Account & Access Facility

Australian Military Bank

Terms & Conditions of use

Effective 13 June 2023

The Australian Military Bank Account and Access Facility is issued by:
Australian Military Bank Limited ABN 48 087 649 741
Australian Financial Services Licence 237 988.

open to all who serve and support

How to Contact Us

Details

Mail: Australian Military Bank • PO Box H151 • Australia Square • NSW 1215

Phone: 1300 13 23 28 (Monday to Friday during business hours EST).
Email: service@australianmilitarybank.com.au
Website: australianmilitarybank.com.au

Or visit us at any of our branches, details of which can be found on our website.

Important Numbers

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

Visa Card Hotline

• **Australia wide toll free**: 1800 648 027 • **Sydney Metropolitan Area:** (02) 8299 9101

Codes of Practice

We warrant that we will comply with:

• the ePayments Code • the Customer Owned Banking Code of Practice

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.

Financial Claims Scheme:

Under the Financial Claims Scheme (FCS), deposits are protected up to $250,000 for each account holder per authorised deposit-taking institution (ADI) incorporated in Australia. Australian Military Bank is an ADI. For further information about the FCS visit the website: www.fcs.gov.au.

Contents

Contents

PART A - Account Keeping Conditions of Use

This document should be read in conjunction with our Schedule of Fees and Charges and our Interest Rate Schedule. Together they form the Terms and Conditions for our Account and Access Facility.

What is the account and access facility?

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

- Visa Debit Card
- chequing
- BPAY® (registered to BPay Pty Ltd ABN 69 079 137 518)
- Osko Payments
- internet and mobile banking
- EFTPOS and ATM access
- direct debit request
- PayTo.

Please refer to Part H - Summary of Accounts & Availability of Access Facilities 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 may need to become a member of Australian Military Bank before we can issue the Account and Access Facility to you. Membership involves acquiring a member share in Australian Military Bank. We may waive the requirement for membership in certain circumstances.

Proof of identity required

The law requires us to verify your identity when you open an account or the identity of any person you appoint as a signatory to your account. We may also ask you to verify your identity periodically while you hold a membership with us.

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

If you want to appoint a signatory to your account, the signatory will also have to provide proof of identity, as above.

What accounts can I open?

Please see Part H - Summary of Accounts & Availability of Access Facilities 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 an 'all to sign' or 'either/or to sign' basis:

- 'all to sign' means all joint holders must sign withdrawal forms, cheques, etc
- 'either/or to sign' means any one joint holder can sign withdrawal slips, cheques, etc.

All joint accounts will initially be set up as an 'either/or to sign' basis. However, any one joint account holder can instruct us to:

- cancel or suspend this arrangement, making it 'all to sign'
- suspend the account to allow the joint account holders time to reach agreement about dispersal of the account funds.

All joint account holders must consent to convert the operation of a joint account from 'all to sign' to 'either/or to sign.' We may also make a joint account 'all to sign' if we become aware of a dispute between account holders.

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 including for Self Managed Superannuation Funds (SMSF)

You can open an account as a trust account, including for a Self-Managed Super Fund (SMSF). 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.

You agree to indemnify us against any claim made upon us in relation to, or arising out, of that trust.

What fees and charges are there?

Please refer to the Schedule of Fees & Charges brochure for current fees and charges. We may vary fees or charges from time to time.

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

What interest can I earn on my account?

Our Interest Rates brochure 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.

Part H-Summary of Accounts & Availability of Access Facilities 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 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 exemptions, otherwise withholding tax applies to all interest earned on the joint account.

Businesses need only quote their ABN instead of a TFN.

Third party signatories

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

Subject to any contrary authority agreed by the account holder and the Bank, the third party signatory you authorise does NOT have authority to:

- change any of the signatory authorisations on the account
- give another third party access or authority to operate on the account
- redeem Fixed Term Deposits
- change contact details, including the mailing address for statements
- close an account.

You can specify which of your accounts under Australian Military Bank Account & Access Facility you give the authorised person authority to operate on.

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.

The third party's authority to operate on your account ceases:

- when you or your attorney tell us
- on your death.

Making deposits to the account

You can make deposits to the account:

- by cash or cheque at any branch
- 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 at selected ATMs, if your account is linked to an access card
- via Bank@Post at any participating Australia Post Offices

unless otherwise indicated in Part H - Summary of Accounts & Availability of Access Facilities.

Deposits using electronic equipment

We are responsible for a deposit into a facility received by our electronic equipment or a device, 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

You can only access the proceeds of a cheque when it has cleared, which can take up to 10 business days.

Withdrawing or transferring from the account

You can make withdrawals from the account:

- over the counter at any branch
- by direct debit
- by cheque, if your account is linked to a cheque book
- by internet and mobile banking
- by Osko payment
- by BPAY® to make a payment to a biller
- 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)

- Via Bank@Post at any participating Australia Post Office
- by PayTo

unless otherwise indicated in Part H - Summary of Accounts & Availability of Access Facilities.

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 and Blocking or Delaying Transactions. 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 our action.

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 or by buying a bank cheque. Please check:

- Part H - Summary of Accounts & Availability of Access Facilities for any restrictions on withdrawals applying to certain accounts
- the Schedule of Fees & Charges brochure for any applicable daily cash withdrawal limits or other transaction limits.

Withdrawals using our bank cheques

This is a cheque Australian Military Bank draws payable to the person you nominate. You can purchase a bank cheque from us for a fee: see the Schedule of Fees & Charges brochure.

If a bank cheque is lost or stolen, you can ask us to stop payment on it. You will need to complete a form of request, giving us evidence of the loss or theft of the cheque. You will also have to give us an indemnity – the indemnity protects us if someone else claims that you wrongfully authorised us to stop the cheque.

We cannot stop payment on our bank cheque if you used the cheque to buy goods or services and you are not happy with them. You must seek compensation or a refund directly from the provider of the goods or services. You should contact a Government Consumer Agency if you need help.

Transaction limits

We limit the amount of daily withdrawals or payments you may make using electronic methods, either generally or in relation to a particular facility.

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 also require you to apply for new transaction limits if you change any passcode. We will require you to provide proof of identity that satisfies us. We may reduce transaction limits to zero for security reasons.

You can find out current transaction limits for your accounts by visiting our website FAQs section or by calling 1300 13 23 28. We may, in our discretion, agree to vary a transaction limit on your request.

Overdrawing an account

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

Alternatively, we can honour the transaction and overdraw your account. We may charge you a fee for each day (or part of a day) your account is overdrawn: see the Schedule of Fees & Charges brochure.

Account statements

We will send you account statements quarterly. You can ask us for an account statement at any time. We may charge a fee for providing additional statements or copies: see the Schedule of Fees & Charges brochure.

We may offer 'digital only' accounts, with statements provided electronically via internet or mobile banking only: see Part H - Summary of Accounts & Availability of Access Facilities. 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
- 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 Schedule of Fees & Charges. 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 2 for our contact details.

What happens if I change my name or contact details?

You must let us know immediately if you change your name or contact details (including email address or mobile phone number), by telephoning us on 1300 13 23 28 or by visiting one of our branches.

Dormant accounts

If no transactions are carried out on your account for at least 24 months (other than transactions initiated by Australian Military 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, 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 member, 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 for Centrelink Direct Credit 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.

Closing accounts, cancelling access facilities and blocking or delaying transactions

You can close the Account and Access Facility at any time. However, you will have to surrender your cheque book and any access card at the time. We may defer closure and withhold sufficient funds to cover payment of outstanding cheque, 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 and paying you the balance of your account
- close or suspend the Account and Access Facility (including delaying or not processing transactions) without notice where it is reasonable, such as to protect you from potential harm or loss (eg scams) or comply with our legal and regulatory obligations (including our own policies)
- cancel any access facility for security reasons or if you breach these Conditions of Use.

Notifying changes

We may change fees, charges, interest rates and other conditions at any time. The following table sets out 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 to or debited from your account	20 days
Increasing your liability for losses relating to ePayments (see the ePayments Conditions of Use Section 3 on page 18 for a list of ePayments)	20 days
Imposing, removing or changing any periodic transactions limit	20 days
Changing any other term or condition	When we communicate with you next.

If there is a change or introduction of a government charge that you may directly or indirectly pay as part of your banking service, we will promptly notify you after we have been notified, unless the government has already publicized the introduction or change.

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

- notification by letter or other direct communication
- notification by electronic direct mail (eDM)
- 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 appropriate to the nature and extent of the change, as well as the cost effectiveness of the method of notification.

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 via our mobile banking app
- by advertisement in the media, for some notices only.

Statements and notices will usually be sent electronically unless you direct otherwise.

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. 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 Part H- Summary of Accounts & Availability of Access Facilities), 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 Schedule of Fees & Charges.

Anti money laundering/counter-terrorist financing and sanctions (AML/CTF)

To meet our legal and regulatory obligations, such as those under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, we may:

- Collect information about you
- Perform monitoring of accounts and access facilities
- Disclose information relating to you or your account to Australian and/or overseas government or regulator bodies (including Australian Transaction Reports and Analysis Centre) as required or authorised by law (in some instances these bodies may share it with relevant foreign authorities)
- Stop, prohibit, delay, block or freeze transactions
- Close your account or deal with it in a way required by AML/CTF laws
- Take other actions required by AML/CTF laws.

We are not liable for any loss or damage you, or any other person, may suffer in connection with us taking such action.

You must provide us with all information reasonably needed to comply with AML/CTF laws, sanctions, regulations, requests, directives and policies of Australian regulators as well as our policies associated with enforcing these laws.

PART B - Access Facilities

Chequing

Chequing allows you to make payments by cheque. We will issue you with a cheque book and we will debit your account for the value of cheques you draw. We will only issue you a cheque book when you request one.

If you have insufficient funds in your nominated account, we may instruct the Bank to dishonour your cheque. However, we have a discretion to allow the cheque to be paid and to overdraw your account for this purpose. If you overdraw your account, we will charge you interest and fees. Please refer to the section Overdrawing an Account on page 10.

We may not give you access to chequing if your banking history with Australian Military Bank is not satisfactory or if you are under 18 years of age.

Cheque security

A member cheque deposited at another bank will typically take up to ten business days to clear. We may dishonour a cheque where there are insufficient funds, the cheque is more than 15 months old ('stale'), the cheque is post-dated, the cheque has not been completed correctly or altered, or where a stop payment has been placed on the cheque.

To reduce the risk of your cheque being changed in unauthorised ways, we recommend never giving your cheque book or an uncompleted cheque to anyone. You should always write a cheque in both words and numbers, and never leave a gap between words or numbers.

To stop payment of a member cheque you have written, you must complete a form which is available by contacting us. You should complete this form and notify us as soon as possible, as this cannot be done if a cheque has already been presented. A fee will be charged for processing this.

If you cross out the words "or bearer" and replace with the words "or order", this will mean that the cheque will become an "order Cheque". If the payee also endorses the cheque on its back by naming the person for whom the funds are for and signing it, it will allow the cheque to be paid to another person.

Writing 'account payee only' on a cheque indicates to a financial institution that it should only be deposited in the name of the person to whom the cheque is made out to.

Writing 'Not negotiable' between two parallel lines on the face of a cheque may give the person to whom the cheque is made out to a right to claim funds against the person cashing the cheque, for example if it is stolen.

If you add two parallel lines to a cheque, this means the cheque may only be deposited directly into a bank account.

Direct debit

You can authorise a participating biller to debit amounts from your account, as and when you owe those amounts to the biller. 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 promptly stop the facility within one business day. We suggest that you also contact the biller, to prevent any potential fees that they may impose.

If you believe a direct debit initiated by a biller is wrong, you should contact the biller to resolve the issue. Alternatively, you may contact us. If you give us the information we require we will forward your claim to 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 2 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 please see Part G - PayTo Terms and Conditions of Use.

PART C - ePayments Conditions of Use & Associated Electronic Access Facilities

Section 1. Information about our 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

- Sign the access card as soon as you receive it.
- 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 to report unauthorised use of your access card, BPAY® or internet and mobile banking.
- Immediately report loss, theft or unauthorised use.
- 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 a device.
- Keep a record of the Visa card number and the Visa Card Hotline telephone number for your area with your usual list of emergency telephone 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 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
- Internet and Mobile Banking
- PayTo.

You can use any of these electronic access facilities to access an account, as listed in Part H - Summary of Accounts & Availability of Access Facilities.

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
- withdraw cash from your account
- transfer money between accounts
- deposit cash or cheques into your account (at select ATMs only).

We may choose not to give you a Visa Card if your banking history with Australian Military 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. 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.

Digital wallet

You may load your Visa Card on to your mobile phone in a digital wallet app. Use of the Visa Card details, via the digital wallet, is governed by these Conditions of Use. For specific terms, please see Part E - Digital Wallets Terms of Use.

Section 2. Definitions

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

b) AFCA means the Australian Financial Complaints Authority

c) ATM means automatic teller machine

d) business day means a day that is not a Saturday, a Sunday or a public holiday or bank holiday in the place concerned

e) 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 subscriber that generates a passcode

   iv) contactless devices

f) EFTPOS means electronic funds transfer at the point of sale—a network for facilitating transactions at point of sale

g) facility means an arrangement through which you can perform transactions

h) identifier means information that a user:

   i) may know but is not required to keep secret, and

   ii) must provide to perform a transaction

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

i) manual signature means a handwritten signature, including a signature written on paper and a signature written on an electronic tablet

j) 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) mobile banking passcode

   iv) secret question

   v) code generated by a physical security token

   vi) 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.

k) 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

l) 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 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

m) transaction means a transaction to which these ePayment Conditions of Use apply, as set out in Section 3

n) 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

o) 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) person you authorise us to issue an additional card to.

p) we, us or our means Australian Military Bank Limited

q) you means the person or persons in whose name this Account & 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) incurred 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

c) 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 password 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, includes retailers, merchants, third party payment initiators, communications services providers and other organisations offering facilities, merchant acquirers and subscribers, 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 any other 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 member 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:

a) acknowledge the request for the return of funds, and

b) 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, refer to Part D Complaints and Feedback for AFCA's contact details.

Note: If we are unable to return funds to you because the unintended recipient of a mistaken internet payment does not cooperate, you can complain to our external dispute resolution scheme provider.

9.9. If you receive a payment to your account that is a mistaken internet payment, we have the right to transfer these funds from your account to the extent required by the ePayments Code. 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 section 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.

1. Process where sufficient funds are available and 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.

2. Process where sufficient funds are available and 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:
  - prevent the unintended recipient from withdrawing the funds for 10 further business days, and
  - 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.

3. 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:
  - the receiving ADI must return the funds to the sending ADI, and
  - the sending ADI must return the funds to the holder as soon as practicable.

4. 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.

Section 10. Using internet and mobile banking

10.1. We do not warrant that:

a) the information available to you about your accounts through our internet and mobile banking service is always up to date

b) you will have 24 hours a day, 7 days per week, access to internet and mobile banking

c) data you transmit via internet and mobile banking is totally secure.

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 2 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 an organisation displaying the Visa sign and also then confirm the loss, theft or misuse of the card:

a) with us by telephone or priority paid mail as soon as possible, or

b) by telephoning the Visa Card Hotline number for the country you are in.

VISA CARD HOTLINE

- Australia wide toll free
  1800 648 027
- Sydney Metropolitan Area
  (02) 9959 7480

Section 12. How to report unauthorised use of internet and mobile banking

12.1. If you believe that your passcode for internet/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 2 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 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 access card

b) what ATMs of other financial institutions may be used

c) what the daily cash withdrawal limits are.

Please refer to our website 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. Using Visa outside Australia

14.1. All transactions made in a foreign currency on the Visa Card will be converted into Australian currency by Visa Worldwide, and calculated at a wholesale market rate selected by Visa from within a range of wholesale rates or the government mandated rate that is in effect one day prior to the Central Processing Date (that is, the date on which Visa processes the transaction).

14.2. All transactions made in a foreign currency on the Visa Card are subject to a conversion fee. Please refer to the Schedule of Fees & Charges brochure for the current conversion fee.

14.3. 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.

14.4. Some overseas merchants and electronic terminals allow the cardholder the option to convert the value of the Transaction into Australian dollars at the point of sale, also known as Dynamic Currency Conversion. Once you have confirmed the transaction you will not be able to dispute the exchange rate applied.

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 instruct us by telephone, in person at or in writing (including electronically).

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 the 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 or of access to internet banking service, BPAY®, Osko, or PayTo

18.1. You may cancel your access card, your access to internet and mobile banking, BPAY® or Osko at any time by giving us written notice.

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

a) for security reasons

b) if you breach these Conditions of Use

c) you, or someone acting on your behalf, is being fraudulent

d) we 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 members

e) if we cease to be a participant in Osko

f) for any other reason set out in Part A section Closing Accounts, Cancelling Access Facilities and Blocking or Delaying Transactions

g) in the case of an access card, we may cancel the access card by capture of the access card at any ATM.

18.3. We may cancel your access card or your access to internet and 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 an 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 and 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 and 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 and 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 and 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 (eg. 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.

Please note that, 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

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).

Please note that 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

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

c) please note that the 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

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

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

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

a) make payments from those accounts that have the Osko facility

b) make an Osko payment

c) make scheduled and recurring Osko payments

d) receive payment reminders

e) 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 affect 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

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

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

Where we and the sending financial institution determine that an NPP Payment made to your Account is either a Mistaken Internet Payment (as defined in Section 9) or a Misdirected Payment (where a payment made using a PayID is erroneously directed to an incorrect account because the financial institution that registered the PayID has not registered or maintained the correct information) , 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.

PART D - Complaints and Feedback

If you have a complaint or would like to provide us with any feedback, we would like to hear from you. We have an internal dispute resolution system to deal with any complaints you may have, and we ensure that we deal with any complaint sympathetically and efficiently.

If you want to make a complaint, you can contact our staff:

- Email: complaints@australianmilitarybank.com.au
- Telephone: 1300 13 23 28 from Australia or +61 2 9240 4122 from overseas (8am to 6pm, Monday to Friday, Sydney time)
- In person: at any one of our branches
- In writing: Member Resolution Team at Australian Military Bank; Reply Paid 151 Australia Square NSW 1214.

Our staff will advise you about our complaint handling process and the timeframe for handling your complaint. We have an easy to read guide about our dispute resolution system available to you on request.

If you are not satisfied with the way in which we resolved your complaint, you may refer the complaint to the Australian Financial Complaints Authority (AFCA) using the below details:

- Mail: GPO Box 3 Melbourne VIC 3001
- Toll-free number: 1800 931 678
- Email: info@afca.org.au
- Website: www.afca.org.au

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

PART E - Digital Wallets Terms of Use

These terms apply to the use by you of a card in a Digital Wallet. By registering a card in a Digital Wallet you agree to these terms.

Account or cardholder terms and conditions

- The Terms and Conditions of your card, account and device apply to any use by you of your card in a Digital Wallet.
- To the extent of any discrepancy, the Terms and Conditions of the card/account take precedence over these terms.
- You may also have additional terms issued by your Digital Wallet Provider or your telecommunications service provider which you are required to comply with.

Your responsibilities to keep your card secure and notify us of errors or fraud

- You agree to protect and keep confidential your phone lock passcode, passwords, and all other information required for you to make purchases with your card using the Wallet.
- Always protect your passcode by using a unique number or pattern that is not obvious or can be easily guessed. Take precautions when using your Digital Wallet. Try to memorise your passcode or carefully disguise it. Never keep a record of your passcode with your device, on your device or computer, or tell anyone your passcode.
- If your device has been lost or stolen, or you believe your security credentials have been compromised, you must report this to us immediately. Your existing Terms and Conditions for your device require you to contact us immediately if you believe there are errors or if you suspect fraud with your card/account. This includes any fraud associated with a Digital Wallet.
- We will not be liable for any losses you incur except as specifically described in the Account Agreement or as otherwise provided by law.

Notably, if you let another person be registered on your mobile device, or you share your Protected Information with any other person, you will deemed to have authorised that person to transaction on your account using the Digital Wallet. This means that any transaction conducted using the Digital Wallet initiated by that person using the Protected Information will be authorised by you and the card terms and conditions which deal with unauthorised transactions will not apply.

Generally, subject to protections afforded to you by law, you are liable for unauthorised transaction conducted using the Digital Wallet.

Using a wallet

- Registration of the card into a Digital Wallet is subject to us identifying and verifying you, and is at the discretion of Australian Military Bank.
- Australian Military Bank does not make any guarantees that the Digital Wallet will be accepted at all merchants.
- Australian Military Bank is not the provider of the Digital Wallet and is not responsible for its use and function. You should contact the Digital Wallet Provider's customer service if you have questions concerning how to use the Digital Wallet or problems with the Digital Wallet.

- We are not liable for any loss, injury or inconvenience you suffer as a result of a merchant refusing to accept the Digital Wallet.
- We are not responsible if there is a security breach affecting any information stored in the Digital Wallet or sent from the Digital Wallet. This is the responsibility of the Digital Wallet provider.

Australian Military Bank will not be liable for any loss arising from your use of the Digital Wallet to the extent that the loss was caused by:

- your fraud
- your use of the Digital Wallet in a manner that is inconsistent or not permitted by the issuer of the Digital Wallet, or
- subject to the requirements at law, limited service caused by matters beyond our reasonable control.

Applicable fees

The card's terms and conditions describe the fees and charges which apply to your card. We do not charge any additional fees for adding or using a card in the Digital Wallet. You are responsible for any charges that you may incur from your telecommunications provider.

Suspension or removal of a card from a digital wallet by us

- We can block you from adding an otherwise eligible card to the Digital Wallet, suspend your ability to use a card to make purchases using the Digital Wallet, or cancel entirely your ability to continue to use a card in the Digital Wallet. We may take these actions at any time and for any reason, such as if we suspect fraud with your card, if you have an overdue or negative balance on your card account, if applicable laws change or if directed to do so by the Digital Wallet Provider or the applicable card scheme,
- We may also cease supporting the use of cards in Digital Wallets at any time, if you are in default of your card terms and conditions, for any other reason.

Suspension or removal of a card from a digital wallet by you

- You may remove a card from the Digital Wallet by following the Digital Wallet Provider's procedures for removal.

Devices with same digital wallet provider account

- If you add a card to one of your devices and have other devices sharing the same account ("other devices"), this may permit the card to be added to the other devices and permit users of the other devices to see card information. Please contact your Digital Wallet provider for more information.

Your information

- You agree that we may exchange information about you with the Digital Wallet Provider and the applicable card scheme (such as Visa) to facilitate any purchase you initiate using a card registered in a Digital Wallet.
- By registering your card in a Digital Wallet, you are providing consent for your information to be shared with these parties.
- We may also share your information to make available to you in the Digital Wallet information about your card transactions, or to assist the Digital Wallet Provider in improving the Digital Wallet. We are not responsible for any loss, injury or other harm you suffer in connection with the Digital Wallet Provider's use of your information.

We may collect information relating to your device for the following reasons (but not limited to):

- to ensure that your card properly functions in the Digital Wallet
- for security purposes and to identify fraud
- for us to better provide assistance to you
- to tell you about other Australian Military Bank products and services that may be of interest to you.

We may exchange information with the Digital Wallet provider (e.g. Apple Pay, Google Pay™, etc.) and related service providers (e.g. Cuscal, Visa, etc.):

- to facilitate any purchase you initiate using a card registered in the Digital Wallet
- to enable activation of your new card or ordered replacement card in the Digital Wallet
- to improve the functionality of the Digital Wallet
- in relation to persons involved in suspected security breaches or fraud.

Australian Military Bank is not responsible for any loss, injury or other harm you suffer in connection with the use of this personal information by the Digital Wallet provider or any related service provider.

If you do not want us to collect or disclose this information as described, you should not register a card for use with the Digital Wallet. If you do not want to receive marketing information, please contact us to opt out.

Australian Military Bank's Privacy Policy provides further details regarding the collection and handling of your information.

Biometric information

You may elect to enable biometric authentication to access the Digital Wallet using a biometric identifier registered on your device. A biometric identifier may include facial data, a finger print, or other means through which the manufacturer of the device enables a user to authenticate their identify in order to unlock their device. Biometric identifiers are stored on the user's device, Australian Military Bank does not store or collect biometric information.

You must ensure that your biometric identifier is the only biometric identifier stored on your device. If another person has stored their biometric identifier on the device you use to access your Digital Wallet in breach of these Terms and Conditions, then you acknowledge:

- they will be able to access your Digital Wallet and conduct certain transactions using your Digital Wallet
- these transactions will be treated as having been authorised by you and conducted with your consent and knowledge for the purposes of the Digital Wallet Terms of Use.

We may amend these terms at any time

We may amend these Digital Wallets Terms of Use at any time and notify you of the changes in accordance with our rights under Part A section Notifying Changes.

To participate in the EFTPOS and Visa Secure programmes, you may be asked to verify personal details held by us in order to complete the transaction. Should your EFTPOS or Visa card have been compromised in any way, please notify us immediately as you may be liable for unauthorised transactions.

PART F - EFTPOS Secure and Visa Secure Terms and Conditions of Use

1. Accepting these Conditions of Use

a) By completing or attempting to complete an EFTPOS Secure or Visa Secure transaction, you are deemed to accept these Conditions of Use.

b) You agree to be bound by these Conditions of Use each time you use EFTPOS Secure or Visa Secure.

2. Definitions

In these Conditions of Use:

a) account means your EFTPOS or Visa card account

b) account holder means the person or persons in whose name the account is held

c) additional cardholder means a person other than the account holder who has been nominated by an account holder to operate the account by use of an EFTPOS or Visa card

d) Conditions of Use means these EFTPOS Secure and Visa Secure Terms and Conditions of Use

e) EFTPOS Secure and Visa Secure and EFTPOS and Visa Secure means the online transaction authentication service provided by us (or our nominated service provider)

f) EFTPOS or Visa card means the EFTPOS or Visa debit or credit card issued to you or an additional cardholder by us

g) One Time Password means a single instance authentication method used to authenticate an online merchant payment made by an account through the provision of a unique code that is sent by either Cuscal, or a third-party provider engaged by Cuscal to that account holder by SMS

h) participating online merchant means a retailer or merchant who offers goods or services for sale online, who is a participant in EFTPOS or Visa Secure

i) we, us or our means Australian Military Bank Limited

j) you, your or yours means an account holder (or an additional cardholder), as relevant, who makes an online transaction using EFTPOS or Visa Secure.

3. Application of conditions of use

These Terms and Conditions of Use apply to the EFTPOS and Visa Secure service and the EFTPOS and Visa Secure transactions conducted on your account. In addition to these Terms and Conditions of Use, all other terms and conditions that apply to your EFTPOS or Visa card and account ("Account Terms") still apply. If there is any inconsistency between these Conditions of Use and your Account Terms, your Account Terms will apply to the extent of the inconsistency.

4. Guidelines for maintaining the security of your EFTPOS or Visa card

a) Never lend your EFTPOS or Visa card to anybody

b) Use care to prevent anyone seeing the EFTPOS or Visa card details being entered at the time of authentication

c) Immediately report unauthorised use of the EFTPOS or Visa card to us

d) You should examine periodical statements of your account immediately upon receiving them to identify and report, as soon as possible, any instances where the EFTPOS or Visa card has been used without your authority.

5. Using EFTPOS Secure or Visa Secure

a) You may use EFTPOS and Visa Secure to make purchases online. However, the EFTPOS and Visa Secure Service may only be available in connection with participating online merchants

b) When making an online purchase or other transaction for which EFTPOS and Visa Secure applies, you may be asked to provide certain information to us that allows us to validate your identity and verify that you are the cardholder of the specified EFTPOS or Visa card, such information includes, but is not limited to, a One Time Password. The information that you provide may be validated against information we hold about you and may be validated against information held by third parties

c) If you are unable to provide the requested information to validate your identity, or if the information you provide is inaccurate or incomplete, or if the authentication process otherwise fails, the merchant may not accept your EFTPOS or Visa card or payment for that transaction, and you may be unable to complete an online transaction using your EFTPOS or Visa card

d) In order to use EFTPOS and Visa Secure, you must have the equipment and software necessary to make a connection to the Internet

e) In the event you have a question regarding the authentication process or a transaction using your EFTPOS or Visa card, you should contact us.

6. Additional cardholders

a) Additional cardholders may use the EFTPOS and Visa Secure service but may be required to confirm their identity.

7. Privacy

a) We (or our nominated service provider) may collect personal information about you for the purposes of providing the EFTPOS and Visa Secure service to you

b) You authorise us to disclose personal information to others in order to execute your instructions including, but not limited to, conducting the EFTPOS and Visa Secure services and investigating disputes or allegations of unauthorised transactions, or if it is required by law

c) For more details of how your personal information is handled, please refer to our privacy policy, which can be viewed by accessing our Internet home site or you can obtain a copy by calling us.

8. Termination of EFTPOS Secure or Visa Secure

a) We may discontinue, terminate or suspend (permanently or temporarily) either or both of the EFTPOS Secure or Visa Secure services, or any part of the EFTPOS and Visa Secure services, without giving you prior notice. We may also change any aspect or functionality of the EFTPOS and Visa Secure services at any time without giving you prior notice.

9. Participating online merchant

a) You will know that an online merchant is a participating online merchant because you will see the EFTPOS Secure or Visa Secure logo and you may be asked to verify your identity before completing an online transaction with that merchant

b) We do not endorse or recommend in any way any participating online merchant

c) Your correspondence or business dealings with, or participation in promotions of, online stores through EFTPOS and Visa Secure, including payment for and delivery of related goods or services not purchased via EFTPOS Secure or Visa Secure, and any other terms, conditions, warranties or representations associated with such dealings, are solely between you and the online store. Except as otherwise required by law, we have no responsibility or liability whatsoever arising out of or related to those dealings or the online store's goods, services, acts or omissions.

10. Exclusion of liabilities

a) Subject to any warranty which is imported into these Conditions of Use by law, and which cannot be excluded, the EFTPOS and Visa Secure services are provided by us "as is" without warranty of any kind, either express or implied, including, but not limited to, any implied warranties of merchantability, fitness for a particular purpose, title or non-infringement

b) We will not be liable for any damages whatsoever arising out of or in relation to:

(i) your use of or access to (or inability to use or access) the EFTPOS and Visa Secure services, or

(ii) any other failure of performance, error, omission, interruption or defect, or any loss or delay in transmission or a transaction

c) If you are dissatisfied with any aspect of the EFTPOS Secure or Visa Secure service, your sole and exclusive remedy is to terminate participation in the EFTPOS Secure or Visa Secure transaction or service, as provided in these Terms and Conditions of Use.

11. Your conduct

a. Whilst using the EFTPOS and Visa Secure services and our Internet banking services, you agree not to:

i. impersonate any person or entity using the EFTPOS Secure or Visa Secure authentication processes

ii. upload, post, email or otherwise transmit any material that contains software viruses or any other computer code, files or programs designed to interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment used by the EFTPOS Secure or Visa Secure services or by us

iii. spam or flood our Internet banking service and the EFTPOS Secure or Visa Secure services

iv. modify, adapt, sub-license, translate, sell, reverse engineer, decompile or disassemble any portion of the EFTPOS Secure or Visa Secure services

v. remove any copyright, trademark, or other proprietary rights notices contained in the EFTPOS Secure or Visa Secure services

vi. "frame" or "mirror" any part of the EFTPOS Secure or Visa Secure services without our prior written authorisation

vii. use any robot, spider, site search/retrieval application, or other manual or automatic device or process to retrieve, index, "data mine," or in any way reproduce or circumvent the navigational structure or presentation of the EFTPOS Secure or Visa Secure services

viii. otherwise interfere with, or disrupt the EFTPOS Secure service or our Internet banking services or servers or networks connected to us or the EFTPOS Secure or Visa Secure services or violate these Conditions of Use or any requirements, procedures, policies or regulations in relation to the EFTPOS Secure or Visa Secure services

ix. intentionally or unintentionally violate any applicable local, state, national or international laws or regulations relevant or applicable to the EFTPOS and Visa Secure services.

12. Your liability

a) Your liability for unauthorised transactions is governed by your Account Terms.

b) If you breach these Terms and Conditions of Use, this may affect your liability for unauthorised transactions. If it is determined that you have contributed to the loss, you may be held liable for the transactions notwithstanding that they are unauthorised.

c) If you suspect that your EFTPOS or Visa card details have become known to someone else or there is a security concern, you must immediately notify us of such security concern. If you delay in notifying us of the security concern after you knew or ought to have known of the security concern, you may be in breach of these Conditions of Use and you may be liable for all transactions on the EFTPOS or Visa card until notification occurs.

d) For further details as to reporting a breach of card details, refer to your Account Terms.

13. Errors

If you believe an EFTPOS Secure or Visa Secure transaction is wrong or unauthorised or a periodical statement contains any instances of unauthorised use or errors, you should contact us immediately.

14. Changes to conditions of use

We can change these Conditions of Use at any time in accordance with our rights under Part A section Notifying Changes.

PART G - PayTo Terms and Conditions of Use

1. Definitions

In these Conditions of Use:

a) account means your account with us

b) direct debit has the meaning given to the term Direct Debit Request in the BECS Procedures available at https://www.auspaynet.com.au/resources/direct-entry

c) mandate management service means the central, secure database operated by NPP Australia Limited of Payment Agreements

d) migrated DDR mandates has the meaning given in section 7(a)

e) merchant means a merchant with which you have established, or would like to establish, a Payment Agreement

f) NPP means the New Payments Platform operated by NPP Australia Limited

g) NPP payments means electronic payments cleared and settled by participating financial institutions via the NPP

h) our intellectual property has the meaning given in section 8(j)

i) 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

j) 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

k) 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

l) transfer has the meaning given in section 5(a)

m) 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

n) we, us and our means Australian Military Bank Limited

o) you and your means the Account holder whether that be an individual, a group of 2 or more individuals.

2. Creating a payment agreement

a) PayTo allows payers to establish and authorise Payment Agreements with Merchants or Payment Initiators who offer PayTo as a payment option

b) 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 the Merchant or Payment Initiator with your personal information including your BSB and account number, or your PayID. You are responsible for ensuring the correctness of the information you provide for the purpose of establishing a Payment Agreement. Any personal information or data you provide to the Merchant or Payment Initiator will be subject to the privacy policy and terms and conditions of the relevant Merchant or Payment Initiator

c) Payment Agreements must be recorded in the Mandate Management Service in order for NPP Payments to 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 the Payment Agreement, and provide details of the Merchant or Payment Initiator named in the Payment Agreement, 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 deemed to be effective. If you decline, we will note that against the record of the Payment Agreement in the Mandate Management Service

d) We will only process payment instructions in connection with a Payment Agreement when you have confirmed the associated Payment Agreement and it is effective. We will process payment instructions received from the Merchant's or Payment Initiator's financial institution when the Payment Agreement is effective. We will not be liable to you or any other person for loss suffered as a result of 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

e) 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

f) If you believe the payment amount or frequency or other detail presented is in 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.

3. Amending a payment agreement

a) Your Payment Agreement may be amended by the Merchant or Payment Initiator from time to time, or by us on your instruction

b) We will notify you of proposed amendments to the payment terms of the 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. The Mandate Management Service will notify us of the amendment request and we will notify you of the proposed amendment. 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 they Payment Agreement will continue on existing terms

c) Amendment requests which are not confirmed or declined within 5 calendar days of being sent to you, will expire. If you do not authorise or decline the amendment request within this period of time, the amendment request will be deemed to be declined

d) 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

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

f) Once a Payment Agreement has been established, you may instruct us to amend your name or Account details in the Payment Agreement only. Account details may only be replaced with the BSB and account number of an account you hold with us. If you wish to amend the Account details to refer to an account with another financial institution, you may give us a transfer instruction (see section 6. 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.

4. Pausing your payment agreement

a) 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 will not be liable for any loss that you or any other person may suffer as a result of the pausing of a Payment Agreement that is in breach of the terms of an agreement between you and the relevant Merchant or Payment Initiator

b) Merchants and Payment Initiators may pause and resume their Payment Agreements. If the Merchant or Payment Initiator pauses a Payment Agreement to which you are a party, we will promptly notify you of that, and of any subsequent resumption. We will not be 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.

5. Transferring your payment agreement

a) 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

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

c) 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

d) 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 transfer requests within 14 days, however not that all Payment Agreements will be Transferrable to us and we will notify you if a transfer is not possible.

6. Cancelling your payment agreement

a) 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 you 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

b) Merchants and Payment Initiators may cancel Payment Agreements. We will notify you promptly if they do so. We will not be liable to you or any other person for loss incurred as a result of cancellation of your Payment Agreement by the Merchant or Payment Initiator.

7. Migration of direct debit arrangements

a) A Merchants and Payment Initiators who has an existing Direct Debit arrangements with you, may migrate it to a Payment Agreements, as a Migrated DDR Mandates. We are not obliged to provide notice of a Migrated DDR Mandate to you for you to confirm or decline. We will process instructions received from a Merchant or Payment Initiator on the basis of a Migrated DDR Mandate

b) A Migrated DDR has the effect of 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, in the same manner as for other Payment Agreements.

8. General PayTo provisions

a) A Payment Agreement can only be linked to an account that has the PayTo Facility

b) You must ensure that you carefully consider any Payment Agreement creation request, or amendment request made in respect of your Payment Agreement or Migrated DDR Mandates and promptly respond to such requests. We will not be 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 or Migrated DDR Mandate

b) You must notify us immediately if you no longer hold or have authority to operate the Account from which a payments under a Payment Agreement or Migrated DDR Mandate have been/will be made

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

d) You are responsible for ensuring that you comply 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 the cancellation or pausing of a Payment Agreement or Migrated DDR Mandate, including for a breach of any agreement that you have with that Merchant or Payment Initiator. Any disputed payments should be referred to your Merchant or Payment Initiator in the first instance

e) You are responsible for ensuring that you have sufficient funds in your Account to meet the requirements of all your Payment Agreements and Migrated DDR Mandates. We are not responsible for any loss that you suffer as a result of your account having insufficient funds under a Payment Agreement. See section Overdrawing an Account on page 10. Fees may be payable to third parties in accordance with their terms and conditions

f) 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

g) From time to time we may ask you to confirm that all of your Payment Agreements and Migrated DDR Mandates are accurate and up to date. You must promptly respond to any such notification. Failure to respond may result in us pausing the Payment Agreement/s or Migrated DDR Mandate/s

h) We recommend that you allow notifications from Australian Military Bank on 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

i) When using our services, you must ensure that:

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

(ii) you do not use PayTo to send threatening, harassing or offensive messages to the Merchant, Payment Initiator or any other person

(iii) you keep all passwords and PINs are kept confidential and are not disclosed to any other person.

j) 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 license (or where applicable, sub-license) for the Term to use Our Intellectual Property for the sole purpose of using PayTo in a way that is consistent with the terms of this agreement

k) 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:

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

(ii) 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

(iii) 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)

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

l) We may cancel or suspend your use of PayTo at any time and at our absolute discretion. See Part A section Closing Accounts, Cancelling Access Facilities and Blocking or Delaying Transactions.

m) We may amend the terms and conditions relating to PayTo at any time by providing you with reasonable notice of any change. See Part A section Notifying Changes. If you do not accept our amendments, you may cease using PayTo

n) You must comply with all applicable laws in connection with your use of PayTo

o) We will accurately reflect all information you provide to us in connection with a Payment Agreement or a Migrated DDR Mandate in the Mandate Management Service

p) We may monitor your Payment Agreements or Migrated DDR Mandates for misuse, fraud and security reasons. You acknowledge and consent to us pausing or cancelling all or some of your Payment Agreement or Migrated DDR Mandates if we reasonably suspect misuse, fraud or security issues. We will promptly notify you by of any such action to pause or cancel your Payment Agreement

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

r) 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 Agreements 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 by all to sign must be provided by all signatories

s) We may impose limits on the value of payments that can be made using PayTo. 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

t) If your Payment Agreement is linked to a PayID:

- transferring your PayID to another financial institution/account (whether with us or another financial institution) will not automatically transfer the Payment Agreement to that financial institution/account, and payments under the linked Payment Agreement will fail (subject to paragraph (u)
- closing your PayID will cause payments under the linked Payment Agreement to fail (subject to paragraph(u).

u) To ensure payments under a linked Payment Agreement continue after transferring or closing the PayID you will need to either:

- link the Payment Agreement to an account with us. See section 3 Amending a Payment Agreement
- transfer the Payment Agreement to another financial institution. See section 5 Transferring your Payment Agreement.

9. Privacy

a) By confirming a Payment Agreement and/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/s and Migrated DDR Mandates 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.

PART H - Summary of Accounts & Availability of Access Facilities

	Everyday Accounts					Savings Accounts				
	Access Account	Pension Account	Mess Account	Recruit Salary Saver	Military Rewards	Junior Saver	Christmas Club	DIY Super Saver	Star Saver Direct	Online Saver[11]
Account Eligibility	Personal Members	Members 55 years or older & receiving Government Pension	Defence related clubs, canteens & messes	Persons between the age of 12 – 30 (inclusive)[11]	Personal Members, over 18 & Australian citizens & see Note 3	Persons under 18 – see note 9	Personal Members	Trustees of self-managed superannuation funds (SMSF)	All Members	Personal Members
Minimum opening balance	$1	$1 Pension deposit by direct credit only - see Note 2	$1	$1	$1 $2,000 per month for no monthly service fee	$1	$1	$1	$1	$1
Maximum balance	x	x	x	x	x	x	x	x	$500,000	$500,000
Funds available at call	✓	✓	✓	✓	✓ & see Note 4	✓	✓ & see Note 5	✓	✓ & see Note 6	✓ & see Note 6
Statements, posted or available electronically (Note 10)	Either	Either	Either	Either	Electronic	Either	Either	Either	Either	Either
Visa Card	✓	✓	Unlimited cardholders	✓	✓	✓	x	x	x	x
Internet/Mobile Banking	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Member Cheques	✓	✓	✓	x	x	x	x	x	x	x
Direct Entry Credits	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Direct Entry Debits	✓	✓	✓	✓	✓	x	x	✓	x	x
Periodical Payments	✓	✓	✓	✓	✓	✓	x	✓	✓	✓
Pay anyone	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
BPAY®	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
Pay To	✓	✓	✓	✓	✓	✓	✓	✓	✓	x
Interest see Note 1	Type A	Type C	Type A	Type E	Type E	Type B	Type D	Type E	Type C	Type E

PART H - Summary of Accounts & Availability of Access Facilities

	Term Deposits		
	Investment Plus	**Income Plus**	**Teen Plus**
Account Eligibility	Members	Members	Members with Junior Saver accounts
Minimum opening balance	$1,000	$1,000	$500
Maximum balance	At Bank's discretion	At Bank's discretion	At Bank's discretion
Funds available at call	At maturity - see Note 7	At maturity - see Note 7	At maturity - see Note 7
Statements, posted or available electronically (Note 10)	Either	Either	Either
Visa Card	Not available	Not available	
Internet/Mobile Banking	Not available		
Member Cheques	Not available		
Direct Entry Credits	Not available		
Direct Entry Debits	Not available		
Periodical Payments	Not available		
Pay Anyone	Not available		
BPAY®	Not available		
Interest Calculation Method	Type E	Type E	Type E
Interest Paid	At maturity for terms of 12 months or less. Annually for terms greater than 12 months.	Monthly	At maturity for terms of 12 months or less. Annually for terms greater than 12 months.
Automatic roll over on maturity	✓ and see Note 8	✓ and see Note 8	✓ and see Note 8

PART H - Summary of Accounts & Availability of Access Facilities

Notes

1.

	Interest Rate Types				
	Type A	**Type B**	**Type C**	**Type D**	**Type E**
Interest calculation method	Minimum monthly	Daily balance on tiered rates	Daily balance on tiered rates	Minimum monthly	Daily balance
Interest payment	Annually on 31 May	Quarterly at the end of March, June, September & December	Monthly	Annually on 31 October	Monthly

2. If you are not eligible or for any 12-month period your pension is not deposited by direct credit, we will convert the account to an Access Account.

3. This account offers a cents gifting program. At the end of each month, the cents on the account balance (up to 0.99 cents) per account will be matched by Australian Military Bank and donated to selected Defence related charities. Account owners can either direct which charities offered by Australian Military Bank that their total monies will be donated to, or, where no charity is selected, the donation will be split equally amongst the charities.

4. 1% cash back on Visa payWave purchases under $100 in Australia (capped at $25 per month), applies when you deposit $2,000 or more per calendar month (excluding transfers from other Australian Military Bank accounts) into your Military Rewards account. Your account will be credited with the cash back in the calendar month after which your deposit and any respective transactions are made. This means that when your Military Rewards account is closed, you will not receive any cash back credits for transactions that occur in the calendar month in which the account is closed. The intent of the cash back offer is to reward eligible Military Rewards account holders with 1% cash back (capped at $25 per month) on eligible general everyday purchases. The 1% cash back offer may be changed or withdrawn at any time at our sole discretion. Should this offer be used in a manner that is not satisfactory or in line with the intent of the offer, we may place a stop or freeze on your account, refuse to apply the rebate to any or all of the purchases, or reverse the amount of the cash backs previously paid to you. You agree that you will conduct your transactions honestly, fairly and in line with how a reasonable person would conduct purchases. This means that if a purchase normally would not be eligible for cash back, you will not manipulate your conduct or purchases to artificially activate the cash back benefit. For clarity, unsatisfactory conduct falling outside the intent of the offer may include (but is not limited to), splitting larger purchases into smaller multiple transactions, conducting repeated transactions under $100 at the same merchant within an unreasonably short period of time or opening multiple accounts under the same name for the purpose of obtaining multiple cash back mounts in excess of the monthly cap.

5. Withdrawals can only be made during the period 1 November to 31 January.

6. Funds may be transferred in and out of the Star Saver Direct and Online Saver via Mobile Banking or Online Banking and then withdrawn, subject to the conditions of that other account. Withdrawals from the Online Saver may only be made to a nominated linked account.

7. If you wish to withdraw the whole or part of your term deposit early, you must provide us with 31 days' notice. Withdrawing all or part of your term deposit will result in reduced interest being paid. Interest on the withdrawn amount will be reduced by 75% where the withdrawal is made in the first half of the term (calculated from the total days of the term deposit), and reduced by 25% where it occurs in the last half of the term. This reduced interest will be subtracted from your interest payable, unless this interest has already been paid out to you, in which case it will be subtracted against your principal.

8. Australian Military Bank will try to contact you before maturity for your instructions regarding the repayment or reinvestment of your principal and interest. If Australian Military Bank does not hear from you prior to maturity, the Bank will renew the deposit for the same term and at an interest rate applicable to the like Term Deposit available on that day. Australian Military Bank will send you confirmation. You may contact the Bank within 7 days to redeem or change the terms of the Term Deposit.

9. After turning 18, Australian Military Bank may convert this account to a different account. We will notify you before this occurs.

10. We may charge a fee for posting paper statements. Please refer to Schedule of Fees and Charges.

PART H - Summary of Accounts & Availability of Access Facilities

11. Recruit Salary Saver and Online Saver are limited to a maximum of one account per membership.

Australian Military Bank

Contact Us

1300 13 23 28

PO Box H151 Australia Square NSW 1215

Australia wide branch network

service@australianmilitarybank.com.au

www.australianmilitarybank.com.au

Australian Military Bank Ltd ABN 48 087 649 741
AFSL and Australian Credit Licence Number 237 988