Account & Access Facility Conditions Of Use

How to contact us

- In person: Visit us at any branch, see our website for branch details;
- Telephone: 13 61 91;
- Email: info@australianmutual.bank;
- Postal Address: PO Box 881 Haymarket NSW 1240;
- Website: www.australianmutual.bank.

To report the loss, theft or unauthorised use of your Visa Card

- **In Australia**

  Call the Visa card Hotline on 1800 648 027 – 24 hours a day, everyday. Please also contact us to report the loss, theft or unauthorised use;
- **Overseas**

  Call +61 2 8299 9101 (Vigil Helpline) or call the Visa International Hotline.

To report the loss of any other access facility, or any other unauthorised transaction, contact us as set out above in How to contact us.

Customer Owned Banking Code of Practice

We warrant that we will comply with the Customer Owned Banking Code of Practice. You can download a copy of the Customer Owned Banking Code of Practice at www.customerownedbanking.asn.au.

ePayments Code

We warrant that we will comply with the ePayments Code.

Privacy

We have a privacy policy that sets out:

- our obligations regarding the confidentiality of your personal information; and
- how we manage your personal information.

We will give you details on how to access our privacy policy whenever we request personal information from you and when you first join Australian Mutual Bank. It is always available on request and you can download it from our website at www.australianmutual.bank.

How our Conditions of Use become binding on you

Please note that by opening an account or using an access facility you become bound by these Conditions of Use.

Accessing copies of the Conditions of Use

Please keep these Conditions of Use in a safe place so you can refer to it when needed. Alternatively, you can view and download our current Conditions of Use from our website at www.australianmutual.bank.

Financial Claims Scheme

The Financial Claims Scheme (FCS) protects depositors through the provision of a guarantee on deposits (up to the cap) held in authorised deposit-taking institutions (ADIs) incorporated in Australia and allows quick access to their deposits if an ADI becomes insolvent.

The Bank is an ADI. Depositors with the Bank may be entitled to receive a payment from the FCS, subject to a limit per depositor. For further information about the FCS visit the website at: http://www.fcs.gov.au.

Table of contents

Account Operations

What is the Australian Mutual Bank Account and Access Facility?

The Australian Mutual Bank Account and Access Facility is a facility that gives you transaction, savings and term deposit accounts as well as these facilities for accessing accounts:

- Visa Card;
- BPAY® (registered to BPAY® Pty Ltd ABN 69 079 137 518);
- Osko Payments;
- PayTo;
- Internet and Mobile Banking;
- EFTPOS and ATM access;
- Direct Debit requests;
- Bank@Post.

Please refer to the *Summary of Accounts & Availability of Access Facilities* brochure for available account types, the conditions applying to each account type and the access methods attaching to each account type.

How do I open an account?

You will need to become a member of the Bank before we can issue the Australian Mutual Bank Account and Access Facility to you. To become a member, you will need to:

- complete an application form; and
- subscribe for a share in the Bank.

Proof of identity required

The law requires us to verify your identity when you open an account and the identity of any person you appoint as a signatory to your account.

In most cases you can prove your identity by showing us a government issued photo identity document, such as a driver licence or passport.

If you do not have photo ID, please contact us to discuss what other forms of identification may be acceptable. In some circumstances we may verify your identity electronically using information you provide.

What accounts can I open?

When we issue you with the Australian Mutual Bank Account and Access Facility, you have access to the Transaction Account. You can then activate other accounts as needed. Please first check the *Summary of Accounts & Availability of Access Facilities* brochure for the different account types available, any special conditions for opening, and the features and benefits of each account type.

Joint accounts

A joint account is an account held by two or more persons. The important legal consequences of holding a joint account are:

- the right of survivorship – when one joint holder dies, the surviving joint holders automatically take the deceased joint holder's interest in the account (for business accounts different rules may apply - see note below);
- joint and several liability – if the account is overdrawn, each joint holder is individually liable for the full-amount owing.

You can operate a joint account on a 'joint operation' or 'individual operation' basis:

- 'joint operation' means 2 or more joint holders must authorise any withdrawal, payment or transfer from the account;
- 'individual operation' means any one joint holder can authorise any withdrawal, payment or transfer from the account.

By default, new joint accounts will be opened on an individual operation basis unless the joint holders instruct otherwise in the account opening application. The joint holders can jointly change account operating instructions in writing at any time.

However, irrespective of the joint account operating instructions, any one joint holder can instruct us to:

- change the account operation to joint operation by all joint holders only; or
- suspend the account to allow the joint holders time to reach agreement about dispersal of the account funds.

In which case these instructions will remain in effect until all joint holders agree otherwise.

We may also change the account operation to joint operation by all joint holders only, if we become aware of a dispute between the joint holders, or of the bankruptcy of any joint holder.

Please note that some access facilities (such as access cards) may not be available if the joint account operates on a joint operation basis.

Irrespective of the joint account operating instructions, all joint account holders will need to provide instructions to:

- close the account;
- appoint a third-party signatory to the account.

The above applies to joint personal accounts. For joint business accounts, such as partnership accounts, we may accept and rely on different account operating instructions. Please contact us for information about joint business accounts.

Note: The right of survivorship does not automatically apply to joint business accounts, such as partnerships. A partner's interest in a business joint account would normally pass to beneficiaries nominated in the partner's will or next-of-kin if there is no will. If you are operating a business partnership joint account, you should obtain your own legal advice to ensure your wishes are carried out.

Trust accounts

You can open an account as a trust account. However:

- we are not taken to be aware of the terms of the trust;
- we do not have to verify that any transactions you carry out on the account are authorised by the trust.

What fees and charges are there?

Please refer to the *Fees & Charges and Transaction Limits* brochure for current fees and charges. We may vary fees or charges from time to time as set out under "*Notifying changes*" on page 7.

We will debit your primary operating account for all applicable government taxes and charges.

What interest can I earn on my account?

Our *Deposit Interest Rates Schedule* provides information about our current deposit and savings interest rates. Our website also has information about our current deposit and savings interest rates. We may vary deposit or savings interest rates from time to time on all deposit accounts except our term deposit accounts. Our *Summary of Accounts & Availability of Access Facilities* brochure discloses how we calculate and credit interest to your account.

What are the taxation consequences?

Interest earned on an account is income and may be subject to income tax.

Disclosing your Tax File Number (TFN)

When you apply for the Australian Mutual Bank Account and Access Facility we will ask you whether you want to disclose your Tax File Number or exemption. If you disclose it, we will note your TFN against any account you activate.

You do not have to disclose your TFN to us. If you do not, we will deduct withholding tax from interest paid on the account at the highest marginal rate.

For a joint account, each holder must quote their TFN and/or exemption, otherwise withholding tax applies to all interest earned on the joint account.

Businesses need only quote their ABN instead of a TFN.

Declaration of residency for tax purposes

To enable us to comply with Australian Tax Law, we are required to confirm all account holders tax residency. If you are a tax resident of another country, you will need to complete a *FATCA/ CRS self-certification* form and provide us with your Taxpayer Identification Number (TIN).

If there are any changes to your tax residency, please advise us immediately.

Third party access

You can authorise us at any time to allow another person (a signatory) to operate on your account. However, we will need to verify this person's identity before they can access your account.

You are responsible for all transactions your authorised person carries out on your account. You should ensure that the person you authorise to operate on your account is a person you trust fully.

For personal accounts, a signatory's authority is limited to:

- carrying out withdrawals, payments or transfers from the account;
- making enquiries about account balances and transactions on the account, including any debit balance or available credit on a transactional account.

For business accounts please contact us about applicable signatory options.

You may revoke the signatory's authority at any time by giving us written notice.

Making deposits to the account

You can make deposits to the account:

- by cash at selected branches (see website for details);
- by direct credit e.g. from your employer for wages or salary – please note that we can reverse a direct credit if we do not receive full value for the direct credit;
- by transfer from another account with us;
- by transfer from another financial institution;
- by cash or cheque drawn on Australian banks via Bank@ Post;
- by cheque drawn on overseas banks at selected branches (see website for details);

unless otherwise indicated in the *Summary of Accounts & Availability of Access Facilities* brochure.

Deposits using electronic equipment

We are responsible for a deposit into a facility received by our electronic equipment, from the time you complete the deposit, subject to verification of the amount or amounts deposited.

If there is a discrepancy between the amount recorded as being deposited by the electronic equipment and the amount recorded by us as being received, we will contact you as soon as practicable about the difference.

Note that electronic deposits may not be processed on the same day.

Depositing cheques drawn on Australian banks

Cheques drawn on Australian banks may only be deposited to your account via Bank@Post.

You can only access the proceeds of a cheque when it has cleared. Cheques deposited via Bank@Post usually clear in 7 business days.

Depositing cheques drawn on Overseas banks

Cheques drawn on an overseas institution have longer clearance periods and proceeds will not be available for drawing on your account until cleared.

Depositing cheques - general

All cheques for deposit can only be accepted if in the name of the account holder. We may accept a cheque into a joint account which is payable to any one or more of the joint account holders.

If a cheque deposited to your account is dishonoured by the paying bank, we may charge a fee. Please refer to our *Fees & Charges and Transaction Limits* brochure.

Withdrawing or transferring from the account

You can make or authorise withdrawals or transfers from the account:

- over the counter at selected branches (see website for details);
- by direct debit;
- internet or mobile banking (including by Osko payment where available);

- by BPAY® to make a payment to a biller;
- by PayTo;
- at selected ATMs, if your account is linked to an access card;
- via selected EFTPOS terminals, if your account is linked to an access card (note that merchants may impose restrictions on withdrawing cash and in some cases, charge a fee);
- via Bank@Post;

unless otherwise indicated in the *Summary of Accounts & Availability of Access Facilities* brochure.

We will require acceptable proof of your identity before processing withdrawals in person or acceptable proof of your authorisation for other types of withdrawal transactions.

Debiting transactions generally

We will debit transactions received on any one day in the order we determine in our absolute discretion. Transactions will not necessarily be processed to your account on the same day.

We have the right to decline to accept your authorisation for any transaction if we are uncertain for any reason of the authenticity or validity of the authorisation or your legal capacity to give the authorisation. We may also delay or not process a transaction for any of the reasons set out in "*Closing accounts, cancelling access facilities & delaying, blocking, freezing or refusing transactions"* on page 6. We will not be liable to you or any other person for any loss or damage which you or such other person may suffer as a result of us reasonably exercising these rights.

If you close your account before a transaction debit is processed, you will remain liable for any dishonour fees incurred in respect of that transaction.

Over the counter withdrawals

Generally, you can make over-the-counter withdrawals in cash.

Please check:

- the *Summary of Accounts & Availability of Access Facilities* brochure for any restrictions on withdrawals applying to certain accounts;
- the *Fees & Charges and Transaction Limits* brochure for any applicable daily cash withdrawal limits or other transaction limits.

Transaction limits

We limit the amount of daily withdrawals or payments you may make, either generally or in relation to a particular facility. These transaction limits are set out in the *Fees & Charges and Transaction Limits* brochure.

Please note that merchants, billers or other financial institutions may impose additional restrictions on the amount of funds that you can withdraw, pay or transfer.

We may, on application from you, agree to vary a transaction limit. We may also require you to apply for new transaction limits if you change any passcode. We may reduce transaction limits to zero for security reasons.

Overdrawing an account

You must keep sufficient cleared funds in your account to cover your direct debit and electronic transactions (including PayTo payments). If you do not, we can dishonour the transaction and charge dishonour fees: see the *Fees & Charges and Transaction Limits* brochure.

Alternatively, we can honour the transaction and overdraw your account. We will charge you:

- interest at our current overdraft rate, calculated on the daily closing balance; or
- a fee for each day (or part of a day) your account is overdrawn: see the *Fees & Charges and Transaction Limits* brochure.

'Cleared funds' means: the proceeds of cheque deposits to your account once the cheque is cleared, cash deposits and direct credits.

Sweep facility

You may nominate an account (the first account) which is to have either a nominated minimum balance or to be maintained in credit. You may then nominate a second account, which authorises us to transfer, automatically, sufficient funds to keep the first account at its nominated balance or in credit. However, we are not obliged to transfer funds if there are insufficient funds in the second account to draw on.

Account statements

We will send you account statements at least every 6 months. You can ask us for an account statement at any time. We may charge a fee for providing additional statements or copies: see the *Fees & Charges and Transaction Limits* brochure.

We may offer 'digital only' accounts, with statements provided electronically via internet or mobile banking only: see the *Summary of Accounts & Availability of Access Facilities* brochure.

For all other accounts, statements will normally be provided electronically via internet or mobile banking unless:

- you request that statements be sent in paper form;
- you have not registered for internet banking access; or
- you have not provided us with an email address or mobile phone number we can use to notify you when the statements are available;

in which case we will provide paper statements and may charge you a fee: see the *Fees and Charges and Transaction Limits* brochure. We may provide paper statements in other circumstances.

We recommend that you check your account statement as soon as you receive it. Immediately notify us of any unauthorised transactions or errors. Please refer to "*How to contact us"* on page 1 for our contact details.

What happens if my details change?

You must let us know immediately if you change any of your personal details including your name, address, email address or mobile phone number. You can update your contact details via internet banking or by contacting us *(*see "*How to contact us"* on page 1).

Dormant accounts

If no transactions are carried out on your account for at least 12 months (other than transactions initiated by the Bank, such as crediting interest or debiting fees and charges) we may write to you asking if you want to keep the account open. If you do not reply within 10 business days of the date of our notice to you, we will treat your account as dormant.

Once your account becomes dormant, we may:

- charge a dormancy fee;
- stop paying interest or reduce the amount of interest.

If your account remains dormant for 7 years we have a legal obligation to remit balances exceeding $500 to the Australian Securities and Investment Commission as unclaimed money.

Account combination

If you have more than one account with us, we may apply a deposit balance in any account to any other deposit account in the same name which is overdrawn.

When you cease to be a customer we may combine all your accounts (whether deposit or loan accounts) you have with us provided the accounts are all in the same name.

We will not combine accounts if to do so would breach the Code of Operation: Recovery of Debts from Customer Nominated Bank Accounts in receipt of Services Australia income support payments or Department of Veterans Affairs' payments and any successor Code (both when enforcing indebtedness owed to us and, to the extent the law permits, when facilitating enforcement by a third party judgement creditor).

We will give you written notice promptly after exercising any right to combine your accounts.

Term deposits

1. A minimum of $5000 will apply to all new deposits.

2. Your Term Deposit is lodged for a fixed term as specified in your *Certificate of Investment*. Subject to clause 6, the interest rate is fixed, and is not subject to variation, during the term. Interest is calculated on the daily closing balance. The annual interest rate applying to your Term Deposit is specified in your Certificate of Investment.

3. Interest is paid at maturity. For terms greater than 12 months, interest is also paid annually (unless paid more frequently). Where available, you may at the time of application select fortnightly or monthly interest payments, which may be subject to lower interest rates (refer to the Bank's *Deposit Interest Rate Schedule* for current rates). Interest will only be compounded to the principal at maturity. Interest payments made other than on maturity will be credited or paid to your nominated account at the Bank or other ADI. If you do not nominate an account, interest will be credited to an account you hold at the Bank.

4. We will follow the instructions received from you when the Term Deposit account was established as to how it will be treated at maturity. You may change these instructions by providing notice to us before the maturity date. However, if you have not provided any instructions to us before the maturity date of your Term Deposit, we will renew the Term Deposit for the same term (or most similar term then available), at the standard interest rate then payable by the Bank on deposits for that amount and term.

5. When you re-invest your Term Deposit, you should be aware that higher interest rates may be available for other terms. Before making your decision, you should review the Bank's *Deposit Interest Rates Schedule* (currently available at www.australianmutual.bank).

6. On closure of the Term Deposit, including at maturity, the principal and any unpaid accrued interest will be paid to your nominated deposit account. Amounts payable on closure prior to maturity are subject to clauses 7 & 8.

7. You may withdraw part or all of the Term Deposit before maturity. A reduced rate of interest will be paid on the amount withdrawn for the period from the Deposit Date to the date of early redemption. We may waive this condition for cases of emergency and financial hardship. Refer to the Bank's *Deposit Interest Rate Schedule* for current early redemption rates.

8. If interest has been previously paid at the certificate rate and part or all of the Term Deposit is redeemed prior to maturity, the interest previously paid will be recalculated at the early redemption rate. The difference will be deducted from the interest payable at the time of redemption, or if this is not sufficient, an adjustment of the withdrawn principal amount will occur.

9. Term Deposits of $1,000,000 and over are subject to acceptance by the Bank and rates are by negotiation.

Would you like more information?
Please visit the Bank's website to find further information on your accounts and to see how we manage your personal information at www.australianmutual.bank.

Closing accounts, cancelling access facilities & delaying, blocking, freezing or refusing transactions

You can close the Australian Mutual Bank Account and Access Facility at any time. However, you will have to surrender any access card at the time. We may defer closure and withhold sufficient funds to cover payment of outstanding electronic transactions and fees, if applicable.

You can cancel any access facility on request at any time.

We can close the Account and Access Facility in our absolute discretion by giving you at least 14 days' notice. However, without prior notice, we can close, or suspend your access to, any account, cancel any access facility, or delay, block, freeze or refuse any transaction:

- if we reasonably believe doing so will protect you or us from harm or loss;
- if we reasonably suspect fraudulent or illegal use of the account or access facility;
- if we reasonably suspect that a transaction may breach a law or sanction;
- to comply with our legal and regulatory obligations, including with our related policies and procedures; or
- if you fail to provide us with information or documents we reasonably request.

We will act fairly and reasonably towards you when taking such action without prior notice.

If we close your account, we will pay you the net credit balance in the account unless we reasonably believe that our legal or regulatory obligations prevent us from doing so and subject to our right to combine accounts (see "*Account combination*" on page 6).

No tolerance for financial abuse

Bank accounts must not be used for engaging in any form of financial abuse, unlawful conduct, or any offensive, threatening,

defamatory, harassing, or controlling behaviour. If such activity is detected or reported, we may issue a warning, restrict access, or close your account.

If you are experiencing financial abuse and wish to discuss support options, please contact us. Further information on financial abuse is available on our website.

Notifying changes

We may change fees, charges, interest rates and other conditions applicable to the Account & Access Facility at any time. We will act reasonably in making these changes and only do so for legitimate business purposes. If you do not like the change, you can ask us to close your Account and Access Facility, or close any account or cancel any access facility in it, in accordance with these Conditions of Use: see "*Closing accounts, cancelling access facilities & delaying, blocking, freezing or refusing transactions*" on page 6.

The following table sets when we will notify you of any change.

Type of change	Notice
Increasing any fee or charge	20 days
Adding a new fee or charge	20 days
Reducing the number of fee-free transactions permitted on your account	20 days
Changing the minimum balance to which an account keeping fee applies	20 days
Changing the method by which interest is calculated	20 days
Changing the circumstances when interest is credited or debited to your account	20 days
Increasing your liability for losses relating to ePayments (see the ePayments Conditions of Use Section 3 on page 10 for a description of ePayments)	20 days
Imposing, removing or changing any periodic transaction limit relating to ePayments	20 days
Changing an interest rate	the day of change

For all other changes, we will provide reasonable notice (which, depending on the nature of the change, may be before or after the change is made). If we reasonably consider that such a change is unfavourable to you, we will provide at least 20 days' notice. However, we may give shorter, or no, advance notice of a change unfavourable to you if it is reasonable for us to manage a material and immediate risk.

We may use various methods, and combinations of methods, to notify you of any changes, such as:

- notification by letter or other direct communication (including by electronic means);
- notification on or with your next statement of account;
- notification on or with the next newsletter;
- advertisements in the local or national media;
- notification on our website.

However, we will always select a method or methods we reasonably consider appropriate to the nature and extent of the change, as well as the cost and effectiveness of the method of notification.

We will always provide notice in accordance with any applicable law or industry code (such as the Customer Owned Banking Code of Practice).

If there is a change to, or introduction of a government charge that you directly or indirectly pay as part of your banking service, we will tell you about this reasonably promptly after the government notifies us, unless the government itself publicises the introduction or change.

How we send notices & statements

To the extent permitted by law, we may send you notices and statements:

- by post, to the address recorded in our records or to a mailing address you nominate;
- by electronic means, including by email to an email address you have given us, SMS to a mobile phone number you have given us, or push notification to our mobile banking app;
- by advertisement in the media or our website, for some notices only;
- by other means we agree with you.

We may, instead of sending you a notice or statement, post notices or statements to our website or internet banking service for you to retrieve. In that case we will notify you via email or other electronic means, when information is available for you to retrieve.

Unless the account is a digital only product (see the *Summary of Accounts & Availability of Access Facilities* brochure), you can revert to receiving paper notices or statements, at any time. We may charge a fee for providing paper statements or notices: see the *Fees and Charges and Transaction Limits* brochure.

You must ensure your address and other contact details, including email address and mobile phone number, are correct and up to date at all times.

Direct debit

One way you can authorise a participating biller to debit amounts from your eligible account (using your BSB and account number), as and when you owe those amounts to the biller, is as a direct debit. The biller will provide you with a Direct Debit Request (DDR) Service Agreement for you to complete and sign to provide them with this authority.

To cancel the DDR Service Agreement, you can contact either the biller or us. If you contact us, we will take action within 1 business day to cancel the facility. We suggest that you also contact the biller.

We will promptly investigate if you inform us that a direct debit was not authorised or is otherwise irregular. We suggest that you also contact the biller. However, we are not liable to compensate you for your biller's error.

If you set up the payment on your Visa debit card, please contact us directly about unauthorised or irregular debits.

We can cancel your direct debit facility, in our absolute discretion, if 3 consecutive direct debit instructions are dishonoured. If we do this, billers will not be able to initiate a direct debit from your account under their DDR Service Agreement. Under the terms of their DDR Service Agreement, the biller may charge you a fee for each dishonour of their direct debit request.

This section does not apply to PayTo, which provides an alternative method to pre-authorise a biller to debit amounts from your eligible account. For PayTo see "*Electronic Access Facilities and ePayments conditions of use*" Section 28 to Section 36.

Electronic access facilities and ePayments conditions of use

SECTION 1. INFORMATION ABOUT YOUR EPAYMENT FACILITIES

You should follow the guidelines in the box below to protect against unauthorised use of your access cards, devices and passcodes. These guidelines provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised ePayments. Liability for such transactions will be determined in accordance with the ePayments Conditions of Use and the ePayments Code.

Important Information About Protecting Your Access Cards, Devices and Passcodes

- Familiarise yourself with your obligations to keep your access card and passcodes secure;
- Familiarise yourself with the steps you have to take to report loss or theft of your access card or device, or to report unauthorised use of your access card, BPAY®, Osko or PayTo payment facility, internet or mobile banking;
- Immediately report lost, theft or unauthorised use or access (see "*How to contact us*" on page 1);
- If you change a passcode, do not select a passcode which represents your birth date or a recognisable part of your name;
- Never write or save the passcode on any access card, mobile phone, computer or device, even if disguised;
- Never write the passcode on anything which is kept with or near any access card, mobile phone, computer or device;
- Never lend the access card to anybody;
- Never tell or show the passcode to another person;
- Use care to prevent anyone seeing the passcode being entered on any electronic equipment;
- Keep a record of the VISA card number and the VISA Card Hotline phone number for your area with your usual list of emergency phone numbers;
- Check your statements regularly for any unauthorised use;
- Immediately notify us when you change your address, and ensure your contact details, including email address and mobile phone number, are correct and up to date at all times;
- ALWAYS access the internet banking service only using the OFFICIAL phone numbers and URL addresses;
- NEVER access internet banking via a link in an email, SMS or other electronic message;
- If accessing internet banking on someone else's PC, laptop, tablet or mobile phone, ALWAYS DELETE your browsing history;
- ALWAYS REJECT any request to provide or to confirm details of your passcode. We will NEVER ask you to provide us with these details.

If you fail to ensure the security of your access card, access facility and passcodes you may increase your liability for unauthorised transaction.

These ePayment Conditions of Use govern all electronic transactions made using any one of our access cards or facilities, listed below:

- Visa Card;
- BPAY®;
- Osko Payments;
- PayTo;
- Internet Banking;
- Mobile Banking;

You can use any of these electronic access facilities to access an account, as listed in the *Summary of Accounts & Availability of Access Facilities* brochure.

Visa Card

Visa Card allows you to make payments at any retailer displaying the Visa Card logo, anywhere in the world. You can also withdraw cash from your account, anywhere in the world, using an ATM displaying the Visa Card logo. We will provide you with a PIN to use with your Visa Card. Visa Card also allows you to:

- check your account balances;
- transfer money between accounts.

We may choose not to give you a Visa Card if, in our reasonable opinion, your banking history with the Bank is not satisfactory or if you are under 18 years of age.

Important Information about Chargebacks for VISA Card

If you wish to dispute a Visa Card transaction you should notify us as soon as possible but within 120 days. Under the card scheme rules we can seek a refund of Visa Card purchases from the merchant's financial institution in certain circumstances, such as non-delivery of goods or services ordered, unauthorised purchases, or payments under a regular payment arrangement that you had already cancelled. This is called a 'chargeback'.

The card scheme rules impose strict timeframes on requesting chargebacks. We will need to investigate a disputed transaction to determine if we have a right to a chargeback. You must provide us with any information or material we request to investigate the transaction and support the chargeback request. If we determine that we have a right to a chargeback we will seek it without delay.

It is in your own interest to notify us as soon as possible if you become aware of circumstances which might entitle us to claim a chargeback on your behalf.

However, you should seek to resolve the issue with the merchant first.

Please note that chargebacks do not apply to BPAY® payments.

CONFIRMATION OF PAYEE

Confirmation of Payee service

1.1 Confirmation of Payee is a service that applies when sending money to an account using BSB and account number. It is designed to help payers avoid scams or mistaken payments.

1.2 The Confirmation of Payee service matches the account details entered (which must also include an account name) with the account details held by the recipient's financial institution and displays the outcome, which could be a match, a close match or a no match.

1.3 If the intended recipient is a business or other organisation, or the outcome is a match or close match, then the account name will be displayed to the payer.

Conducting a Confirmation of Payee lookup

1.4 When making a payment from your account using BSB and account number it is the user's responsibility to ensure they provide the correct BSB and account number.

1.5 The Confirmation of Payee service will provide the user with a match, a close match or a no match outcome. If the user thinks the account details were entered incorrectly, they can check them again before making the payment. If something does not seem right, the user should check the account details with the intended recipient before proceeding, or choose not to proceed with the payment.

1.6 You must not use, and must ensure any other user does not use, the Confirmation of Payee service other than for its intended purpose, or in breach of these Conditions of Use. We may limit or suspend use of the Confirmation of Payee service from your account if we believe it reasonably necessary to protect you, us or a third party from possible fraudulent activity, scams or other activity that may cause loss or damage.

1.7 We are not responsible for the accuracy of the recipient's account details provided to us from the recipient's financial institution.

Use and disclosure of your account details

1.8 You authorise, and provide consent to:

(a) us to use, store and disclose your account details in the Confirmation of Payee service; and

(b) payers' financial institutions to use and disclose your account details for the purposes of the Confirmation of Payee service and prior to making payments to you.

1.9 In special circumstances we may allow you to opt-out of the Confirmation of Payee service. Please contact us on 13 61 91.

1.10 However, even if you do opt-out of the service, we will still confirm, disclose, store and use your account details through the Confirmation of Payee service for use by government agencies for the purposes of making a payment to you.

1.11 In some circumstances you may provide alternative names to be recorded on your account for use in the Confirmation of Payee service. Please contact us on 13 61 91.

SECTION 2. DEFINITIONS

(a) **access card** means an ATM card, debit card or credit card and includes our Visa Card.

(b) **account details** means our record of your account, including BSB, account number, account name, your full legal name, any other name you prefer us to use and account activity.

(c) **AFCA** means the Australian Financial Complaints Authority.

(d) **ATM** means automatic teller machine.

(e) **BECS Procedures** means the Bulk Electronic Clearing System Procedures as existing from time to time.

(f) **business day** means a day that is not a Saturday, a Sunday or a public holiday or bank holiday in the place concerned.

(g) **device** means a device we give to a user that is used to perform a transaction. Examples include:

(i) ATM card

(ii) debit card or credit card, whether physical or virtual

(iii) token issued by a us that generates a passcode.

(h) **direct debit** means a "Direct Debit Request" as defined in the BECS Procedures.

(i) **EFTPOS** means electronic funds transfer at the point of sale—a network for facilitating transactions at point of sale.

(j) **facility** means an arrangement through which you can perform transactions.

(k) **identifier** means information that a user:

(i) knows but is not required to keep secret; and

(ii) must provide to perform a transaction.

Examples include an account number, customer number or PayID. An identifier also includes a token generated from information that would otherwise be an identifier.

(l) **Mandate Management Service** means the central, secure database operated by NPP Australia Limited of Payment Agreements.

(m) **manual signature** means a handwritten signature, including a signature written on paper and a signature written on an electronic tablet.

(n) **Migrated DDR Mandates** has the meaning given in clause 33.1.

(o) **NPP** means the New Payments Platform operated by NPP Australia Limited.

(p) **NPP Payments** means electronic payments cleared and settled by participating financial institutions via the NPP.

(q) **Osko** by BPAY in most instances is a near real-time payment system which enables you to transfer funds between participating banks.

(r) **passcode** means a password or code that the user must keep secret, that may be required to authenticate a transaction or user. A passcode may consist of numbers, letters, a combination of both, or a phrase.

Examples include:

(i) personal identification number (PIN);

(ii) internet banking password;

(iii) code generated by a physical security token;

(iv) code provided to a user by SMS, email or in a mobile application.

A passcode does not include a number printed on a device (e.g. a security number printed on a credit or debit card).

Note: a passcode includes single-use passwords or codes, as well as passwords or codes that are used more than once.

(s) **pay anyone banking facility** means a facility where a user can make a payment from one bank account to a third party's bank account by entering, selecting or using a Bank/State/Branch (BSB) and account number, PayID or other identifier, but does not include BPAY® or PayTo payments.

(t) **Payment Agreement** means an agreement established by you and an approved merchant or Payment Initiator, by which you authorise us to make payments from your account. Other than in Section 28 "*CREATING A PAYTO PAYMENT AGREEMENT*", it includes a Migrated DDR Mandate.

(u) **Payment Initiator** means an approved payment service provider who, whether acting on behalf of you or a merchant, is authorised by you to initiate payments from your account.

(v) **PayTo** means the service which enables us to process NPP Payments from your account in accordance with and on the terms set out in a Payment Agreement you have established with a merchant or Payment Initiator that subscribes to the service.

(w) **regular payment arrangement** means either a recurring or an instalment payment agreement between you (the cardholder) and a merchant in which you have preauthorised the merchant to bill your account using your debit card or credit card details at predetermined intervals (e.g. monthly or quarterly) or at intervals agreed by you. The amount may differ or be the same for each transaction.

(x) **transaction** means a transaction to which these ePayment Conditions of Use apply, as set out in Section 3.

(y) **Transfer ID** means a unique identification number generated by the Mandate Management Service in connection with a request to transfer one or more Payment Agreements.

(z) **unauthorised transaction** means a transaction that is not authorised by a user. It does not include any transaction that is performed by you or another user, or by anyone who performs a transaction with the knowledge and consent of you or another user.

(aa) **user** means you or an individual you have authorised to perform transactions on your account, including:

(i) a third party signatory to your account;

(ii) a person you authorise us to issue an additional card to.

(ab) **we, us, or our** means Australian Mutual Bank Ltd.

(ac) **you** means the person or persons in whose name this Account and Access Facility is held.

SECTION 3. TRANSACTIONS

3.1. These ePayment Conditions of Use apply to payment, funds transfer and cash withdrawal transactions that are:

(a) initiated using electronic equipment; and

(b) not intended to be authenticated by comparing a manual signature with a specimen signature.

3.2. Without limiting clause 3.1, these ePayment Conditions of Use apply to the following transactions:

(a) electronic card transactions, including ATM, EFTPOS, credit card and debit card transactions that are not intended to be authenticated by comparing a manual signature with a specimen signature;

(b) bill payment transactions;

(c) pay anyone banking facility transactions;

(d) online transactions performed using a card number and expiry date;

(e) online bill payments (including BPAY®);

(f) direct debits;

(g) transactions using mobile devices;

(h) PayTo Payments.

SECTION 4. WHEN YOU ARE NOT LIABLE FOR LOSS

4.1. You are not liable for loss arising from an unauthorised transaction if the cause of the loss is any of the following:

(a) fraud or negligence by our employee or agent, a third party involved in networking arrangements, or a merchant or their employee or agent;

(b) a device, identifier or passcode which is forged, faulty, expired or cancelled;

(c) a transaction requiring the use of a device and/or passcode that occurred before the user received the device and/or passcode (including a reissued device and/or passcode);

(d) a transaction being incorrectly debited more than once to the same facility;

(e) an unauthorised transaction performed after we have been informed that a device has been misused, lost or stolen, or the security of a passcode has been breached.

4.2. You are not liable for loss arising from an unauthorised transaction that can be made using an identifier without a passcode or device. Where a transaction can be made using a device, or a device and an identifier, but does not require a passcode, you are liable only if the user unreasonably delays reporting the loss or theft of the device.

4.3. You are not liable for loss arising from an unauthorised transaction where it is clear that a user has not contributed to the loss.

4.4. In a dispute about whether a user received a device or passcode:
(a) there is a presumption that the user did not receive it, unless we can prove that the user did receive it;
(b) we can prove that a user received a device or passcode by obtaining an acknowledgement of receipt from the user;
(c) we may not rely on proof of delivery to a user's correct mailing or electronic address as proof that the user received the device or passcode.

SECTION 5. WHEN YOU ARE LIABLE FOR LOSS

5.1. If Section 4 does not apply, you may only be made liable for losses arising from an unauthorised transaction in the circumstances specified in this Section 5.

5.2. Where we can prove on the balance of probability that a user contributed to a loss through fraud, or breaching the passcode security requirements in Section 6:
(a) you are liable in full for the actual losses that occur before the loss, theft or misuse of a device or breach of passcode security is reported to us;
(b) you are not liable for the portion of losses:
(i) incurred on any one day that exceeds any applicable daily transaction limit;
(ii) incurred in any period that exceeds any applicable periodic transaction limit;
(iii) that exceeds the balance on the facility, including any pre-arranged credit;
(iv) incurred on any facility that we and you had not agreed could be accessed using the device or identifier and/or passcode used to perform the transaction.

5.3. Where:
(a) more than one passcode is required to perform a transaction; and
(b) we prove that a user breached the passcode security requirements in Section 6 for one or more of the required passcodes, but not all of the required passcodes you are liable under clause 5.2 only if we also prove on the balance of probability that the breach of the passcode security requirements under Section 6 was more than 50% responsible for the losses, when assessed together with all the contributing causes.

5.4. You are liable for losses arising from unauthorised transactions that occur because a user contributed to losses by leaving a card in an ATM, as long as the ATM incorporates reasonable safety standards that mitigate the risk of a card being left in the ATM.

Note: Reasonable safety standards that mitigate the risk of a card being left in an ATM include ATMs that capture cards that are not removed after a reasonable time and ATMs that require a user to swipe and then remove a card in order to commence a transaction.

5.5. Where we can prove, on the balance of probability, that a user contributed to losses resulting from an unauthorised transaction by unreasonably delaying reporting the misuse, loss or theft of a device, or that the security of all passcodes has been breached, you:
(a) are liable for the actual losses that occur between:
(i) when the user became aware of the security compromise, or should reasonably have become aware in the case of a lost or stolen device; and
(ii) when the security compromise was reported to us.
(b) are not liable for any portion of the losses:
(i) incurred on any one day that exceeds any applicable daily transaction limit;
(ii) incurred in any period that exceeds any applicable periodic transaction limit;
(iii) that exceeds the balance on the facility including any pre-arranged credit;
(iv) incurred on any facility that we and you had not agreed could be accessed using the device and/or passcode used to perform the transaction.

Note: You may be liable under clause 5.5 if you were the user who contributed to the loss, or if a different user contributed to the loss.

5.6. Where a passcode was required to perform an unauthorised transaction, and clauses 5.2-5.5 do not apply, you are liable for the least of:
(a) $150, or a lower figure determined by us;
(b) the balance of the facility or facilities which we and you have agreed can be accessed using the device and/or passcode, including any prearranged credit;
(c) the actual loss at the time that the misuse, loss or theft of a device or breach of passcode security is reported to us, excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit.

5.7. In deciding whether on the balance of probabilities we have proved that a user has contributed to losses under clauses 5.2 and 5.5:
(a) we must consider all reasonable evidence, including all reasonable explanations for the transaction occurring;
(b) the fact that a facility has been accessed with the correct device and/or passcode, while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the passcode security requirements in Section 6;
(c) the use or security of any information required to perform a transaction that is not required to be kept secret by users (for example, the number and expiry date of a device) is not relevant to a user's liability.

5.8. If a user reports an unauthorised transaction on a credit card account, debit card account or charge card account we will not hold you liable for losses under Section 5 for an amount greater than your liability if we exercised any rights

we had under the rules of the card scheme at the time the report was made, against other parties to the scheme (for example, charge-back rights).

This clause does not require us to exercise any rights we may have under the rules of the card scheme. However, we cannot hold you liable under this clause for a greater amount than would apply if we had exercised those rights.

SECTION 6. PASSCODE SECURITY REQUIREMENTS

6.1. Section 6 applies where one or more passcodes are needed to perform a transaction.

6.2. A user must not:

(a) voluntarily disclose one or more passcodes to anyone, including a family member or friend;

(b) where a device is also needed to perform a transaction, write or record passcode(s) on a device, or keep a record of the passcode(s) on anything:

(i) carried with a device;

(ii) liable to loss or theft simultaneously with a device unless the user makes a reasonable attempt to protect the security of the passcode.

(c) where a device is not needed to perform a transaction, keep a written record of all passcodes required to perform transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the passcode(s).

Note: If you or another user breaches these passcode security requirements, we may not be required to indemnify you for loss arising from that breach. See Section 5.

6.3. For the purpose of clauses 6.2(b)–6.2(c), a reasonable attempt to protect the security of a passcode record includes making any reasonable attempt to disguise the passcode within the record, or prevent unauthorised access to the passcode record, including by:

(a) hiding or disguising the passcode record among other records;

(b) hiding or disguising the passcode record in a place where a passcode record would not be expected to be found;

(c) keeping a record of the passcode record in a securely locked container;

(d) preventing unauthorised access to an electronically stored record of the passcode record.

This list is not exhaustive.

6.4. A user must not act with extreme carelessness in failing to protect the security of all passcodes where extreme carelessness means a degree of carelessness that greatly exceeds what would normally be considered careless behaviour.

Note 1: An example of extreme carelessness is storing a user name and passcode for internet banking in a diary, computer or other personal electronic device that is not password protected under the heading 'Internet banking codes'.

Note 2: For the obligations applying to the selection of a passcode by a user, see clause 6.5.

6.5. A user must not select a numeric passcode that represents their birth date, or an alphabetical passcode that is a recognisable part of their name, if we have:

(a) specifically instructed the user not to do so;

(b) warned the user of the consequences of doing so.

6.6. The onus is on us to prove, on the balance of probability, that we have complied with clause 6.5.

6.7. Where we expressly authorise particular conduct by a user, either generally or subject to conditions, a user who engages in the conduct, complying with any conditions, does not breach the passcode security requirements in Section 6.

6.8. Where we expressly or implicitly promote, endorse or authorise the use of a service for accessing a facility (for example, by hosting an access service on our electronic address), a user who discloses, records or stores a passcode that is required or recommended for the purpose of using the service does not breach the passcode security requirements in Section 6.

6.9. For the purposes of clause 6.8, we are not taken to have promoted, endorsed or authorised a user's use of a particular service merely because we have chosen to use the service for our own purposes or have not actively prevented the user from accessing a service.

SECTION 7. LIABILITY FOR LOSS CAUSED BY SYSTEM OR EQUIPMENT MALFUNCTION

7.1. You are not liable for loss caused by the failure of a system or equipment provided by any party to a shared electronic network to complete a transaction accepted by the system or equipment in accordance with a user's instructions.

7.2. Where a user should reasonably have been aware that a system or equipment provided by any party to a shared electronic network was unavailable or malfunctioning, our liability is limited to:

(a) correcting any errors;

(b) refunding any fees or charges imposed on the user.

SECTION 8. NETWORK ARRANGEMENTS

8.1. We must not avoid any obligation owed to you on the basis that:

(a) we are a party to a shared electronic payments network;

(b) another party to the network caused the failure to meet the obligation.

8.2. We must not require you to:

(a) raise a complaint or dispute about the processing of a transaction with any other party to a shared electronic payments network;

(b) have a complaint or dispute investigated by another party to a shared electronic payments network.

SECTION 9.
MISTAKEN INTERNET PAYMENTS

9.1. In this Section 9:

(a) **mistaken internet payment** means a payment by a user through a 'pay anyone' banking facility and processed by an ADI where funds are paid into the account of an unintended recipient because the user enters or selects a Bank/State/Branch (BSB) number and/or identifier that does not belong to the named and/or intended recipient as a result of:

(i) the user's error; or

(ii) the user being advised of the wrong BSB number and/or identifier.

Note: this definition of mistaken internet payment is intended to relate to typographical errors when inputting an identifier or selecting the incorrect identifier from a list. It is not intended to cover situations in which the user transfers funds to the recipient as a result of a scam.

(b) **receiving ADI** means an ADI whose customer has received an internet payment;

(c) **unintended recipient** means the recipient of funds as a result of a mistaken internet payment.

9.2. When you report a mistaken internet payment, we must investigate whether a mistaken internet payment has occurred.

9.3. If we are satisfied that a mistaken internet payment has occurred, we must as soon as reasonably possible and by no later than 5 business days from the time of the user's report of a mistaken internet payment, send the receiving ADI a request for the return of the funds.

Note: Under the ePayments Code, the receiving ADI must within 5 business days of receiving our request:

(i) acknowledge the request for the return of funds; and

(ii) advise us whether there are sufficient funds in the account of the unintended recipient to cover the mistaken internet payment.

9.4. If we are not satisfied that a mistaken internet payment has occurred, we will not take any further action.

9.5. We must inform you of the outcome of the reported mistaken internet payment in writing and within 30 business days of the day on which the report is made.

9.6. You may complain to us about how the report is dealt with, including that we:

(a) are not satisfied that a mistaken internet payment has occurred;

(b) have not complied with the processes and timeframes set out in clauses 9.2-9.5, or as described in the box below.

9.7. When we receive a complaint under clause 9.6 we must:

(a) deal with the complaint under our internal dispute resolution procedures;

(b) not require you to complain to the receiving ADI.

9.8. If you are not satisfied with the outcome of a complaint, you are able to complain to AFCA.

9.9 If you receive a mistaken internet payment into your account and we are required under the ePayments Code as receiving ADI to return the funds to the payer's ADI then we will, without seeking your consent, transfer the funds from your account. If there are insufficient funds in your account you must co-operate with us to facilitate repayment of the funds.

Information about a receiving ADI's obligations after we request return of funds

The information set out in this box is to explain the process for retrieving mistaken payments under the ePayments Code, setting out what the processes are, and what you are entitled to do.

This information does not give you any contractual entitlement to recover the mistaken payment from us or to recover the mistaken payment from the receiving ADI.

Process where sufficient funds are available & report is made within 10 business days:

- If satisfied that a mistaken internet payment has occurred, the receiving ADI must return the funds to the sending ADI, within 5 business days of receiving the request from the sending ADI if practicable or such longer period as is reasonably necessary, up to a maximum of 10 business days;
- If not satisfied that a mistaken internet payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder;
- The sending ADI must return the funds to the holder as soon as practicable.

Process where sufficient funds are available & report is made between 10 business days & 7 months:

- The receiving ADI must complete its investigation into the reported mistaken payment within 10 business days of receiving the request;
- If satisfied that a mistaken internet payment has occurred, the receiving ADI must:
  - (a) prevent the unintended recipient from withdrawing the funds for 10 further business days; and
  - (b) notify the unintended recipient that it will withdraw the funds from their account, if the unintended recipient does not establish that they are entitled to the funds within 10 business days commencing on the day the unintended recipient was prevented from withdrawing the funds.
- If the unintended recipient does not, within 10 business days, establish that they are entitled to the funds, the receiving ADI must return the funds to the sending ADI within 2 business days after the expiry of the 10 business day period, during which the unintended recipient is prevented from withdrawing the funds from their account;
- If the receiving ADI is not satisfied that a mistaken internet payment has occurred, it may seek the consent of the unintended recipient to return the funds to the holder;

- The sending ADI must return the funds to the holder as soon as practicable.

Process where sufficient funds are available and report is made after 7 months:

- If the receiving ADI is satisfied that a mistaken internet payment has occurred, it must seek the consent of the unintended recipient to return the funds to the user;
- If not satisfied that a mistaken internet payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder;
- If the unintended recipient consents to the return of the funds:
  (a) the receiving ADI must return the funds to the sending ADI; and
  (b) the sending ADI must return the funds to the holder as soon as practicable.

Process where sufficient funds are not available:

- Where the sending ADI and the receiving ADI are satisfied that a mistaken internet payment has occurred, but there are not sufficient credit funds available in the account of the unintended recipient to the full value of the mistaken internet payment, the receiving ADI must exercise discretion, after appropriate weighing of interests of the sending consumer and unintended recipient and information reasonably available to it about the circumstances of the mistake and the unintended recipient, in deciding whether it should pursue return of the total value of the mistaken internet payment, pursue the return of a partial amount of the mistaken internet payment, or not pursue any return of funds;
- The above processes where sufficient funds are available will also apply where insufficient funds are available, but only in relation to the value of the insufficient funds available.

Our Conditions of Use require you to report these events to us immediately:

- if your Device has been lost or stolen;
- you believe your security credentials have been compromised;
- if you believe there are errors;
- if you suspect fraud associated with your Digital Wallet.

You may become liable for any unauthorised transactions if you unreasonably delay notifying us.

SECTION 10.
USING INTERNET OR MOBILE BANKING

10.1. We do not warrant that:
  (a) the information available to you about your accounts through our internet or mobile banking service is always up to date;
  (b) you will have 24 hours a day, 7 days per week, access to internet or mobile banking;
  (c) data you transmit via internet or mobile banking is totally secure.

10.2 Internet and mobile banking will not be available from some countries including Cuba, Iran, North Korea, Syria and Russia.

SECTION 11.
HOW TO REPORT LOSS, THEFT OR UNAUTHORISED USE OF YOUR ACCESS CARD OR PASSCODE

11.1. If you believe your access card has been misused, lost or stolen or the passcode has become known to someone else, you must immediately contact us during business hours or the access card HOTLINE at any time.

Please refer to "*How to contact us*" on page 1 for our contact details.

11.2. We will acknowledge your notification by giving you a reference number that verifies the date and time you contacted us. Please retain this reference number.

11.3. The access card HOTLINE is available 24 hours a day, 7 days a week.

11.4. If the access card HOTLINE is not operating when you attempt notification, nevertheless, you must report the loss, theft or unauthorised use to us as soon as possible during business hours. We will be liable for any losses arising because the access card HOTLINE is not operating at the time of attempted notification, provided you report the loss, theft or unauthorised use to us as soon as possible during business hours.

11.5. If the loss, theft or misuse, occurs outside Australia you must notify us:
  (a) Call +61 2 8299 9101 (Vigil Helpline); or
  (b) Contact us by secure message (via internet banking or the mobile banking app), email us on info@australianmutual.bank, call +61 2 9678 2111; or
  (c) Calling the VISA Card Hotline number for the country you are in.

Visa Card Hotline
Australia Wide Toll Free
1800 648 027

SECTION 12.
HOW TO REPORT UNAUTHORISED USE OF INTERNET OR MOBILE BANKING

12.1. If you believe that your passcodes for internet or mobile banking transactions have been misused, lost or stolen, or, where relevant, your passcode has become known to someone else, you must contact us immediately. Please refer to "*How to contact us"* on page 1 for our contact details. We will acknowledge your notification by giving you a reference number that verifies the date and time you contacted us. Please retain this reference number.

12.2. If you believe an unauthorised transaction has been made and your access method uses a passcode, you should change that passcode.

SECTION 13.
USING THE ACCESS CARD

13.1. You agree to sign the access card immediately upon receiving it and before using it as a means of preventing fraudulent or unauthorised use of the access card. You must ensure that any other cardholder you authorise also signs their access card immediately upon receiving it and before using it.

13.2. We will advise you from time to time:

(a) what transactions may be performed using the access card;

(b) what ATMs of other financial institutions may be used; and

(c) what the daily cash withdrawal limits are.

Please refer to the *Fees & Charges and Transaction Limits* brochure for details of current transaction limits.

13.3. You may only use your access card to perform transactions on those accounts we permit. We will advise you of the accounts which you may use your access card to access.

13.4. The access card always remains our property.

SECTION 14.
INTERNATIONAL TRANSACTION FEES

We charge you an international transaction conversion fee of 3%, debited to your account on the transaction date, of which a service and assessment fee of up to 1% is payable by us to Visa and 1% is payable by us to Cuscal Ltd (as applicable), for any Retail Purchase or Cash Advance transaction in:

- Foreign currency once converted to Australian dollars; and/or
- Australian dollars (or any other currency), when either the merchant or its financial institution/payment processor is located or registered overseas, including transactions that involve Dynamic Currency Conversion (that is where a transaction denominated in a foreign currency is converted to Australian dollars which is a service that is offered by certain ATMs and merchants). The process of conversion and the exchange rates applied will be determined by the relevant ATM, merchant, or Dynamic Currency Conversion service provider as the case may be. We do not determine whether a Card transaction will be converted into Australian dollars by the merchant or ATM, and you may have to check with the relevant merchant or ATM provider;
- Please note that even though an online shopping website with a domain name ends in '.com.au' might appear to be an Australian business, they or their bank might be located overseas. This means you could still be charged an international transaction fee;
- Some overseas merchants and electronic terminals charge a surcharge for making a transaction using your Visa card. Once you have confirmed that transaction you will not be able to dispute the surcharge. The surcharge may appear on your statement as part of the purchase price;
- Some overseas merchants and electronics terminals allow the cardholder the option to convert the value of the Transaction into Australian dollars at the point of sale, also known as a Dynamic Currency Conversion. Once you have confirmed the transaction you will not be able to dispute the exchange rate applied;
- You agree to reimburse us for any costs, fees or charges of any nature arising out of a failure to comply with any exchange control requirements or tax laws.

This fee applies only when you make a transaction with a merchant or its financial institution/payment processor that is located or registered outside Australia.

Note: It may not always be clear that the merchant or its financial institution/payment processor is located or registered outside Australia.

SECTION 15.
ADDITIONAL ACCESS CARD

15.1. You may authorise us, if we agree, to issue an additional access card to an additional cardholder provided this person is over the age of 18 (unless we agree to a younger age).

15.2. You will be liable for all transactions carried out by this cardholder.

15.3. We will give each additional cardholder a separate passcode.

15.4. You must ensure that any additional cardholders protect their access card and passcode in the same way as these ePayment Conditions of Use require you to protect access card and passcode.

15.5. To cancel the additional access card you must notify us by phone, in person at any branch or in writing (including electronically). Please refer to "*How to contact us"* on page 1 for our contact details.

15.6. You will not be liable for the continued use of the additional access card after its cancellation.

SECTION 16.
USE AFTER CANCELLATION OR EXPIRY OF ACCESS CARD

16.1. You must not use your access card:

(a) before the valid date or after the expiration date shown on the face of access card; or

(b) after the access card has been cancelled.

16.2. You will continue to be liable to reimburse us for any indebtedness incurred through such use whether or not you have closed your account.

SECTION 17.
EXCLUSIONS OF ACCESS CARD WARRANTIES AND REPRESENTATIONS

17.1. We do not warrant that merchants or ATMs displaying access card signs or promotional material will accept access card.

17.2. We do not accept any responsibility should a merchant, bank or other institution displaying access card signs or promotional material, refuse to accept or honour access card.

17.3. We are not responsible for any defects in the goods and services you acquire through the use of the Visa Card. You acknowledge and accept that all complaints about these goods and services must be addressed to the supplier or merchant of those goods and services.

SECTION 18. CANCELLATION OF ACCESS CARD, INTERNET OR MOBILE BANKING SERVICE , BPAY®, OSKO® OR PAYTO

18.1. You may cancel your access card, your access to internet or mobile banking , BPAY®, Osko or PayTo at any time by giving us written notice or contact us on 13 61 91.

18.2. We may, acting reasonably, immediately cancel or suspend your access card or your access to internet or mobile banking, BPAY®, Osko or PayTo at any time:

(a) for security reasons;

(b) if you breach these Conditions of Use;

(c) if we reasonably suspect that you, or someone acting on your behalf, is being fraudulent;

(d) in the case of Osko, if we reasonably suspect that you are using Osko in a manner that is likely to affect our ability to continue providing Osko to you or our other customers;

(e) in the case of Osko or PayTo, if we cease to be a participant in Osko or PayTo;

(f) in the case of access card, we may cancel the access card by capture of the access card at any ATM;

(g) for any other reason set out in "*Closing accounts, cancelling access facilities & delaying, blocking, freezing or refusing transactions"* on page 6.

18.3. We may cancel your access card or your access to internet or mobile banking , BPAY®, Osko or PayTo for any reason by giving you 30 days' notice. The notice does not have to specify the reasons for cancellation.

18.4. In the case of access card, you will be liable for any transactions you make using your access card before the access card is cancelled but which are not posted to your account until after cancellation of access card.

18.5. In the case of internet or mobile banking, BPAY®, Osko or PayTo, if, despite the cancellation of your access to the relevant access method, you carry out a transaction using the relevant access method, you will remain liable for that transaction.

18.6. Your access card or your access to internet or mobile banking, BPAY®, Osko or PayTo will be terminated when:

(a) we notify you that we have cancelled your access card or your access method to the account with us;

(b) you close the last of your accounts with us to which the access card applies or which has internet or mobile banking , BPAY®, Osko or PayTo access;

(c) you alter the authorities governing the use of your account or accounts to which the access card applies or which has internet or mobile banking, BPAY®, Osko or PayTo access (unless we agree otherwise).

18.7. In the case of access card, we may demand the return or destruction of any cancelled access card.

SECTION 19. USING BPAY®

19.1. You can use BPAY® to pay bills bearing the BPAY® logo from those accounts that have the BPAY® facility.

19.2. When you tell us to make a BPAY® payment you must tell us the biller's code number (found on your bill), your Customer Reference Number (e.g. your account number with the biller), the amount to be paid and the account from which the amount is to be paid.

19.3. We cannot effect your BPAY® instructions if you do not give us all the specified information or if you give us inaccurate information.

Note: legally, the receipt by a biller of a mistaken or erroneous payment does not necessarily discharge, wholly or in part, the underlying debt you owe that biller.

SECTION 20. PROCESSING BPAY® PAYMENTS

20.1. We will attempt to make sure that your BPAY® payments are processed promptly by participants in BPAY®, and you must tell us promptly if:

(a) you become aware of any delays or mistakes in processing your BPAY® payment;

(b) you did not authorise a BPAY® payment that has been made from your account; or

(c) you think that you have been fraudulently induced to make a BPAY® payment.

Please keep a record of the BPAY® receipt numbers on the relevant bills.

20.2. A BPAY® payment instruction is irrevocable.

20.3. Except for future-dated payments you cannot stop a BPAY® payment once you have instructed us to make it and we cannot reverse it.

20.4. We will treat your BPAY® payment instruction as valid if, when you give it to us, you use the correct access method.

20.5. You should notify us immediately if you think that you have made a mistake (except for a mistake as to the amount you meant to pay).

Note: you must provide us with written consent addressed to the biller who received that BPAY® 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 BPAY® payment.

20.6. A BPAY® payment is treated as received by the biller to whom it is directed:

(a) on the date you direct us to make it, if we receive your direction by the cut off time on a banking business day, that is, a day in Sydney or Melbourne when banks can effect settlements through the Reserve Bank of Australia; and

(b) otherwise, on the next banking business day after you direct us to make it.

Note: BPAY® payment may take longer to be credited to a biller if you tell us to make it on a Saturday, Sunday or a public holiday or if another participant in BPAY® does

not process a BPAY® payment as soon as they receive its details.

20.7. Notwithstanding this, a delay may occur processing a BPAY® payment if:

(a) there is a public or bank holiday on the day after you instruct us to make the BPAY® payment;

(b) you tell us to make a BPAY® payment on a day which is not a banking business day or after the cut off time on a banking business day; or

(c) a biller, or another financial institution participating in BPAY®, does not comply with its BPAY® obligations.

20.8. If we are advised that your payment cannot be processed by a biller, we will:

(a) advise you of this;

(b) credit your account with the amount of the BPAY® payment; and

(c) take all reasonable steps to assist you in making the BPAY® payment as quickly as possible.

20.9. You must be careful to ensure you tell us the correct amount you wish to pay. If you make a BPAY® payment and later discover that:

(a) the amount you paid was greater than the amount you needed to pay you must contact the biller to obtain a refund of the excess; or

(b) the amount you paid was less than the amount you needed to pay you can make another BPAY® payment for the difference between the amount you actually paid and the amount you needed to pay.

20.10. If you are responsible for a mistaken BPAY® payment and we cannot recover the amount from the person who received it within 20 banking business days of us attempting to do so, you will be liable for that payment.

SECTION 21. FUTURE-DATED BPAY® PAYMENTS

Please note that this is an optional facility depending on whether we offer it.

You may arrange BPAY® payments up to 60 days in advance of the time for payment. If you use this option you should be aware of the following:

(a) you are responsible for maintaining, in the account to be drawn on, sufficient cleared funds to cover all future-dated BPAY® payments (and any other drawings) on the day(s) you have nominated for payment or, if the account is a credit facility, there must be sufficient available credit for that purpose;

(b) if there are insufficient cleared funds or, as relevant, insufficient available credit, the BPAY® payment will not be made and you may be charged a dishonour fee;

(c) you are responsible for checking your account transaction details or account statement to ensure the future-dated payment is made correctly;

(d) you should contact us if there are any problems with your future-dated payment;

(e) you must contact us if you wish to cancel a future-dated payment after you have given the direction but before the date for payment. You cannot stop the BPAY® payment on or after that date.

SECTION 22. CONSEQUENTIAL DAMAGE FOR BPAY® PAYMENTS

22.1. This clause does not apply to the extent that it is inconsistent with or contrary to any applicable law or code of practice to which we have subscribed. If those laws would make this clause illegal, void or unenforceable or impose an obligation or liability which is prohibited by those laws or that code, this clause is to be read as if it were varied to the extent necessary to comply with those laws or that code or, if necessary, omitted.

22.2. We are not liable for any consequential loss or damage you suffer as a result of using BPAY®, other than loss due to our negligence or in relation to any breach of a condition or warranty implied by the law of contracts for the supply of goods and services which may not be excluded, restricted or modified at all, or only to a limited extent.

SECTION 23. USING OSKO

23.1. You can use Osko® to make payments from those accounts that have the Osko facility to:

(a) make an Osko® payment;

(b) make scheduled and recurring Osko® payments;

(c) receive payment reminders;

(d) pay bills bearing the Osko® logo from those accounts that have the Osko® facility.

23.2. When you tell us to make an Osko® payment you must tell us the payee's PayID or the details of the payee's account, the amount to be paid and the account from which the amount is to be paid.

23.3. We cannot effect your Osko® instructions if you do not give us all the specified information or if you give us inaccurate information.

SECTION 24. PROCESSING OSKO® PAYMENTS

24.1. We will attempt to make sure that your Osko® payments are processed promptly by participants in Osko®, and you must tell us promptly if:

(a) you become aware of any delays or mistakes in processing your Osko® payment;

(b) you did not authorise an Osko® payment that has been made from your account; or

(c) you think that you have been fraudulently induced to make an Osko® payment.

24.2. An Osko® payment instruction is irrevocable.

24.3. Except for scheduled and recurring Osko® payments, you cannot stop an Osko® payment once you have instructed us to make it and we cannot reverse it.

24.4. We will treat your Osko® payment instruction as valid if, when you give it to us, you use the correct access method.

24.5. You should notify us immediately if you think that you have made a mistake (except for a mistake as to the amount you meant to pay).

24.6. If we are advised that your payment cannot be processed by a biller, we will:

(a) advise you of this;

(b) credit your account with the amount of the Osko® payment; and

(c) take all reasonable steps to assist you in making the Osko® payment as quickly as possible.

SECTION 25. SCHEDULED AND RECURRING OSKO® PAYMENTS

Please note that this is an optional facility depending on whether we offer it.

You may schedule Osko® payments up to 60 days in advance of the time for payment and you can also schedule recurring Osko® payments. If you use this option you should be aware of the following:

(a) you are responsible for maintaining, in the account to be drawn on, sufficient cleared funds to cover all scheduled and recurring Osko® payments (and any other drawings) on the day(s) you have nominated for payment or, if the account is a credit facility, there must be sufficient available credit for that purpose;

(b) if there are insufficient cleared funds or, as relevant, insufficient available credit, the Osko® payment will not be made and you may be charged a dishonour fee;

(c) you are responsible for checking your account transaction details or account statement to ensure that the scheduled or recurrent Osko® payment is made correctly;

(d) you should contact us if there are any problems with your scheduled or recurrent Osko® payments;

(e) you must contact us if you wish to cancel a scheduled or recurrent Osko® payment after you have given the direction but before the date for payment.

SECTION 26. REGULAR PAYMENT ARRANGEMENTS

26.1. You should maintain a record of any regular payment arrangement that you have entered into with a merchant.

26.2. To change or cancel any regular payment arrangement you should contact the merchant or us at least 15 days prior to the next scheduled payment. If possible you should retain a copy of this change/cancellation request.

26.3. Should your card details be changed (for example if your Visa Card was lost, stolen or expired and has been replaced) then you must request the merchant to change the details of your existing regular payment arrangement to ensure payments under that arrangement continue. If you fail to do so your regular payment arrangement may not be honoured, or the merchant may stop providing the goods and/or services.

26.4. Should your Visa Card or your accounts with us be closed for any reason, you should immediately contact the merchant to change or cancel your regular payment arrangement, as the merchant may stop providing the goods and/or services.

SECTION 27. AUTHORITY TO RECOVER MISTAKEN OR MISDIRECTED PAYMENTS

27.1 Where we and the sending financial institution determine that an Osko® or other NPP Payment made to your account is either a Mistaken Payment or a Misdirected Payment, we may, without your consent, and subject to complying with any other applicable terms and conditions, deduct from your account, an amount up to the original amount of the Mistaken Payment or Misdirected Payment. We will notify you if this occurs.

27.2 **Misdirected Payment** means an NPP Payment using a PayID, erroneously directed to an incorrect account because the financial institution that registered the PayID has not registered or maintained the correct information.

Mistaken Payment means an NPP Payment by a payer who is a 'user' as defined in the ePayments Code, erroneously directed to the wrong account as a result of the payer's error (for example, by inputting incorrect payee account details, either by accident or because the payee gave them the incorrect account details).

SECTION 28. CREATING A PAYTO PAYMENT AGREEMENT

28.1. PayTo allows you to establish and authorise Payment Agreements with merchants or Payment Initiators who offer PayTo as a payment option.

28.2. If you elect to establish a Payment Agreement with a merchant or Payment Initiator that offers PayTo payment services, you will be required to provide that merchant or Payment Initiator with your personal information including your BSB and account number, or your PayID. You are responsible for ensuring the information you provide to the merchant or Payment Initiator is correct. Any personal information or data you provide to the merchant or Payment Initiator will be subject to their own privacy policy and terms and conditions.

28.3. Payment Agreements must be recorded in the Mandate Management Service before NPP Payments can be processed in accordance with them. The merchant or Payment Initiator is responsible for creating and submitting a record of each Payment Agreement to their financial institution or payments processor for inclusion in the Mandate Management Service. The Mandate Management Service will notify us of the creation of any Payment Agreement established using your account or PayID details. We will notify you of the creation of a Payment Agreement, and provide details of the merchant or Payment Initiator, the payment amount and payment frequency (if these are provided) to seek your confirmation of the Payment Agreement. You may confirm or decline any Payment Agreement presented for your approval. If you confirm, we will record your confirmation against the record of the Payment Agreement in the Mandate Management Service and the Payment Agreement will then be effective. If you decline, we will note that against the record of the Payment Agreement in the Mandate Management Service.

28.4. We will only process payment instructions in connection with a Payment Agreement once you have confirmed the Payment Agreement and it is effective. Once the Payment Agreement is effective we will process payment instructions received from the merchant's or Payment Initiator's financial institution. We are not liable for any loss you or any other person may suffer as a result of our processing a payment instruction submitted under a Payment Agreement that you have confirmed.

Payment instructions may be submitted to us for processing immediately after you have confirmed the Payment Agreement so you must take care to ensure the details of the Payment Agreement are correct before you confirm them.

28.5. If a Payment Agreement requires your confirmation within a timeframe stipulated by the merchant or Payment Initiator, and you do not provide confirmation within that timeframe, the Payment Agreement may be withdrawn by the merchant or Payment Initiator.

28.6. If you believe the payment amount or frequency or other detail presented is incorrect, you may decline the Payment Agreement and contact the merchant or Payment Initiator and have them amend and resubmit the Payment Agreement creation request.

28.7. This Section 28 does not apply to Migrated DDR Mandates.

SECTION 29. AMENDING A PAYMENT AGREEMENT

29.1. Your Payment Agreement may be amended by the merchant or Payment Initiator from time to time, or by us on your instruction.

29.2. We will notify you of proposed amendments to a Payment Agreement requested by the merchant or Payment Initiator. Such amendments may include variation of the payment amount (if a fixed amount) or payment frequency. You may confirm or decline any amendment request presented for your approval. If you confirm, we will record the confirmation against the record of the Payment Agreement in the Mandate Management Service and the amendment will then be effective. If you decline, the amendment will not be made and the Payment Agreement will continue on existing terms.

29.3. If you do not confirm or decline an amendment request within 5 calendar days of it being sent to you, then the amendment request will be deemed to be declined.

29.4. If you decline the amendment request because it does not reflect the updated terms of the agreement that you have with the merchant or Payment Initiator, you may contact them and have them resubmit the amendment request with the correct details. We are not authorised to vary the details in an amendment request submitted by the merchant or Payment Initiator.

29.5. Once an amendment request has been confirmed by you, we will promptly update the Mandate Management Service with this information.

29.6. Once a Payment Agreement has been established, you may instruct us to amend your name or transfer the Payment Agreement to another account you hold with us. If you wish to transfer the Payment Agreement to an account with another financial institution, you may when available give us a transfer instruction (see Section 31 "*TRANSFERRING YOUR PAYMENT AGREEMENT*"). We may decline to act on your instruction to amend your Payment Agreement if we are not reasonably satisfied that your request is legitimate. You may not request us to amend the details of the merchant or Payment Initiator, or another party.

SECTION 30. PAUSING YOUR PAYMENT AGREEMENT

30.1. You may instruct us to pause and resume your Payment Agreement. We will act on your instruction to pause or resume your Payment Agreement promptly by updating the record of the Payment Agreement in the Mandate Management Service. The Mandate Management Service will notify the merchant's or Payment Initiator's financial institution or payment processor of the pause or resumption. While the Payment Agreement is paused, we will not process payment instructions in connection with it. We are not liable for any loss that you or any other person may suffer as a result of you pausing a Payment Agreement.

Before pausing a Payment Agreement you should ensure this will not breach, or result in a breach of, any contract you have with the merchant or Payment Initiator.

30.2. A merchant or Payment Initiator may pause and resume a Payment Agreement to which you are a party, in which case we will promptly notify you of that pause or subsequent resumption. We are not liable for any loss that you or any other person may suffer as a result of the pausing of a Payment Agreement by the merchant or Payment Initiator.

SECTION 31. TRANSFERRING YOUR PAYMENT AGREEMENT

31.1. When available, you may ask us to initiate the transfer of a Payment Agreement to an account at another financial institution. We will provide you with a Transfer ID to provide to your new financial institution to enable them to complete the transfer.

31.2. Your new financial institution will be responsible for obtaining your consent to transfer the Payment Agreement and for updating the Payment Agreement in the Mandate Management Service. The updated Payment Agreement will only become effective upon being updated in the Mandate Management Service.

31.3. Until the transfer is completed, the Payment Agreement will remain linked to your account with us and payments under the Payment Agreement will continue to be made from your account with us. If the other financial institution does not complete the transfer within 14 calendar days, the transfer will be deemed to be ineffective and payments under the Payment Agreement will continue to be made from your account with us.

31.4. When available to transfer a Payment Agreement that you have with another financial institution to us, you will need to obtain a Transfer ID from that institution and provide it to us. We will use reasonable endeavours to process the transfer within 14 calendar days. Not all Payment Agreements will be transferrable to us. If we are unable to complete a transfer, we will notify you and advise you of your options.

SECTION 32. CANCELLING YOUR PAYMENT AGREEMENT

32.1. You may instruct us to cancel a Payment Agreement on your behalf. We will act on your instruction promptly by updating the record of the Payment Agreement in the Mandate Management Service. The Mandate Management Service will notify the merchant's or Payment Initiator's financial institution or payment processor of the cancellation. We are not liable for any loss that you or any other person may suffer as a result of cancelling a Payment Agreement. You may remain liable to the merchant or Payment Initiator for payments that would otherwise have been paid under the Payment Agreement, including for any cancellation fees.

32.2. A merchant or Payment Initiator may cancel a Payment Agreement to which you are a party, in which case we will promptly notify you of that cancellation. We are not liable for any loss that you or any other person may suffer as a result of cancellation of your Payment Agreement by the merchant or Payment Initiator.

SECTION 33. MIGRATION OF DIRECT DEBIT ARRANGEMENTS

33.1. A merchant or Payment Initiator who has an existing direct debit arrangement with you, may migrate it to a Payment Agreement, as a Migrated DDR Mandate. We are not obliged to notify you of a Migrated DDR Mandate. We will process instructions received from a merchant or Payment Initiator on the basis of a Migrated DDR Mandate.

A Migrated DDR Mandate takes effect without your confirmation. If you do not consent to the migration of a direct debit arrangement you should contact the merchant or Payment Initiator.

33.2. A Migrated DDR Mandate has effect as a Payment Agreement. You may amend, pause (and resume), cancel or transfer your Migrated DDR Mandates, and will receive notice of amendment, pause or resumption, or cancellation initiated by the merchant or Payment Initiator of your Migrated DDR Mandates, in the same manner as for other Payment Agreements.

SECTION 34. GENERAL PAYTO PROVISIONS

34.1. A Payment Agreement can only be linked to an account that has the PayTo facility.

34.2. You must carefully consider any Payment Agreement creation request, or amendment request made in respect of a Payment Agreement, and promptly respond to such requests. We are not liable for any loss that you suffer as a result of any payment processed by us in accordance with the terms of a Payment Agreement.

34.3. You must notify us immediately if you no longer hold or have authority to operate the account from which a payment under a Payment Agreement has been or will be made.

34.4. You must promptly respond to any notification that you receive from us regarding the pausing or cancellation of a Payment Agreement for misuse, fraud or for any other reason. We are not responsible for any loss that you suffer as a result of you not promptly responding to such a notification.

34.5. You are responsible for complying with the terms of any agreement that you have with a merchant or Payment Initiator, including any termination notice periods. You are responsible for any loss that you suffer in connection with you cancelling or pausing a Payment Agreement, including for a breach of any agreement that you have with that merchant or Payment Initiator.

34.6. You are responsible for ensuring that you have sufficient funds in your account to meet the requirements of all your Payment Agreements. We are not responsible for any loss that you suffer as a result of your account having insufficient funds to meet a payment instruction under a Payment Agreement. See "*Overdrawing an account*" on page 5 for our rights if there are insufficient funds in your account.

34.7. If you receive a Payment Agreement creation request or become aware of payments being processed from your account that you are not expecting or experience any other activity that appears suspicious or erroneous, please report such activity to us immediately.

34.8. From time to time we may ask you to confirm that your Payment Agreements are accurate and up to date. You must promptly respond to any such request. Failure to respond may result in us pausing the Payment Agreements.

34.9. We recommend that you allow notifications from your mobile banking to your smartphone to ensure that you're able to receive and respond to Payment Agreement creation requests, amendment requests and other notifications in a timely way.

34.10. You are responsible for ensuring that:

(a) all data you provide to us or to any merchant or Payment Initiator that subscribes to PayTo is accurate and up to date;

(b) you do not use PayTo to send threatening, harassing or offensive messages to the merchant, Payment Initiator or any other person; and

(c) any passwords/PINs needed to access the facilities we provide are kept confidential and are not disclosed to any other person.

34.11. All intellectual property, including but not limited to the PayTo trade marks and all documentation, remains our property, or that of our licensors (Our Intellectual Property). We grant to you a royalty free, non-exclusive licence (or where applicable, sub-licence) for the term to use Our Intellectual Property for the sole purpose of using PayTo in a way that is consistent with these terms and conditions.

34.12. Where an intellectual property infringement claim is made against you, we will have no liability to you under this agreement to the extent that any intellectual property infringement claim is based upon:

(a) modifications to Our Intellectual Property by or on behalf of you in a manner that causes the infringement;

(b) use of any item in combination with any hardware, software or other products or services in a manner that causes the infringement and where such combination was not within the reasonable contemplation of the parties given the intended use of the item;

(c) your failure to use corrections or enhancements to Our Intellectual Property that are made available to you (except where the use of corrections or enhancements would have caused a defect in PayTo or would have had the effect of removing functionality or adversely affecting the performance of PayTo); and

(d) your failure to use Our Intellectual Property in accordance with this agreement.

34.13. We may cancel or suspend your use of PayTo in accordance with our rights under Section 18 "*CANCELLATION OF ACCESS CARD, INTERNET OR MOBILE BANKING SERVICE , BPAY®, OSKO® OR PAYTO*".

34.14. We may amend the terms and conditions relating to PayTo in accordance with our rights under "*Notifying changes*" on page 7. If you do not accept our amendments, you may cease using PayTo.

34.15. You must comply with all applicable laws in connection with your use of PayTo.

34.16. We will accurately reflect all information you provide to us in connection with a Payment Agreement in the Mandate Management Service.

34.17. We may monitor your Payment Agreements for misuse, fraud and security reasons. You acknowledge and consent to us pausing or cancelling all or some of your Payment Agreements if we reasonably suspect misuse, fraud or security issues. We will promptly notify you of any such action.

34.18. If you become aware of a payment being made from your account, that is not permitted under the terms of your Payment Agreement or that was not authorised by you, contact us immediately and submit a claim. We will promptly respond to all claims and if the claim is founded, we will refund your account. We are not liable to you for any payment made that was in fact authorised by the terms of your Payment Agreement.

34.19. We may impose daily, or other periodic, limits on the value of payments that can be made using PayTo These limits are set out in the *Fees & Charges and Transaction Limits* brochure. We may reject any payment instructions from a merchant or Payment Initiator that will cause you to exceed any such limit. We are not liable for any loss that you or any other person may suffer as a result of us rejecting a payment instruction under this clause.

34.20. If your Payment Agreement is linked to a PayID:

(a) transferring your PayID to another account (whether with us or another financial institution) will not automatically transfer the Payment Agreement to that account, and payments under the linked Payment Agreement will fail (subject to clause 34.21);

(b) closing your PayID will cause payments under the linked Payment Agreement to fail (subject to clause 34.21).

34.21. To ensure payments under a linked Payment Agreement continue after transferring or closing the PayID you will also need to either link the Payment Agreement to an account with us (see Section 29 "*AMENDING A PAYMENT AGREEMENT*") or when available transfer the Payment Agreement to another financial institution (see Section 31 "*TRANSFERRING YOUR PAYMENT AGREEMENT*").

SECTION 35. PRIVACY AND PAYTO

By confirming a Payment Agreement or permitting the creation of a Migrated DDR Mandate against your account with us, you acknowledge that you authorise us to collect, use and store your personal information and the details of your Payment Agreement or Migrated DDR Mandate in the Mandate Management Service, and that these details may be disclosed to the financial institution or payment processor for the merchant or Payment Initiator, for the purposes of creating payment instructions and constructing NPP Payment messages and enabling us to make payments from your account.

SECTION 36. AUTHORITY FOR PAYTO INSTRUCTIONS

Your instructions in relation to a Payment Agreement must be provided in accordance with the account operating instructions for the account that is, or is intended to be, linked to the Payment Agreement. This includes instructions to confirm or decline a Payment Agreement or the merchant's or Payment Initiator's amendments to a Payment Agreement, or to amend, pause, resume, cancel or transfer a Payment Agreement. For example, instructions to confirm a Payment Agreement linked to a joint account operated on an 'all to sign' basis must be provided by all the joint holders.

SECTION 37. DIGITAL WALLETS

When this section applies

37.1. This Section applies when you, or an additional card-holder, add an Eligible Card to a Digital Wallet on a Supported Device. This Section applies in addition to the terms and conditions that apply to the Account and Eligible Card.

Digital Wallet services

37.2. Each Digital Wallet is a service provided by the Digital Wallet provider, and not by us. The Digital Wallet provider is responsible for the functionality and operation of the Digital Wallet. We are not liable to you for any loss or damage you suffer as a result of any malfunction, failure or unavailability of a Digital Wallet, or the failure or refusal of any merchant to process payments using a Digital Wallet.

Your security obligations

37.3. You, and each additional card holder, must take reasonable steps to secure the Supported Device and any PIN or other passcode registered to the Supported Device in the same way as you would your Eligible Card and related passcode, in accordance with these Conditions of Use.

Device security

37.4 You, and each additional card holder, must:

(a) ensure that only your, or the additional card-holder's, biometric identifier (e.g. fingerprint) is registered on the Supported Device;

(b) not allow any other person's biometric identifier to remain, or be, registered on the Supported Device;

(c) not select a PIN or other passcode registered to the Supported Device that is easily guessed (e.g. your date of birth);

(d) not share any PIN or other passcode registered to the Supported Device with any person;

(e) not write or record the PIN or other passcode on the Supported Device, or on anything:

(i) carried with the Supported Device;

(ii) liable to loss or theft simultaneously with the Supported Device unless you, or the additional card-holder make a reasonable attempt to protect the security of the PIN or other passcode.

(f) not leave the Supported Device unattended, and lock it when not in use;

(g) before disposing of a Supported Device, remove or unlink the Eligible Card from it.

37.5. If you, or an additional card holder:

(a) allow another person's biometric identifier to remain, or be, registered on the Supported Device; or.

(b) share any PIN or other passcode registered to the Supported Device with any person, then you are taken to have authorised that person to carry out transactions using the Supported Device and you will be responsible for their use of the Eligible Card.

Lost or stolen devices or unauthorised use

37.6. You should immediately notify us if:

(a) a Supported Device is lost or stolen;

(b) you suspect that any PIN, passcode or other security credential registered to a Supported Device has become known to someone else;

(c) you suspect that someone else has used or could use a Supported Device to carry out a transaction on your Account without permission.

You may become liable for any unauthorised transactions if you unreasonably delay notifying us.

If your Supported Device is lost or stolen you should immediately remove or unlink your Eligible Card from the Digital Wallet where possible.

Privacy

37.7. We may share and exchange with the Digital Wallet provider and the relevant card scheme network (e.g. Visa or EFTPOS) personal information about you in relation to your set up and use of the Digital Wallet, to allow you to use the Eligible Card in the Digital Wallet.

Changes to this section

37.8. We may change this Section at any time and notify you of the changes in accordance with these Conditions of Use. You agree to us providing notification electronically.

Termination

37.9. We may suspend or terminate the use of an Eligible Card in a Digital Wallet without notice at any time, including if:

(a) you, or an additional card-holder, breach this Section;

(b) we reasonably suspect an unauthorised transaction has occurred or for other security reasons;

(c) we are required by a regulatory or government body.

Definitions

37.10. In this Section:

Account means your account with us to which an Eligible Card is linked.

Digital Wallet means any digital wallet service provided by a third party including without limitation Apple Pay as provided by Apple Inc. and Google Pay as provided by Google Inc.

Eligible Card means a debit or credit card issued by us that can be added to a Digital Wallet.

Supported Device means any device or equipment that can be used to access your Account using a Digital Wallet, and is not given by us e.g. mobile phone, smart watch.

Complaints

If you want to make a complaint, please speak to our staff:

- at any branch; or
- by calling 13 61 91.

You may also make a complaint:

- by emailing complaints@australianmutual.bank.

We will handle your complaint fairly and try to resolve it as soon as possible. If we cannot resolve the issue on the spot, we will do our best to complete our investigation and inform you of our decision within 21 days. We will let you know if we need more time.

For more information about our complaint handling process we have a guide to our dispute resolution system available on our website or on request.

Australian Financial Complaints Authority

If you are not satisfied with our response, or handling of your complaint, you may refer the matter to the Australian Financial Complaints Authority (AFCA). AFCA provides a free and independent external resolution service.

You can contact AFCA at:

Postal Address:	Australian Financial Complaints Authority Limited GPO Box 3 Melbourne VIC 3001;
Website:	www.afca.org.au;
Email:	info@afca.org.au;
Telephone:	1800 931 678.

Customer Owned Banking Code of Practice compliance

If you have a complaint about our compliance with the Customer Owned Banking Code of Practice, you can contact the Customer Owned Banking Code Compliance Committee. Please be aware that the Committee is not a dispute resolution body and cannot provide financial compensation.

You can contact the Committee at:

Postal Address:	Customer Owned Banking Code Compliance Committee PO Box 14240 Melbourne VIC 8001;
Website:	www.cobccc.org.au;
Email:	info@codecompliance.org.au;
Telephone:	1800 931 678.