Card Account Access Conditions of Use, this clause prevails to the extent of that inconsistency.
- (i) A B_{PAY} payment from the Card account is treated as a purchase transaction.
- (j) Except for postdated payments (Clause 3.14 (o)) we will not accept an order to stop a B_{PAY} payment once we have been instructed to make the B_{PAY} payment.
- (k) Generally, a B_{PAY} payment will be treated as received by the biller to whom it is directed:
- on the date we are told to make that B_{PAY} payment, if we receive the instruction before 4.00pm WST on a business day; or
 - on the next business day, if we receive the instruction after 4.00pm WST on a business day, or on a nonbusiness day.
- (l) A delay may occur in processing a B_{PAY} payment where a biller, or another financial institution participating in the B_{PAY} Scheme, does not comply with its obligations under the B_{PAY} Scheme.

- (m) Care must be taken by all users to enter the correct amount to be paid to a biller and to enter the correct biller details. If the amount entered is greater than was intended, you must contact the biller to obtain a refund of the excess. If less, a further BPAY payment can be made. If the payment is made to a person other than the biller intended to be paid and we cannot recover it from the recipient within 20 business days, you are liable for the amount.
- (n) If we are advised that a BPAY payment cannot be processed by a biller, we will advise you, credit your Card account with the amount of the BPAY payment, and take all reasonable steps to assist in making the BPAY payment as quickly as possible.
- (o) Postdated BPAY payments:
 - (i) a BPAY payment may be requested for a date in the future, however, we will only make the BPAY payment if the requirements of Clause 3.10 are met. If the date stipulated is not a business day, we will make the BPAY payment on the next business day. In the event that your credit limit, your daily BPAY payment limit or any other limit we impose in accordance with Clause 3.11 is exceeded, it will be necessary to resubmit the BPAY payment instruction.
 - (ii) a future-dated BPAY payment instruction may be altered or cancelled before its stipulated date for payment, provided the instruction to alter or cancel the payment is given before the payment cut-off time the business day immediately prior to the stipulated date.
- (p) We may charge a fee to correct errors on your Card account due to incorrect BPAY instructions.
- (q) You acknowledge that the receipt by a biller of a mistaken or erroneous payment does not or will not constitute under any circumstances part or whole satisfaction of any underlying debt owed between you and that biller.
- (r) You should check your Card account carefully and promptly report to us, as soon as you become aware of them, any BPAY payments that you think are errors or are BPAY payments that you did not authorise. (Note: The longer the delay between the date of your BPAY payment and when you tell us of the error, the more difficult it may be to correct the error. For example, we or your biller may not have sufficient records or information available to us to investigate the error. If this is the case you may need to demonstrate that an error has occurred, based on your own records, or liaise directly with the biller to correct the error).

- (s) Your liability for unauthorised and fraudulent B_{PAY} payments will be determined in accordance with Part 7 of these Credit Card Account Access Conditions of Use.
- (t) Disputes in relation to unauthorised, fraudulent or wrong B_{PAY} payments will be handled in accordance with Part 8 of these Credit Card Account Access Conditions of Use, however, no chargeback rights are available in respect of a B_{PAY} payment from your Card account.
- (u) **If we make the wrong payment**
If a B_{PAY} payment is made to a person or for an amount which is not in accordance with the instructions given to us and your Card account was debited with the payment, we will credit that payment amount to your account.
- (v) **Biller consent**
If you tell us that a B_{PAY} payment made from your Card account is unauthorised, you must give us your written consent addressed to the biller who received that B_{PAY} payment, consenting to us obtaining from the biller information about your account with that biller or the B_{PAY} payment, including your customer reference number and such information as we reasonably require to investigate the B_{PAY} payment. If you do not give us that consent, the biller may not be permitted under law to disclose to us the information we need to investigate or rectify that B_{PAY} payment.
- (w) **Consequential damage and indemnity**
Subject to Part 7 of these Credit Card Account Access Conditions of Use and the EFT Code:
- (i) we are not liable for any consequential loss or damage you may suffer as a result of using the B_{PAY} Scheme, other than due to any loss or damage you suffer due to our negligence, or in relation to any breach of a condition or warranty implied by law under consumer protection legislation in contracts for the supply of goods and services and which may not be excluded, restricted or modified at all or only to a limited extent; and
 - (ii) you indemnify us against any loss or damage we may suffer due to any claim, demand or action of any kind brought against us arising directly or indirectly because you:
 - did not observe any of your obligations under; or
 - acted negligently or fraudulently in connection with, this Clause 3.14.

3.15 BPAY View

- (a) You may use BPAY View to receive or access bills electronically from participating billers nominated by you. You can access a bill by accessing Bankwest Online Banking.
- (b) You need to register in order to use BPAY View. Call us on **13 17 18** to find out how to register, or register online via Bankwest Online Banking.
- (c) If you register with BPAY View, you:
 - (i) agree to our disclosing to billers nominated by you:
 - such of your personal information (for example your name, email address and the fact that you are our customer) as is necessary to enable billers to verify that you can receive bills and statements electronically using BPAY View (or telling them if you cease to do so); and
 - that an event in paragraph (d) (ii), (iii), (iv), (v) or (vi) has occurred;
 - (ii) agree to us or a Biller (as appropriate) collecting data about whether you access your emails, the Bankwest Online Banking website and any link to a bill or statement;
 - (iii) agree to receive bills and statements electronically and agree that this satisfies the legal obligations (if any) of a Biller to give you bills and statements. For the purposes of this clause we are the agent for each Biller nominated by you under (i) above.
- (d) You may receive paper bills and statements from a Biller instead of electronic bills and statements:
 - (i) at your request to a Biller (a fee may be charged by the applicable Biller for supplying the paper bill or statement to you if you ask for this in addition to an electronic form);
 - (ii) if you or a Biller de-register from BPAY View;
 - (iii) if we receive notification that your email mailbox is full, so that you cannot receive any email notification of a bill or statement;
 - (iv) if your email address is incorrect or cannot be found and your email is returned to us undelivered;
 - (v) if we are aware that you are unable to access your email or Bankwest Online Banking or a link to a bill or statement for any reason; or
 - (vi) if any function necessary to facilitate BPAY View malfunctions or is not available for any reason for longer than the period specified by the applicable Biller.

- (e) You agree that when using BPAY View:
- (i) if you receive an email notifying you that you have a bill or statement, then that bill or statement is received by you:
 - when we receive confirmation that your server has received the email notification, whether or not you choose to access your email; and
 - at the email address nominated by you;
 - (ii) if you receive notification via Bankwest Online Banking without an email then that bill or statement is received by you:
 - when a notification is posted on Bankwest Online Banking, whether or not you choose to access Bankwest Online Banking; and
 - via Bankwest Online Banking;
 - (iii) bills and statements delivered to you remain accessible through Bankwest Online Banking for the period determined by the Biller up to a maximum of 18 months, after which they will be deleted, whether paid or not;
 - (iv) you will contact the Biller directly if you have any queries in relation to bills or statements.
- (f) You must:
- (i) check your emails or log onto Bankwest Online Banking at least weekly;
 - (ii) tell us if your contact details (including email address) change;
 - (iii) tell us if you are unable to access your email or log onto Bankwest Online Banking or a link to a bill or statement for any reason; and
 - (iv) ensure your mailbox can receive email notifications (e.g. it has sufficient storage space available).
- (g) BPAY View billing errors:
- (i) for the purposes of this paragraph (g) a BPAY View billing error means any of the following:
If you have successfully registered with BPAY View:
 - failure to give you a bill (other than because you failed to view an available bill);
 - failure to give you a bill on time (other than because you failed to view an available bill on time);
 - giving a bill to the wrong person;
 - giving a bill with incorrect details;
If your BPAY View deregistration has failed for any reason:
 - giving you a bill if you have unsuccessfully attempted to deregister from BPAY View.

- (ii) you agree that if a billing error occurs:
- you must immediately upon becoming aware of the billing error take all reasonable steps to minimise any loss or damage caused by the billing error, including contacting the applicable Biller and obtaining a correct copy of the bill; and
 - the party who caused the error is responsible for correcting it and paying any charges or interest which would ordinarily be payable to the applicable Biller due to any consequential late payment and as a result of the billing error.
- (iii) you agree that for the purposes of this paragraph (g) you are responsible for a billing error if the billing error occurs as a result of an act or omission by you or the malfunction, failure or incompatibility of computer equipment you are using at any time to participate in BPAY View.

Part 4 – Pay AnyBody Conditions of Use

4.1 About this Part

This Part (together with Parts 1, 6, 7 and 8) applies to all transactions involving the use of the Pay AnyBody Service (Pay AnyBody). Pay AnyBody is an extension of Bankwest Online Banking (see Part 3). If there is any inconsistency between this Part and Part 3, this Part prevails to the extent of that inconsistency.

4.2 What is Pay AnyBody?

Pay AnyBody is a Service which allows a User to transfer funds from an account with us to:

- another account (except a credit card account) held by you with another financial institution; or
- another person's account (except a credit card account) held with us or with another financial institution.

4.3 Daily Pay AnyBody transfer limit

The maximum aggregate amount of Pay AnyBody transfers you may instruct us to make on any business day is your daily Pay AnyBody transfer limit. You may choose a limit of either \$1,500.00 or \$5,000.00.

You may at any time alter your choice of limit. To decrease the limit, submit a 'Quick Form' via Bankwest Online Banking. To increase the limit, print off an 'Internet Security Declaration' from the Bankwest website, and when completed fax or post it to the Internet Banking Customer Support Team or deliver it to one of our Customer Service Centres.

4.4 Making a Pay AnyBody transfer

- (a) To make a Pay AnyBody transfer you must enter the BSB number, account number and account name in respect of the account to which the funds are to be transferred, together with a description of the transaction. We shall not be obliged to effect a Pay AnyBody transfer if the information is incomplete and/or inaccurate, there is a technical failure which prevents us from processing the transfer, the transfer would cause the credit limit of the Card account or your daily Pay AnyBody transfer limit to be exceeded.
- (b) A Pay AnyBody transfer from the Card account is treated as a cash advance.

4.5 Postdated Pay AnyBody transfers

- (a) A Pay AnyBody transfer may be requested for a date in the future, however, we will only make the transfer if the requirements of Clause 3.10 are met. If the date stipulated is not a business day, we will make the transfer on the next business day.
- (b) A future-dated Pay AnyBody transfer may be altered or cancelled before its stipulated date, provided the instruction to alter or cancel the transfer is given before 11.30pm WST on the business day immediately prior to the stipulated date.

4.6 Cancelling a Pay AnyBody transfer

We are not obliged to cancel a Pay AnyBody transfer once we have accepted the instruction to make it. It may be possible in some cases to cancel an initiated Pay AnyBody transfer. A fee is payable for any such cancellation.

4.7 Mistakes as to the amount of a Pay AnyBody transfer

Care must be taken by all users to enter the correct amount to be transferred. If the amount entered is greater than was intended you should seek a refund from the recipient. If less, a further transfer can be made.

4.8 Processing Pay AnyBody transfers

- (a) Generally, a Pay AnyBody transfer will be treated as received:
 - on the date we are told to make that Pay AnyBody transfer, if we receive the instruction before 3.00pm WST on a business day; or
 - on the next business day, if we receive the instructions after 3.00pm WST on a business day, or on a non-business day.

Delays may arise because of conduct of the recipient financial institution for which we will not be responsible.

- (b) If we are advised that a Pay AnyBody transfer cannot be processed by another financial institution, we will advise you, credit your Card account with the amount of the Pay AnyBody transfer, and take all reasonable steps to assist in making the Pay AnyBody transfer as quickly as possible.

4.9 If we make the wrong payment

If a Pay AnyBody transfer is made to a person or for an amount which is not in accordance with the instructions given to us, and your Card account was debited with the payment, we will credit that payment amount to your account.

Part 5 – Regular Payments

5.1 About this Part

This section provides you with information about Regular Payment Arrangements.

5.2 Maintain a record of any Regular Payment Arrangements

Cardholders are encouraged to maintain a record of any Regular Payment Arrangement they elect to enter into with a Merchant.

5.3 Changing Regular Payment Arrangements

To either change or cancel a Regular Payment Arrangement you should contact the Merchant at least 15 days prior to the next scheduled payment and if possible you should retain a copy of the change/cancellation request made to the Merchant. Until you attempt to cancel the Regular Payment Arrangement we must accept any instructions received from the Merchant.

Should your Card number change, you must request the Merchant change the details of the existing Regular Payment Arrangement to ensure it continues. If you fail to make this request your Regular Payment Arrangement either may not be honoured by us, or the Merchant may stop providing the goods and/or services.

Should you elect to close your Card account or we close your Card account you should contact the Merchant to revise your Regular Payment Arrangement as the Merchant may stop providing the goods and/or services.

Part 6 – Security of Access Methods

6.1 What do users need to do to safeguard their Access Methods?

Users must protect relevant Access Methods to prevent unauthorised access to their Card account. Users must take care to ensure that access methods are not misused, lost or stolen and that secret codes do not become known to anyone else.

6.2 Guidelines

This clause contains guidelines which should be followed by users to guard against unauthorised use of an Access Method. These guidelines provide examples only of security measures and will not determine your liability for losses resulting from any unauthorised transactions. Liability for unauthorised transactions will be determined in accordance with Part 7 of these Credit Card Account Access Conditions of Use and the EFT Code.

To protect the Card:

- sign the Card as soon as it is received;
- carry the Card whenever possible;
- always keep the Card in a safe, secure place and check regularly to ensure it has not been lost or stolen;
- never lend the Card to anybody or permit any other person to use the Card or Card Details; and
- when the transaction is complete remember to take the Card and the transaction receipt.

To protect the Card Details:

- do not give or tell the Card Details to anyone; and
- use care to prevent anyone seeing the Card Details when entering them at Electronic Equipment.

To protect the Secret Code:

- where the Secret Code is issued by us, memorise the Secret Code when it is received. Once memorised, destroy our notice of the Secret Code. If a User forgets the Secret Code they may apply to us for it to be reissued;
- if given the option to select a Secret Code, users should not select a Secret Code which represents a name, date, telephone number, car registration or anything else that could be associated with them, or select a Secret Code which has an easily retrievable combination (such as repeated numbers or letters);
- never tell or show a Secret Code to anyone, including a family member, friend or persons in authority (such as a bank officer or police officer);
- do not record a Secret Code on the Card and/or Security Token;

- do not record the Secret Code on anything which is kept with or near the Card or Security Token without making a reasonable attempt to disguise the Secret Code;
- do not keep a record of the Secret Code (without making any reasonable attempt to disguise the Secret Code) with any article kept with the Card or Security Token which is liable to be lost or stolen simultaneously with the Card;
- do not record the Secret Code on a computer or telephone or related articles without making a reasonable attempt to disguise the Secret Code or prevent unauthorised access to the records;
- do not keep the Card or Security Token and a Secret Code together, for example in a bag or wallet, in a car or in the same piece furniture;
- do not keep a record of the Secret Code with any document containing the reference numbers for the Card account such as statements; and
- if a User suspects that someone else may know a Secret Code or that an unauthorised person is using a Secret Code, they should contact us immediately to request the issue of a new Secret Code.

We do not consider the following to be reasonable attempts to disguise a Secret Code:

- recording the disguised Secret Code on their Card;
- disguising the Secret Code by reversing the number sequence;
- describing the disguised record as a secret code record;
- disguising the Secret Code as a telephone number where no other numbers are recorded;
- disguising the Secret Code as a telephone number, postcode, amount or date with the Secret Code in its correct sequence within the number;
- disguising the Secret Code using alphabetical characters, i.e. A=1, B=2, C=3 etc. or in any other easily understood code; or
- recording the Secret Code as a series of numbers or letters with any of them marked to indicate the Secret Code.

Users must not use any other forms of disguise which are similarly unsuitable because another person can easily work out the Secret Code.

At Electronic Equipment:

- be careful to prevent anyone else from seeing the Secret Code being entered;
- watch out for mirrors, security cameras or any means which enable other people to see the Secret Code being entered;
- when the transaction is complete remember to take the Card, transaction receipt and any cash; and
- do not access Phone Banking or Bankwest Online Banking directly from a facility where the details entered may be recorded by a third party, e.g. a hotel telephone or a computer at an internet cafe.

To protect the Security Token:

- carry the Security Token whenever possible;
- always keep the Security Token in a safe, secure place and check regularly to ensure it has not been lost or stolen;
- do not record account numbers, your PAN, or Secret Code details on the Security Token;
- do not drop the Security Token or expose it to high heat, water or attempt to disassemble it;
- do not keep the Security Token with any document containing the reference numbers for nominated accounts or with other account information such as statements or cheque books;
- do not lend the Security Token to anyone, or permit anyone to use the Security Token.

Part 7 – Loss, Theft or Unauthorised Use of Your Access Method

7.1 What users have to do

If any Card or Security Token has been lost, stolen or used without authorisation, or a Secret Code has become known to someone else, you or any additional cardholder must immediately tell us or, in the case of a Card, tell any bank displaying the Visa or MasterCard symbol, in writing or by calling us.

We will require all information about how the loss, theft or unauthorised use occurred.

We will issue a notification number which should be kept as evidence of the date and time of the notification.

If for any reason the emergency telephone facility is unavailable and this prevents the User from calling us you will not be liable for any unauthorised transactions which could have been prevented during this period if the User had been able to telephone us. However, the User must notify us within a reasonable time of the emergency facility becoming available again.

7.2 What is your liability for unauthorised EFT transactions?

The following relates to liability for EFT transactions which are carried out without the knowledge and consent of a User. You are liable for all EFT transactions carried out in respect of your Card account with the knowledge and consent of a User.

7.2.1 When you are not liable

You will not be liable for any unauthorised EFT transactions that occur:

- before the User has received their Card, Security Token or Secret Code (as relevant);
- after we receive notification that a Card or Security Token (as relevant) has been lost/stolen, used without authority, or the Secret Code has become known to someone else;
- relating to any component of an Access Method that is forged, faulty, expired or cancelled;
- by the fraudulent or negligent conduct of our employees or agents, or the employees or agents of merchants or of companies or persons involved in the EFT system;
- where it is clear that the User has not contributed to the loss; or
- due to the same transaction being incorrectly debited more than once to the Card account.

7.2.2 When you are liable

Where we prove on the balance of probabilities that the User has contributed to losses in respect of a Card account resulting from an unauthorised EFT Transaction by:

- the User's fraud;
- (in all cases except where the unauthorised EFT Transaction was made using Bankwest Online Banking and the User has been issued with a Security Token) voluntarily disclosing the Secret Code to anyone, including a family member or friend;
- (where the unauthorised EFT Transaction was made using Bankwest Online Banking and the User has been issued with a Security Token) voluntarily disclosing the Token PIN **and** showing the Security Token or otherwise disclosing the Token Code to anyone, including a family member or friend;
- (where the unauthorised EFT Transaction was made using Bankwest Online Banking and the User has been issued with a Security Token), **either**:
 - (i) voluntarily disclosing the Token PIN, **or**
 - (ii) showing the Security Token (or otherwise disclosing the Token Code), to anyone, including a family member or friend, where this disclosure is more than 50% responsible for the losses when all contributing causes are assessed together;
- (in all cases except where the unauthorised EFT Transaction was made using Bankwest Online Banking and the User has been issued with a Security Token), indicating a Secret Code on the Card, or keeping a record of a Secret Code (without making any reasonable attempt to protect the security of the record) on the one article, or on several articles, carried with the Card or liable to loss or theft simultaneously with the Card;
- (where the unauthorised EFT Transaction was made using Bankwest Online Banking and the User has been issued with a Security Token) indicating the Token PIN on the Security Token, or keeping a record of the Token PIN (without making any reasonable attempt to protect the security of the code record) on the one article, or on several articles, carried with the Security Token or liable to loss or theft simultaneously with the Security Token;
- where the Access Method comprises a Secret Code without a Card or Security Token, keeping a record of a Secret Code (without making any reasonable attempt to protect the security of the code records) on the one article, or on several articles that are liable to loss or theft simultaneously;

- when changing a Secret Code, selecting a Secret Code which represents the User's birth date or a recognisable part of the User's name; or
- acting with extreme carelessness in failing to protect the security of the Secret Code;

you will be liable for the losses which occur before we are notified of the unauthorised use, loss or theft of the Card or Security Token, or breach of the security of the Secret Code; or by:

- unreasonably delaying notifying us of the unauthorised use, theft or loss of the Card or Security Token, or that the Secret Code has become known to someone else;

you will be liable for the losses which occur between when the User became aware of the loss, theft or unauthorised use (or should reasonably have become aware in the case of a lost or stolen Card or Security Token) and when we were actually notified.

However, in all cases you will not be liable for:

- (a) that portion of the loss incurred on any one day which exceeds any applicable daily transaction limits;
- (b) that portion of the loss incurred in a period which exceeds any other periodic transaction limit applicable to that period;
- (c) losses incurred on any accounts which you had not agreed with us could be accessed using the Access Method;
- (d) losses that would exceed the amount of your liability had we exercised our rights (if any) under the Credit Card scheme rules against other parties to that scheme; or
- (e) that portion of the loss which exceeds the credit limit of the Card account.

7.2.3 When your liability is limited

Where a Secret Code was required to perform the unauthorised EFT Transaction and Clause 7.2.2 does not apply, your liability for any loss in respect of the Card account arising from an unauthorised EFT Transaction, if the loss occurs before you notify us of the unauthorised use, loss or theft of the Card or Security Token or the Secret Code becoming known to someone else, is lesser of:

- \$150;
- the actual loss at the time we are notified of the unauthorised use, loss or theft of the Card or Security Token or of the Secret Code becoming known to someone else (except that portion of the loss that exceeds any daily or periodic transaction limits applicable to the use of your Access Method or Card account);

- the credit limit of the Card account; or
- the amount of your liability had we exercised our rights (if any) under the Credit Card scheme rules against other parties to the scheme.

7.2.4 Notwithstanding any of the provisions contained in this clause, your liability will not exceed your liability under the EFT Code.

7.3 What is your liability for other unauthorised transactions?

If, in cases not involving EFT transactions, a Card is used without a User's authority, you are liable for the actual loss arising from the transaction at the time we are notified of the unauthorised use (except that portion of the loss incurred on any one day that exceeds any applicable daily transaction or other periodic transaction limit) less any amount recovered by us in the exercise of our rights (if any) under the Credit Card scheme rules against other parties to that scheme.

7.4 When the electronic banking system or EFT Terminal malfunctions or breaks down

In the event that an EFT Terminal malfunctions or breaks down, manual procedures may be available from the Merchant for retail transactions by using the Card and a signature authorisation procedure.

You will not be responsible for any loss you suffer because our system or our equipment accepted a User's instructions but failed to complete the transaction.

If the users were or should have been aware that the EFT system or equipment was unavailable for use or malfunctioning then our liability is limited to correcting any errors in your Card account and the refund of any charges or fees imposed on you as a result.

Please advise us if an EFT Terminal has a service fault or difficulty. Users can do this through our Customer Service Centres during normal banking hours or by telephoning us.

Part 8 – Procedures For Handling Errors and Disputed Transactions

8.1 How will any errors, mistakes and disputes be handled?

If you believe an entry on your Card account statement is wrong or unauthorised you must tell us immediately by:

- telephoning us;
- logging on to our website (bankwest.com.au) and following the procedures it sets out for disputing a transaction;
- calling into any of our Customer Service Centres; or
- writing to us at the address shown on your Card account statement containing the suspected error.

You must complete a Bankwest Transaction Dispute Form and you should do so promptly. This form can be obtained from any Customer Service Centre, our website or by calling us.

To assist in the dispute resolution process, you will need to provide the following information:

- your name, address, credit card number and account details;
- details and amount of the transaction, charge, refund or payment in question; and
- supporting documentation (examples being: credit card receipt, delivery advice).

We will notify you of the name and contact number of the officer investigating your dispute. We will contact you if we require further information, and you must supply this information within 10 business days.

We have the right under the Credit Card scheme rules to seek the reversal of a credit card transaction, involving a 'chargeback' or debiting of the credit card transaction to the Merchant's account with its financial institution. We may do so on certain grounds, for instance if you claim that an unauthorised mail or telephone transaction, in which you or any Additional Cardholder did not participate, has been debited to your Card account.

We will claim a chargeback right where one exists under the Credit Card scheme rules. Please note, however, that no chargeback right will exist in relation to B_{PAY} payments from your Card account (see Clause 3.14 (t)). We will use our best efforts to chargeback a disputed transaction for the most appropriate reason. This does not mean that the disputed transaction will necessarily be charged back.

The Merchant's financial institution must first accept the claim in order for your claim to be successful. If the Merchant's financial institution rejects a chargeback, we will not accept that rejection unless we are satisfied that the rejection is reasonable and is consistent with the Credit Card scheme rules.

You should make every effort to report a disputed transaction by completing the Bankwest Transaction Dispute Form within 14 days of the date of the account statement which itemises the disputed transaction, so that we may reasonably ask for a chargeback where such right exists.

Failure to report a disputed transaction, charge, refund or payment, and/or provide additional information within this timeframe could affect our ability to claim a chargeback right (if any) under the Credit Card scheme rules. These rules all impose time limits on reporting disputed transactions, charges, refunds or payments.

In certain circumstances where the EFT Code applies, there may be no such timeframes imposed upon your right to make a claim or report a disputed transaction.

8.1.1 If we are unable to resolve the matter immediately to both your and our satisfaction we will advise you in writing of our procedures for further investigation and handling of your complaint.

8.1.2 Within 21 days of receiving your complaint, we will advise you in writing of either:

- the outcome of our investigation; or
- the fact that we need more time to complete our
- investigation.

We will complete our investigation within 45 days of receipt of your complaint unless there are exceptional circumstances.

8.1.3 Subject to Clause 8.1.4, if we are unable to resolve your complaint within 45 days we will write to you and let you know the reasons for the delay and provide you with monthly updates on the progress of our investigation and its likely resolution date, except where we are waiting for a response from you and you have been advised that we require such a response.

8.1.4 If we resolve your complaint by exercising our rights under the Credit Card scheme rules we will:

- apply the time limits under those rules to Clause 8.1.2;
- comply with Clause 8.1.3 as if the reference to '45 days' read '60 days' and the reference to 'monthly updates' read 'updates every two months';
- inform you when you can reasonably expect a decision; and
- suspend your obligation to pay any amount which is the subject of your complaint or any credit or other charges related to that amount until your complaint has been resolved.

8.2 Outcome

On completion of our investigation, we will advise you in writing of the outcome of our investigation and the reasons for our decision, with reference to the relevant provisions of these Credit Card Account Access Conditions of Use and the EFT Code. If we decide that your Card account has been incorrectly charged or credited, we will adjust your account (including any interest and charges) and notify you in writing of the amount of the adjustment. If we decide that you are liable for all or any part of the disputed transaction, we will supply you with copies of any document or other evidence on which we base our findings if these show that your Card account has not been incorrectly charged or credited. We will also advise you if there was any system or equipment malfunction at the time of the transaction. We will advise you in writing that, if you are not satisfied with our findings, you may request a review.

8.3 If you are not satisfied

If you are not satisfied with our findings, you may request our Service Quality Department to review the matter.

Contact them by writing to:

Manager Service Quality
GPO Box E237
Perth WA 6841

or phone or fax to:

Telephone: Freecall 1800 650 111

Fax: (08) 1300 259 233.

When we advise you of our decision we will also advise you of further action you may take in respect of your complaint if you are not satisfied with our decision. For instance, you may be able to refer the matter (free of charge) to:

Financial Ombudsman Service
GPO Box 3
Melbourne VIC 3001

or phone or fax to:

Telephone: 1300 780 808

Fax: (03) 9613 6399

Website: www.fos.org.au.

You may also be able to refer your complaint to consumer affairs departments or small claims tribunals.

8.4 If we fail to comply with these procedures

If we fail to observe the procedures set out in this clause or the EFT Code for handling disputes, allocating liability or communicating the reasons for our decision and that failure contributes to our decision or delays the resolution of your complaint, we may be liable for part or all of the amount of the disputed transaction.

bankwest



bankwest.com.au
13 17 18

Bank of Western Australia Ltd ABN 22 050 494 454 AFSL 236872.
Issued 1 July 2010

8105 010710