Account and Access Facility Terms and Conditions

Effective: 29 March 2024

This document should be read in conjunction with the Fees and Charges Schedule and our latest interest rates available on our website. Together they form the Terms and Conditions for the accounts and services described in this document.

Australian Military Bank

How to Contact Us

Our Details
Phone: 1300 13 23 28 (Monday to Friday, 8am – 6pm and Saturday 9am – 12pm AEST)
Email: service@australianmilitarybank.com.au
Website: australianmilitarybank.com.au
Mail: Australian Military Bank, PO Box H151, Australia Square NSW 1215

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

Other Important Numbers
To report the loss, theft or unauthorised use of your Visa card, call our card hotline (available 24/7):
Calling from within Australia: 1800 648 027
Calling from overseas: +61 2 8299 9101

Financial Hardship
At some point in our lives, we all may experience financial hardship. We're here to help – if you are worried about your financial situation, call us on **1800 855 810** as soon as possible (Monday to Friday 8am – 4pm AEST).

Privacy
In order to provide services to you, we'll collect personal information about you. We'll handle it in accordance with our Privacy Policy which is available at **australianmilitarybank.com.au/privacy**. If you have any questions about our Privacy Policy please call us on 1300 13 23 28 or email us at privacy@australianmilitarybank.com.au.

Open Banking
Open Banking provides Australian Military Bank members with the ability to share your banking data with third parties that have been accredited by the ACCC. You can manage your data sharing arrangements within internet and mobile banking. For more information, please view our Consumer Data Right (CDR) Policy, available at **australianmilitarybank.com.au/disclosuredocuments**.

Contents

Introduction 4
1. Opening an Account 6
   1.1. Proof of identity 9
   1.2. 100% Mortgage Offset accounts 9
   1.3. Term deposits 9
   1.4. Joint accounts 10
   1.5. Child accounts 11
   1.6. Trust accounts 11
   1.7. Third party signatories 11
   1.8. Tax File Number (TFN) 12
   1.9. Foreign Tax Residency Status 12
2. Protecting your accounts 13
   2.1. Password and passcode security 13
   2.2. Protecting your Visa Card 13
   2.3. General security tips 13
3. Fees, charges and interest 14
   3.1. Fees and charges 14
   3.2. Earning interest 14
4. Accessing your accounts 15
   4.1. Branches and our Member Engagement team 15
   4.2. Internet and Mobile Banking 15
   4.3. Visa Card 15
   4.4. ATMs 16
   4.5. Bank@Post 16
   4.6. PayID 16
   4.7. Processing transactions 18
   4.8. Mistaken and misdirected payments 19
5. Depositing funds into your accounts 21
   5.1. Transaction limits 21
   5.2. Direct credits 21
6. Withdrawing funds from your accounts 22
   6.1. Transaction limits 23
   6.2. Visa Card transactions 23
   6.3. Digital Wallets 25
   6.4. EFTPOS 28
   6.5. BPAY payments 28
   6.6. Osko payments 29
   6.7. Future-dated payments 30
   6.8. Direct Debit 30
   6.9. PayTo agreements 30
   6.10. Unauthorised payments 34
   6.11. Liability for loss caused by system or equipment malfunction 36
7. Managing your accounts 37
   7.1. Account statements 37
   7.2. Overdrawn accounts 37
   7.3. Inactive accounts 37
   7.4. Dormant accounts 37
   7.5. Closing or suspending accounts 37
8. Communicating changes 39
9. Complaints and feedback 40
10. Definitions 41

Introduction

The accounts and access facilities detailed in this document are issued by Australian Military Bank (also refer to as 'we', 'us' and 'our').

This document applies to the following products and access facilities:

Products

- Transaction accounts
- Savings accounts
- Term deposits

Access Facilities

- Branch
- Internet and mobile banking
- Visa card access and transactions
- EFTPOS transactions
- Automatic teller machines (ATMs)
- Bank@Post
- Direct credits
- BPAY payments
- External transfers including Osko payments
- Direct debit and PayTo payment agreements

It should be read in conjunction with the Fees and Charges Schedule and our latest interest rates available on our website. Together they form the Terms and Conditions for the accounts and access facilities described in this document.

We'll provide a copy of these Account and Access Facility Terms and Conditions when you open an account. We may also send you updated versions over time, as our terms and conditions change. A copy of the latest document is available at **australianmilitarybank.com.au/disclosuredocuments**.

By becoming a customer of Australian Military Bank, you may need to become a member and shareholder of Australian Military Bank Limited. Refer to our constitution for more information available on our website at **australianmilitarybank.com.au/content/constitution**.

By opening an account or first accessing it, you become bound by these Terms and Conditions.

Customer Owned Banking Code of Practice

We commit to complying with the Customer Owned Banking Code of Practice (COBCOP), and promise we'll:

- be fair and ethical in our dealings with you;
- focus on our customers;
- give you clear information about our products and services;
- be responsible lenders;
- deliver high customer service and standards;
- deal fairly with any complaints;
- recognise our customers' rights as owners;
- comply with our legal and industry obligations;
- recognise our impact on the wider community; and
- support and promote the COBCOP.

You can download a copy of the COBCOP at **customerownedbanking.asn.au**.

ePayments Code
We are bound by and comply with the ePayments Code, including the following types of transactions:

- electronic card transactions, including ATM, EFTPOS, credit card and debit card transactions,
- pay anyone banking facility transactions,
- online transactions performed using a card number and expiry date,
- online bill payments (including BPAY),
- transactions using facilities with contactless features,
- direct debits,
- transactions using mobile devices.

More information can be found at **asic.gov.au**.

Government Deposit Guarantee
Under the Financial Claims Scheme administrated by APRA, the Australian Government has provided a guarantee of deposits up to $250,000 for each of our account holders. For further information about the Financial Claims Scheme, visit **fcs.gov.au**.

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 at the time of applying for a membership or an account, or at periodic intervals while the membership and accounts are operational.
- 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.

1. Opening an Account

Depending on the type of account, you may be able to open it via Internet or Mobile Banking, in-person at a branch or by contacting our Member Engagement team on 1300 13 23 28. You may need to become a member and shareholder of Australian Military Bank before we can open an account for you. Refer to our constitution for more information, available on our website at **australianmilitarybank.com.au/content/constitution**.

Different accounts have different eligibility criteria, restrictions and special features, as summarised below. From time to time we may remove a product from sale, vary the eligibility criteria and/or limit the availability of a product. Any impacted account holders will be notified in accordance with these terms and conditions (refer to **section 8 – Communicating Changes**).

Account Type	Account Name	Eligibility criteria	Min. opening balance	Max. balance	Restrictions	Special Features
Transaction	Military Rewards	▸ 18 years or older, and ▸ Australian citizen, permanent resident, or foreign citizen temporarily deployed to Australia on Defence related business	No minimum	n/a		▸ Cents community gifting program [2] ▸ Visa payWave rebate [3]
	Access	▸ Any age, and ▸ Australian citizen, permanent resident, or foreign citizen temporarily deployed to Australia on Defence related business	No minimum	n/a	▸ Visa Debit card can only be linked to accounts where the account holder is over 13 years of age.	▸ Relationship Rewards rebate [4]
	Recruit Salary Saver [1]	▸ 12 – 30 years old, and ▸ Australian citizen or permanent resident	No minimum	n/a	▸ Restricted to one account per member. ▸ Visa Debit card can only be linked to accounts where the account holder is over 13 years of age.	▸ Relationship Rewards rebate [4]
	Junior Saver [1]	▸ Under 18 years old, and ▸ Australian citizen or permanent resident	No minimum	n/a	▸ Restricted to one account per member. ▸ Visa Debit card can only be linked to accounts where the account holder is over 13 years of age. ▸ When the account holder turns 18, the account will be converted to standard transaction account.	▸ Relationship Rewards rebate [4]
	Pension Access [1]	▸ 55 years or older, ▸ Receiving Government pension, and ▸ Australian citizen or permanent resident	No minimum	n/a	▸ You must be receiving Government pension deposit by direct credit into the account. ▸ If you stop receiving the Government pension, the account will be converted to a standard transaction account. ▸ Interest rate varies based on balance tiers.	▸ Relationship Rewards rebate [4]

Account Type	Account Name	Eligibility criteria	Min. opening balance	Max. balance	Restrictions	Special Features
	MESS	▸ Defence related clubs, canteens & messes	No minimum	n/a		▸ Relationship Rewards rebate [4]
	100% Mortgage Offset	▸ Over 18 years of age, ▸ Australian citizen or permanent resident, and ▸ Have a linked eligible home loan (Value or Standard Variable including DHOAS)	No minimum	n/a	▸ Cannot be linked to non-eligible home loans including RateSaver, Fixed and Construction (including DHOAS).	▸ Relationship Rewards rebate [4]
Savings	Online Saver	▸ 12 years and older, and ▸ Australian citizen or permanent resident	No minimum	n/a	▸ Bonus interest payable if no withdrawals in the calendar month, on balances up to $500,000. ▸ Withdrawals can only be made to linked internal accounts.	▸ Relationship Rewards rebate [4]
	DIY Super Saver	▸ Trustees of self-managed super funds, ▸ Over 18 years old, and ▸ Australian citizen or permanent resident	No minimum	n/a		▸ Relationship Rewards rebate [4]
	Christmas Club	▸ Over 18 years old, and ▸ Australian citizen or permanent resident	No minimum	n/a	▸ Withdrawals can only be made between 1 November and 31 January each year.	▸ Relationship Rewards rebate [4]
Term Deposits	Investment Plus	▸ Over 18 years old, and ▸ Australian citizen or permanent resident	$1,000	$2,000,000	▸ Early withdrawal will result in an interest rate reduction.	
	Income Plus	▸ Over 18 years old, and ▸ Australian citizen or permanent resident	$1,000	$2,000,000	▸ Early withdrawal will result in an interest rate reduction.	
	Teen Plus	▸ Under 18 years old, and ▸ Australian citizen or permanent resident	$500	$2,000,000	▸ Early withdrawal will result in an interest rate reduction.	

Notes:

1. If after opening an account you no longer meet the eligibility criteria, we may convert the account to one of our other accounts.

2. Cents community gifting program

At the end of the month, we'll transfer the cents from your account up to $0.99 and donate it to one of our four Defence charities; Legacy Australia, RSL DefenceCare, Mates4Mates and Solider On. You can select your preferred charity when you open your account. If you do not make a selection, we'll distribute your donation across the charities. We'll then match your donation each month. For example if your account balance is $2,500.49 at the end of the month, we'll donate $0.49 for you and we'll match it, so a total of $0.98 will be donated to the charity. Donations are made under Australian Military Bank's name, not each individual member. We may vary or withdraw this offer at any time.

3. Visa payWave rebate
Earn 1% cashback rebate for transactions under $100 when you tap with Visa payWave to pay (i.e. using the contactless payment option), up to a maximum $25 per month. Applies when you deposit $2,000 or more per calendar month (excluding transfers from other Australian Military Bank accounts). Your account will be credited with the cashback in the following calendar month (e.g. rebate on January transactions will be credited in February). If your account is closed during the month, you will not receive the rebate the following month.

If you make transactions not in line with the intent of the offer such as 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 amounts in excess of the monthly cap, 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.

We may vary or withdraw this offer at any time.

4. Relationship Rewards rebate
Earn up to $50 per month rebate based on your combined balance*, to offset the following transaction fees; EFTPOS, BPAY (excluding staff-assisted), Pay Anyone (excluding staff-assisted) and Direct Debit.

Combined Balance *	Maximum Rebate per month	
	Eligible accounts (excl. Junior Saver)	Junior Saver accounts
$5,000.00 to $19,999.99	$5.00	$10.00
$20,000.00 to $49,999.99	$10.00	$15.00
$50,000.00 to $99,999.99	$20.00	$25.00
$100,000.00 to $199,999.99	$35.00	$40.00
$200,000.00 +	$50.00	$50.00

* Your combined monthly balances for calculating your free transactions allowance are the total closing balances on the last day of the previous month of all your transaction and savings accounts, term deposits, loans, overdrafts and credit card accounts. Unused limits on overdrafts and credit cards are not considered. Negative balances of deposit accounts are deducted from the total. Balances in joint accounts are considered towards the allowance for the primary account holder only. Any unused transaction allowance cannot be carried forward to offset fees in future months. The maximum rebate paid in any given month will not exceed the amount incurred in eligible fees.

We may vary or withdraw this offer at any time.

1.1. Proof of identity

The law requires us to verify your identity when you open an account as well as any person you appoint as a third party signatory to your account. In most cases you can prove your identity by providing one or more documents such as an Australian Driver's License, Australian Passport or Medicare Card. In some circumstances we may verify your identity online with the document issuer or official record holder via third party systems. If you are sending your documents to us, we require these documents to be certified. More information can be found on our website. You'll be unable to open or operate any account until we have verified your identity.

If you do not have a photo ID or for account holders under 18 years of age, please contact us to discuss what forms of identification may be acceptable.

We may also ask you to verify your identity periodically while you hold a membership with us including when making transactions in person at a branch or over the phone, applying for a new product or when the current identification has expired.

1.2. 100% Mortgage Offset accounts

Our Mortgage Offset account is available for eligible home loans and allows the account holder to deposit and withdraw money from the account like a standard everyday transaction account. However, the balance of your Mortgage Offset account is used to reduce (or 'offset') the balance owing on your linked home loan when calculating the monthly home loan interest amount. This means more of each repayment will go towards paying the principal part of your home loan down quicker, rather than paying interest. It does not change the amount of your home loan repayments.

Interest on a home loan is calculated based on its closing balance each day and charged each month. So the amount as well as the number of days you have the funds in your Mortgage Offset account during the month will be used when calculating how much interest is charged to your home loan each month.

1.3. Term deposits

- When opening a new term deposit, you will have 7 days to fund the account otherwise it will be closed and you will need to reapply.
- The interest rate agreed when a term deposit is established is fixed for the term of the deposit.
- You will be able to view your term deposit within internet and mobile banking.
- Depending on the term deposit product selected, interest will be paid:
  - **Investment Plus**; at the end of the term (or annually if the term is more than 12 months)
  - **Income Plus**; monthly
  - **Teen Plus**; at the end of the term (or annually if the term is more than 12 months).
- Interest does not compound on term deposits.
- As part of the process to set up a term deposit, we'll ask for your instructions regarding whether you would like to withdraw or reinvest the funds at the end of the term. You can contact us at anytime to update these instructions. We'll contact you before the term deposit is due to expire to re-confirm these instructions, however if we do not hear from you, we'll follow the instruction provided when the term deposit was set up. The interest rate for reinvestment will be based on the current interest rates at the time.
- If you wish to withdraw your term deposit early, you must provide us with 31 days' notice.
- We do not allow partial withdrawals from a term deposit.

- Early withdrawal from a term deposit will incur the following interest rate reduction:

Portion of term remaining	Interest rate reduction
Less than 20%	20%
20% - 40%	40%
40% - 60%	60%
60% - 80%	80%
More than 80%	90%

  Example:
  Matthew opened a 12 month term deposit for $50,000 on 15 April at an interest rate of 5% p.a. On the 15 December he decides to withdraw his funds to use as a deposit on a new house. Below is how the interest payable will be calculated:
  Portion of term remaining: 4 months / 12 months = 33.33%
  Interest rate reduction: 5% x 40% = 2%
  Interest payable: $50,000 x (5% - 2%) x (8 months / 12 months) = $1,000
- The reduced interest amount will be subtracted from your interest payable, unless this interest has already been paid out to you, in which case it will be subtracted from your principal investment.

1.4. 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 – refer to the 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 approve withdrawals and account changes.
- 'either/or to sign' means any one joint holder can operate the account including making withdrawals and changes to the account.

All joint accounts will initially be set up as an 'either/or to sign' basis. However, at any time 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 disbursal 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 or for the account to be closed. We may also make a joint account 'all to sign' if we become aware of a dispute between account holders.

For joint accounts, each account owner has the Consumer Data Right to share account data with accredited recipients provided all account owners are eligible to share data for the account. Any joint account holder may withdraw their consent for data sharing on an account at any time.

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. Joint Accounts are not available to company or corporate trustee applicants.

1.5. Child accounts

If a child is under 13 years of age, a parent/guardian must open the account on the child's behalf and be a signatory to operate. Children are not permitted to personally transact on an account if under 13 years of age.

If the child is 13 years of age or older, the account can be opened and personally operated on by the child. Depending on the account type, a Visa Debit Card may be linked. A child over the age of 13 years can appoint or remove signatories to operate the account such as a parent/guardian.

For accounts specifically designed for children, we may convert it to another account type when the account holder turns 18 years old by providing written notice (refer to **section 8 – Communicating changes**.

1.6. Trust accounts

You can open an account as a trust account, including 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.

1.7. Third party signatories

You can authorise us to allow another person to operate on your account/s including a power of attorney. However, we will need to verify this person's identity and they may need to become a member of Australian Military Bank before they can access your account. We'll only recognise a power of attorney that is active and complies with the relevant legal requirements.

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 are responsible for all transactions the third party signatory carries out on your account. You should ensure that the third party signatory 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.

We may, at our discretion, refuse to act on any authority to operate or power of attorney document at any time, if the authority or power of attorney is not valid or if we become aware of fraud, non-compliance with the authority or power of attorney or any unlawful activity. To the extent permitted by law, we are not responsible for any decision to act, or not act, on any authority to operate or power of attorney document.

1.8. Tax File Number (TFN)

When you open an account we will ask you whether you want to disclose your TFN or TFN 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, we will then deduct withholding tax from interest paid on the account at the highest marginal tax 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 can quote either their TFN or Australian Business Number (ABN).

1.9. Foreign Tax Residency Status

When you open an account we're required to collect certain information and documents about you in order to determine your Foreign Tax Residency Status. When required by law, we may provide that information to the Australian Tax Office (ATO).

You must advise us within 30 days if your Foreign Tax Residency Status changes by calling 1300 13 23 28.

2. Protecting your accounts

You have a responsibility to protect your Visa card/s, internet and mobile banking accounts, devices and passwords / passcode from unauthorised transactions.

2.1. Password and passcode security

Below are your obligations regarding passwords and passcodes:

- When setting your PIN, passwords and passcodes, do not select ones that are easily identifiable such as birth date, your name, etc.
- Never write or save your passwords and passcodes on your Visa card, mobile phone, computers, etc even if disguised.
- Never voluntarily share your passwords or passcodes with others.
- Use care to prevent anyone seeing the passcode being entered on a device.
- Never share one-time-passcodes (OTPs) with anyone. Including us as we will NEVER ask for this.
- Set a passcode to access your device/s.
- Always reject any request to provide or to confirm details of your PIN, password or passcode. We will NEVER ask you to provide us with these details.
- Notify us immediately when you become aware of, or suspect that your passwords or passcodes have been compromised.

2.2. Protecting your Visa Card

Below are your obligations regarding your Visa Card:

- Sign your Visa card as soon as you receive it.
- When setting your PIN, do not select ones that are easily identifiable such as birth date.
- Never lend your Visa card to someone and take care that people can't see you enter your PIN.
- Check your statements regularly for any unauthorised use.
- Notify us immediately when you become aware of, or suspect that your Visa card has been lost, stolen or compromised.

2.3. General security tips

- Install the latest software and security updates when available,
- Lock your device when not in use and don't leave it unattended,
- Check your statements and transaction listing within internet or mobile banking regularly for any unauthorised use.
- Notify us immediately when you become aware of, or suspect that your device is lost, stolen, or when your device passcode / internet banking password / mobile banking passcode has been compromised.
- Only access internet banking service only using the official URL address
- Don't click on links from Emails, SMS and other electronic messages.
- When borrowing someone's device, always clear your browsing history.

Note: These guidelines provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised payments. Your liability for unauthorised transactions is determined in accordance with the ePayments Code (refer to **section 6.10 – Unauthorised transactions**).

If you fail to ensure the security of your Visa card, internet and mobile banking accounts, passwords / passcode and device or delay advising us they are compromised and this contributes to an unauthorised transaction, then you may be held responsible for those transactions.

3. Fees, charges and interest

3.1. Fees and charges

Please refer to the Fees & Charges Schedule for current fees and charges available on our website. We may vary fees or charges from time to time by providing notice (refer to **section 8 – Communicating changes**).

We will debit your primary account for all fees and charges including any government taxes or charges.

3.2. Earning interest

Depending on the account you hold, it may be eligible to earn interest. Interest earned on an account is income and may be subject to income tax.

The below table indicates how we calculate and pay interest for each type of account. Our latest interest rates are available on our website.

Account Type	Account Name	Eligible to earn interest	Interest paid	Interest calculated
Transaction	Military Rewards	Yes	Monthly	Daily balance
	Access	Yes	Annually – 31 May	Minimum monthly balance
	Recruit Salary Saver	Yes	Monthly	Daily balance
	Junior Saver	Yes	Quarterly – 31 March, 30 June, 30 September, 31 December	Daily balance
	Pension Access	Yes	Monthly	Daily balance Interest rates varies based on below tiered balances: Tier 1: $0 - 49,200 Tier 2: $49,201 - $250,000 Tier 3: >$250,000
	100% Mortgage Offset [1]	No	n/a	n/a
	MESS	Yes	Annually – 31 May	Minimum monthly balance
Savings	Online Saver	Yes (for balances up to $500,000)	Monthly	Daily balance (up to $500,000) Interest rate is split by base rate plus bonus rate if no withdrawal in a calendar month.
	DIY Super Saver	Yes	Monthly	Daily balance
	Christmas Club	Yes	Annually – 31 October	Minimum monthly balance
Term Deposits	Investment Plus [2]	Yes	At maturity (or annually for terms > 12mths)	Daily balance
	Income Plus [2]	Yes	Monthly	Daily balance
	Teen Plus [2]	Yes	At maturity (or annually for terms > 12mths)	Daily balance
Accounts No Longer Available	Star Saver	Yes	Monthly	Daily balance
	Legacy Overdraft	No	n/a	n/a

1. The Mortgage Offset account does not earn interest, rather the balance of the account is used to reduce the balance of the linked home loan when calculating the monthly home loan interest amount.

2. Interest does not compound on Term Deposits.

4. Accessing your accounts

4.1. Branches and our Member Engagement team

We have branches on-base at a number of key Australian Defence Force (ADF) locations. If you are not currently serving in the ADF, don't worry we can still help you. Just call your closest branch to make an appointment. You can find our branch addresses and contact details on our website.

Alternatively, you can call us on 1300 13 23 28 and one of our friendly team members can help you with your accounts.

4.2. Internet and Mobile Banking

We provide internet and mobile banking services which allows you to access, managed and transact on your deposit accounts and any other accounts you are authorised to operate. To use these services you must be at least 13 years of age. Internet and mobile banking services are provided free of charge, however you may incur data charges from your internet or mobile network provider.

The services and features available within internet and mobile banking such as external transfers and BPAY payments may vary depending on your account type (refer to **section 6 – Withdrawing funds from your accounts**). Note: some features in internet banking may not be available in mobile banking (and vice versa). We are also not able to support all devices, browsers and operating systems. You're responsible for ensuring you have a compatible device and software to use these services.

When accessing internet and mobile banking, you'll need to provide your member number and password/passcode. To perform selected activities within internet and mobile banking, you may be required to enter a one-time passcode (OTP), which will be sent to you by SMS or email depending on your communication preferences. Remember: Never share OTPs with anyone, including us.

If you are transferring money to someone you haven't before or raising your transaction limits, we may ask you additional questions, provide warnings or delay the transaction to protect you from falling victim to a scam.

If you believe that your password / passcode for internet/mobile banking transactions have been misused, lost or stolen, or, when relevant, your password / passcode has become known to someone else, you should change it and let us know immediately.

We do not warrant that the information about you and your accounts within internet and mobile banking are always up to date, that the data is totally secure, or that it will be available 24 hours a day, 7 days a week.

4.3. Visa Card

A Visa Card allows you to deposit and withdraw cash at Bank@Post, withdraw cash from ATMs as well as make purchases (online and in-person) at any retailer displaying the Visa Card logo, anywhere in the world.

A Visa Debit card is available on all transaction accounts except for:

- Children aged under 13 years of age.
- Accounts set to "all to sign", or
- If your banking history with Australian Military Bank is not satisfactory.

It is not available on our savings accounts.

You can add additional cardholders to your accounts as well. For our MESS account particularly, you can have unlimited cardholders. You will be liable for all transactions carried out by any additional cardholder/s. To cancel an additional Visa card, please call us.

We will provide you with a Personal Identification Number (PIN) to use with your Visa Card and you agree to sign the physical card when you receive it. You can change your PIN via internet or mobile banking. The Visa Card always remains our property.

You may load your Visa Card on to your mobile phone in a Digital Wallet app (refer to **section 6.3 – Digital Wallets**).

4.4. ATMs

You can use your Visa Debit card to withdraw cash at our ATMs.

You can also use the ATMs of other major banks as well as independent ATM operators. Please note that you may be charged a fees by them, but you'll be notified on the ATM screen and only be charged if you accept the fee and proceed with the transaction.

4.5. Bank@Post

You can make deposits and withdrawals to your transaction accounts linked with a Visa Card at any post office displaying the Bank@Post logo.

4.6. PayID

A PayID is an identifier you can register to receive payments, by linking your bank account to a memorable piece of information, such as your phone number, email address, ABN. PayID is also the name of the service that enables direct payment through this identifier so you can send payments to a PayID without the need to remember BSB and account numbers.

4.6.1. Making and receiving NPP payments using PayID

- The PayID Service may be used to make payments, including Osko Payments.
- In order to receive an NPP Payment into your Account, you must provide the payer with a PayID that is linked to that Account in the same way that you would provide your BSB and Account number for standard payments into your Account.
- You can only create a PayID in respect to an Eligible Account.
- Before you can use your PayID to receive NPP Payments into your Account, you must satisfy us that you own, or are authorised to use, your chosen PayID. We may ask you to provide evidence to establish this to our satisfaction.
- Whether or not you choose to create a PayID for your Account, you and any third party signatories may use a payee's PayID to make an NPP Payment to the payee from your Account provided that:
  - the Account allows you to make NPP Payments;
  - both we and the payee's financial institution support the PayID Service;
  - the payee's account is able to receive the particular NPP Payment; and
  - the PayID is not Locked.
- If you make an NPP Payment to a payee from your Account using the payee's PayID, you must ensure that you input the payee's PayID correctly and check the payee's PayID Name before sending the NPP Payment.

4.6.2. Choosing a PayID and receiving a PayID name

- Your PayID must be a supported PayID Type. We may update the PayID Types that we support from time to time. You can review the most up to date list of PayID Types we support on our website.

- Some PayID Types, for example Organisation IDs, are restricted to business customers and organisations. Only eligible customers will be able to register a PayID that is a restricted PayID Type.
- Your PayID Name may be displayed to payers who send PayID Payments to you.
- At the time that you create your PayID, we will allocate to you a PayID Name that displays to payers.

4.6.3. Creating your PayID

- You can create a PayID using internet banking, mobile banking or by calling us.
- You may choose to create more than one PayID for your Account.
- If your Account is a joint account, each joint account holder can create a unique PayID for the Account.
- If you have a third party signatory on your Account, they may create a unique PayID for the Account.
- Once a PayID is created and linked to your Account, it may not be used in relation to any other account with us or with any other financial institution unless it is transferred to another account in accordance with **section 4.6.4 – Transferring your PayID**.
- You may not create a PayID that already exists within the PayID Service, whether or not that PayID is attributable to you. If you try to create a PayID for your Account which is identical to another PayID in the PayID Service, we will notify you that that PayID already exists and cannot be used. If you receive such a notification, you can contact us by calling our Member Contact Centre on 1300 13 23 28. We cannot disclose personal information in connection with duplicate PayIDs.

4.6.4. Transferring your PayID to another account

- You can transfer your PayID to:
  - another account you hold with us by submitting a request to us in internet or mobile banking or by calling us; or
  - an account you hold with another financial institution by calling us to submit a request.
- A transfer of your PayID to another account you hold with us will generally be effective immediately, unless we notify you otherwise.
- A transfer of your PayID from your Account to another financial institution is a two-step process initiated by you and completed by that financial institution. First, ask us to put your PayID into a transfer state and then complete the transfer via your new financial institution. Until the transfer is completed, NPP Payments made using your PayID will be directed to your Account. If the other financial institution does not complete the transfer within 14 days, the transfer is deemed ineffective and your PayID will remain with your Account until such time as an effective transfer is carried out. You can try to transfer your PayID again at any time.
- You cannot transfer your PayID if it is locked (refer to **section 4.6.7 – Locking and Unlocking a PayID**).

4.6.5. Transferring your PayID from another financial institution to your account

- To transfer a PayID that you created for an account held with another financial institution to your Account, you will need to start the process with that financial institution and then complete the transfer with us.

4.6.6. Closing a PayID

- You can Close your PayID through internet banking, mobile banking or by calling us.
- You must notify us immediately if you no longer own or have authority to use your PayID.

4.6.7. Locking and unlocking a PayID

- We monitor PayID use to manage PayID misuse and fraud. We will Lock your PayID if we reasonably suspect misuse of your PayID or that your PayID is being used to procure NPP Payments fraudulently.
- You can request to unlock your PayID by calling us.

4.6.8. NPP Payments

- We are responsible for ensuring that your PayID and Account details are accurately recorded in the PayID Service.
- When we and the sending financial institution determine that an NPP Payment made to your Account is either a Mistaken Payment or a Misdirected Payment, we may, without your consent, and subject to complying with any other applicable terms and conditions, deduct from your Account, an amount up to the original amount of the Mistaken Payment or Misdirected Payment. We will notify you if this occurs.
- If you have conducted a Mistaken Payment or a Misdirected Payment you need to notify us as soon as possible. There is no guarantee the funds can be returned.

4.6.9. Privacy

- By creating your PayID you authorise:
  - us to record your PayID, PayID Name and Account details (including Account name) (PayID Record) in the PayID Service hosted by NPP Australia Limited; and
  - NPP participants which are payers' financial institutions to use your PayID Record for the purposes of constructing NPP payment messages, enabling payers to make NPP Payments to you, and to disclose your PayID Name to payers for NPP Payment validation.
- To the extent that the creation and use of the PayID Record constitutes a disclosure, storage and use of your personal information within the meaning of the Privacy Law, you consent to that disclosure, storage and use.

4.7. Processing transactions

- We will debit your transactions received on any one day in the order we determine in our absolute discretion. Transactions may not be processed to your account on the same day.
- We can reverse a direct credit if we do not receive full value for the direct credit.
- 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 block, delay or not process a transaction for the reasons set out in section 7.5 – Closing or suspending accounts. 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. Refer to the Fees and Charges Schedule for details.
- We will use best endeavours to ensure that we process transactions initiated by both you and us, correctly. However sometimes errors do occur. If this happens, we may (as appropriate), take the necessary action required to make the necessary adjustments to rectify the error. For example, if a transaction or fee is applied to your account incorrectly, we may reverse that transaction.

4.8. Mistaken and misdirected payments

- Mistaken payment means a payment by a user through a pay anyone banking facility and processed by a financial institution when 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:
  - the user's error, or
  - the user being advised of the wrong BSB number and/or identifier
- 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.
- The table underneath sets out the process we'll follow under the ePayments Code if you make or receive a Mistaken Payment.

YOU MADE A PAYMENT	YOU RECEIVED A PAYMENT
If a report is made within 10 Business Days	
▸ If you report a mistaken payment, we'll assess your request and contact the other financial institution within 5 business days if we are satisfied that a mistaken payment has happened. ▸ If the other financial institution is satisfied that you made a mistaken payment, they must return the funds to us. This may take up to 10 business days. ▸ If the receiving financial institution is not satisfied that you made a Mistaken Payment, they may ask for the recipient to consent to the return of the funds to us. ▸ If the recipient has insufficient funds, the receiving financial institution will take reasonable steps to return the funds to us. ▸ If we receive the funds back from the recipient, we'll return them to you as soon as practicable. ▸ If we are not satisfied that you made a Mistaken payment, we'll not take any further action. ▸ Either way, we'll advise you of the outcome in writing within 30 days of the report being made.	▸ If another financial institution reports to us that you've received a mistaken payment and we are satisfied that a mistaken payment has occurred, we must return the funds to the sending financial institution. This may take up to 10 business days. ▸ If there are insufficient funds in your account, we may debit your other account/s if those accounts have funds or work with you to make other arrangements. ▸ If we are not satisfied that a Mistaken Payment has occurred, we may ask for your consent to return the funds.
If a report is made between 10 Business Days and 7 months	
▸ If you report a mistaken payment, we'll assess your request and contact the other financial institution within 5 business days if we are satisfied that a mistaken payment has happened. ▸ The receiving financial institution has 10 business days to investigate the request. ▸ If they are satisfied that a mistaken internet payment has occurred, they will place a hold on the funds and give the recipient 10 business days to establish that they are entitled to the funds.	▸ If another financial institution reports to us that you've received a mistaken payment and we have 10 Business Days to investigate the request. ▸ If we are satisfied that a mistaken internet payment has occurred, we'll place a hold on the funds and give you 10 business days to establish that you are entitled to those funds. ▸ If there are insufficient funds in your account, we may debit your other account/s if those accounts have funds

▸ If the recipient cannot establish that they are the entitled to the funds, the funds will be returned to us within 2 business days. We'll return the funds to you as soon as practicable. ▸ If the recipient has insufficient funds, the receiving financial institution will take reasonable steps to return the funds to us. ▸ 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. ▸ If a Mistaken payment has not occurred, the receiving financial institution may seek consent from the recipient to return the funds. ▸ If we are not satisfied that you made a Mistaken payment, we'll not take any further action. ▸ Either way, we'll advise you of the outcome in writing within 30 days of the report being made.	or work with you to make other arrangements. ▸ If you cannot establish that you are the entitled recipient to the funds, we'll return the funds to the other financial institution within 2 business days. ▸ If we are not satisfied that a Mistaken Payment has occurred, we may ask for your consent to return the funds.
If a report is made after seven months	
▸ If you report a mistaken payment, we'll assess your request and contact the other financial institution within 5 business days if we are satisfied that a mistaken payment has happened. ▸ If the receiving financial institution is satisfied that a mistaken payment has occurred, they will ask for the recipient to consent to the funds being returned. ▸ If the recipient has insufficient funds, the receiving financial institution will take reasonable steps to return the funds to us. ▸ If we receive the funds back from the recipient, we'll return them to you as soon as practicable. ▸ Either way, we'll advise you of the outcome in writing within 30 days of the report being made.	▸ If another financial institution reports to us that you've received a mistaken payment and we'll investigate the request. ▸ If we are satisfied that a mistaken internet payment has occurred, we'll ask for your consent to return the funds to the sender. ▸ If there are insufficient funds in your account, we may debit your other account/s if those accounts have funds or work with you to make other arrangements.

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.

- If no request has been made by another financial institution and we reasonably believe that a Mistaken Payment has occurred, we may restrict access to those funds in your account while we conduct further investigations.
- We are not liable to you for, and you indemnify us against any and all loss incurred by you or any other person arising from us returning the Mistaken Payment.
- If you are unhappy with how we have dealt with the report of an unauthorised transaction or mistaken payment you can raise a complaint and we will deal with the complaint under our internal dispute resolution procedures, and will not require you to complain to the Receiving Financial Institution. If you are not satisfied with the outcome of a complaint, you can complain to the Australian Financial Complaints Authority. Please refer to **section 9 – Complaints and feedback** for more details.

5. Depositing funds into your accounts

The access facilities available for depositing funds into your account varies based on type of account, as summarised below:

Account Type	Account Name	Branch	Electronic Transfer	Direct credit	Bank@Post
Transaction	Military Rewards	✓	✓	✓	✓
	Access	✓	✓	✓	✓
	Recruit Salary Saver	✓	✓	✓	✓
	Junior Saver	✓	✓	✓	✓
	Pension Access	✓	✓	✓	✓
	100% Mortgage Offset	✓	✓	✓	✓
	MESS	✓	✓	✓	✓
Savings	Online Saver	✓	✓	✓	n/a
	DIY Super Saver	✓	✓	✓	n/a
	Christmas Club	✓	✓	✓	n/a
Accounts No Longer Available	Star Saver	✓	✓	✓	n/a
	Legacy Overdraft	✓	✓	✓	✓

5.1. Transaction limits

Type of Transaction	Maximum Daily Limit
Branch	Cash deposit – $10,000 (unless agreed with the branch)
Bank@Post	Cash deposit - $3,000

5.2. Direct credits

You can deposit money into your transaction and savings accounts using electronic transfer using your BSB and account number or your PayID. You can also provide these details to others (such as your employer) to credit your account.

6. Withdrawing funds from your accounts

The access facilities available for withdrawing funds from your account varies based on type of account, as summarised below:

Account Type	Account Name	Branch	Visa - credit transaction	EFTPOS - savings transaction	Electronic transfers (incl. Osko)	Direct Debit & PayTo	BPAY®	ATM	Bank@Post
Transaction	Military Rewards	✓	✓	✓	✓	✓	✓	✓	✓
	Access	✓	✓	✓	✓	✓	✓	✓	✓
	Recruit Salary Saver	✓	✓	✓	✓	✓	✓	✓	✓
	Junior Saver	✓	✓	✓	✓	✓	✓	✓	✓
	Pension Access	✓	✓	✓	✓	✓	✓	✓	✓
	100% Mortgage Offset	✓	✓	✓	✓	✓	✓	✓	✓
	MESS	✓	✓	✓	✓	✓	✓	✓	✓
Savings	Online Saver	×	n/a	n/a	✓ [1]	×	×	n/a	n/a
	DIY Super Saver	✓	n/a	n/a	✓	✓	✓	n/a	n/a
	Christmas Club [2]	✓	n/a	n/a	✓	✓	✓	n/a	n/a
Accounts No Longer Available	Star Saver	✓	n/a	n/a	✓	✓	✓	n/a	n/a
	Legacy Overdraft	✓	✓	✓	✓	✓	✓	✓	✓

1. Online Saver can only be linked to one account for withdrawals to be made, which can be either an Australian Military Bank account or an external account.

2. Withdrawals from a Christmas Club account can only be made between 1 November and 31 January each year.

6.1. Transaction limits

- We may limit the value of your daily withdrawals, payments or transfers you make, either generally or in relation to a particular service.
- Below are the current maximum daily limits (and are subject to change):

Type of Transaction	Maximum Daily Limit
Internal transfer to another Australian Military Bank account	$200,000
Pay Anyone (excluding Osko)	$30,000
Pay Anyone (using Osko)	$10,000
Overseas	$5,000
BPAY	$30,000
ATM	$1,000 (combined with EFTPOS but excludes any transactions when 'credit' is selected)
EFTPOS	$1,000 (combined with EFTPOS but excludes any transactions when 'credit' is selected)
Branch	Cash withdrawals – $10,000 (unless agreed with the branch)
Bank@Post	Cash withdrawal - $2,000

- When you open an account, we may set the transaction limits lower. You can manage your daily maximum limits through internet and/or mobile banking or by calling us. We may, in our discretion, agree to vary a transaction limit on your request.
- We may also require you to apply for new transaction limits if you change any passcode or contact details. We will require you to provide proof of identity that satisfies us. We may reduce transaction limits to zero for security reasons.
- Merchants, billers or other financial institutions may impose additional restrictions on the value you can withdraw, pay or transfer.
- If you need to transfer funds for higher amount than the daily limit, please contact us and we can organise a SWIFT transfer or a staff assisted external transfer depending on when the funds are required. Refer to the Fees and Charges Schedule.

6.2. Visa Card transactions

A Visa Card allows you to deposit and withdraw cash at Bank@Post, withdraw cash from ATMs as well as make purchases (online and in-person) at any retailer displaying the Visa Card logo, anywhere in the world.

You may load your Visa Card on to your mobile phone in a Digital Wallet app (refer to **section 6.3 – Digital Wallets**).

6.2.1. 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.

Please note that chargebacks do not apply to BPAY® payments using your Visa Card.

Reporting loss, theft or unauthorised use of your Visa card or PIN

- If you believe your Visa 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 card hotline available 24/7.
  Within Australia: 1800 648 027
  Outside Australia: + 61 2 8299 9101
- If the 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 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.

You will be liable for any transactions you make using your Visa Card before the Visa Card is cancelled but which are not posted to your account until after cancellation of the Visa Card.

6.2.2. Foreign currency transactions

- 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).
- All transactions made in foreign currency or with a merchant located overseas (even if the transaction is in Australian currency) using a Visa Card are subject to a conversion fee. Please refer to the Fees and Charges Schedule for the current conversion fee.
- Some overseas merchants and electronic terminals charge a surcharge for making a transaction using your Visa Card. Once you have confirmed that transaction you will not be able to dispute the surcharge. The surcharge may appear on your statement as part of the purchase price.
- Some overseas merchants and 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.

6.2.3. Regular payments

- A regular payment arrangement means either a recurring or an instalment payment agreement between you (the cardholder) and a Merchant in which you have authorised 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.
- 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.
- Should your card details be changed (for example if your Visa Card was lost, stolen or expired and has been replaced) or you close your accounts with us, 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.

6.2.4. Visa Secure

Visa Secure is a 3D secure fraud prevention measure to add an additional layer of security when you are shopping with a participating online merchant.

- When making an online purchase or other transaction for which 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 Visa card, such information includes, but is not limited to, a One Time Passcode (OTP). The information that you provide may be validated against information we hold about you and may be validated against information held by third parties.
- 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 Visa card payment for that transaction, and you may be unable to complete an online transaction using your Visa card.

6.2.5. Exclusions of Visa card warranties and representations

- We do not warrant that merchants or ATMs displaying the Visa card signs or promotional material will accept Visa card.
- We do not accept any responsibility should a merchant, bank or other institution displaying the Visa card signs or promotional material, refuse to accept or honour the Visa card.
- 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.

6.3. Digital Wallets

Digital Wallets allow users to download an app, provision a virtual Visa Card and make contactless payments using a compatible mobile device. The minimum age limit to use this feature is 13 years of age and depends on your Digital Wallet provider such as Apply Pay and Google Pay. Check with your Digital Wallet provider for details. These terms apply and are deemed accepted when you register and use a Visa Card in a Digital Wallet.

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

- You agree to protect and keep confidential your passcodes (including your mobile device lock passcode) and all other information required for you to make purchases with your card using the Digital 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.

If you let another person use your mobile device, or you share your confidential information required to make purchases with your card using the Digital Wallet, you will deemed to have authorised that person to transact on your account. This means that any transaction

conducted using the Digital Wallet initiated by that person using the information your provided will be authorised by you and the 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 transactions conducted using the Digital Wallet.

6.3.2. Using a wallet

- Registering a card into a Digital Wallet is subject to us identifying and verifying you, and is at our discretion.
- We do not make any guarantees that the Digital Wallet will be accepted at all merchants.
- We are not the provider of the Digital Wallet and are 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.

We 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.

6.3.3. 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.

6.3.4. 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.

6.3.5. 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.

6.3.6. 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.

6.3.7. 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.

We are 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.

Our Privacy Policy is available on our website and provides further details regarding the collection and handling of your information.

6.3.8. 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 fingerprint, 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, we do 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 these terms and conditions.

6.4. EFTPOS

When you use your Visa Debit card for purchases, you may have the option to select "savings". This is classified as an EFTPOS transaction.

6.4.1. EFTPOS Secure

EFTPOS Secure is a 3D secure fraud prevention measure to add an additional layer of security when you are shopping with a participating online merchant.

- When making an online purchase or other transaction for which EFTPOS 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 card, such information includes, but is not limited to, a One Time Passcode (OTP). The information that you provide may be validated against information we hold about you and may be validated against information held by third parties
- 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 card or payment for that transaction, and you may be unable to complete an online transaction using your EFTPOS Visa card

6.5. BPAY payments

We are a member of the BPAY Scheme and subscribe to the electronic payments system known as BPAY Payments. We'll let you know if this changes.

6.5.1. Using BPAY

- You can use BPAY to pay bills bearing the BPAY logo from those accounts that have the BPAY facility.
- When you tell us to make a BPAY payment you must tell us the biller's code number and customer reference number (found on your bill), the amount to be paid and the account from which the amount is to be paid.
- You should ensure the account you pay from is correct and has sufficient funds. If you have insufficient funds in your account (or available credit), the BPAY payment will not be made.
- You cannot stop a BPAY payment once it's been made. Make sure it's for the correct amount and that you've used the correct Biller Code and Customer Reference Number.
- You can set up future-dated payments. However, if they fall on a date that is not a Business Day may be processed the next Business Day. You are responsible for ensuring there are sufficient funds in the account before the payment is made. You are also responsible for checking your account transaction details or account statement to ensure any future-dated payments are made correctly. You can manage and cancel future-dated payment instructions within internet and mobile banking.
- Delays may happen if your BPAY payment is made on a weekend, public or bank holiday or if the Biller or another financial institution does not comply with the BPAY rules.

6.5.2. Mistaken BPAY payments

- The ePayments Code may apply to your BPAY transaction.
- If you've made a mistaken BPAY payment, please tell us immediately. We'll try to fix it by trying to get it back from the Biller, but we're not liable for any loss or damage you suffer as a result of making a mistaken BPAY payment, except in the circumstances described below.
- If a BPAY payment is made incorrectly and not in accordance with your instructions, we'll refund the amount to your account.
- However, if we have refunded the amount to your account and subsequently determine that you're responsible for the mistake, and we can't recover the amount from the recipient within 20 business days of us trying, you have to pay us back.

6.5.3. Unauthorised BPAY payments

- If a BPAY payment was made without your authority, but looked like it came from you, we'll refund you the amount to your account. However, if you didn't comply with our security requirements, and we can't recover the amount from the recipient within 20 business days of us trying, you have to pay us back.

6.5.4. Fraudulent BPAY payments

- If you are the victim of fraud by someone involved in the BPAY Scheme, the perpetrator needs to refund you the money. If they don't, then you bear the loss, unless some other person involved in the BPAY Scheme, knew or should have reasonably known of the fraud, in which case that other person needs to refund you the money that the perpetrator didn't refund.

6.5.5. Disputing a BPAY transaction

- Except Mistaken, Unauthorised and Fraudulent BPAY payments, BPAY payments are irrevocable and no refunds are available through BPAY for disputes with Billers about goods/services. You will need to resolve any disputes regarding goods/services directly with the Biller.
- If you want us to investigate an unauthorised BPAY transaction, you have to give us written consent addressed to the relevant Biller, allowing us to obtain from them information about your transaction and payment with them, as well as any other necessary information to investigate the disputed transaction.
- If you don't provide us with this consent, the Biller doesn't have to give us the information that we need to investigate.
- If you have a complaint about how we have handled a disputed transaction under this section, we'll deal with the complaint under our internal dispute resolution procedures. If you are not satisfied with the outcome of a complaint, you can complain to the Australian Financial Complaints Authority. Please refer to **section 9 – Complaints and feedback** for more details.

6.5.6. Liability for loss

- We are not liable for any loss or damage you suffer as a result of using the BPAY Scheme, unless we acted negligently or breached a condition or warranty regarding the supply of goods or services which can't be excluded or limited under law.
- You indemnify us against any loss or damage we suffer (whether directly or indirectly) as a result of any negligent or fraudulent conduct by you.

6.5.7. Privacy - BPAY

- By using –he BPAY service to make BPAY Payments, you agree that we may need to disclose Personal Information relating to you, to BPAY and/or other BPAY Participants in order to facilitate this service.

6.6. Osko payments

Osko by BPAY® is a secure payment service which enables you to send and receive near real-time payments via internet and mobile banking. We subscribe to Osko under the BPAY Scheme and will let you know if this changes.

6.6.1. Using Osko

- You can use Osko to make payments from accounts that have the Osko facility.
- When you tell us to make an Osko payment you must tell us the payee's BSB and account details or their PayID, the amount to be paid and the account from which the amount is to be paid.
- You should ensure the account you pay from is correct and has sufficient funds. If you have insufficient funds in your account (or available credit), the Osko payment will not be made.

- You cannot stop an Osko payment once it's been made. Make sure it's for the correct amount and that you've used the payee's details.
- You can set up future-dated payments. You are responsible for ensuring there are sufficient funds in the account before the payment is made. You are also responsible for checking your account transaction details or account statement to ensure any future-dated payments are made correctly. You can manage and cancel future-dated payment instructions within internet and mobile banking.

6.7. Future-dated payments

- You can set up one off or regular future-dated payments.
- You are responsible for ensuring there are sufficient funds in the account before the payment is made.
- You are also responsible for checking your account transaction details or account statement to ensure any future-dated payments are made correctly.
- You can manage and cancel future-dated payment instructions within internet and mobile banking.

6.8. 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.
- We will not charge you a fee for cancellation of direct debit facilities.
- 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 payment agreements, which provides an alternative method to pre-authorise a biller to debit amounts from your eligible account. Refer to **section 6.9 - PayTo agreements**.

6.9. PayTo agreements

6.9.1. Creating a PayTo payment agreement

- PayTo allows you to establish and authorise Payment Agreements with Merchants or Payment Initiators who offer this service as a payment option.
- If you establish a Payment Agreement with a Merchant or Payment Initiator that offers this service, you will needed 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 details are correct. Personal information or data you provide to the Merchant or Payment Initiator will be subject to the privacy policy and terms and conditions.
- Payment Agreements must be recorded in the Mandate Management Service to be processed. 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.

- We will process payment instructions received from the Merchant's or Payment Initiator's financial institution when you have confirmed the Payment Agreement and it 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.
- 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.
- 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.
- Consent for establishing a Payment Agreement must be consistent with the term of operations for that account. For example, a joint account set to "all to sign" will require both account holders to consent to the Payment Agreement before it becomes effective.

6.9.2. Amending a PayTo payment agreement

- Your Payment Agreement may be amended by the Merchant or Payment Initiator from time to time, or by us on your instruction.
- We will notify you of proposed amendments to a Payment Agreement requested by the Merchant or Payment Initiator. 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.
- Amendment requests which are not confirmed or declined within 5 calendar days of being sent to you, will be deemed to be declined.
- 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.
- Once an amendment request has been confirmed by you, we will promptly update the Mandate Management Service with this information.
- Once a Payment Agreement has been established, you may 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 (refer to **section 6.9.4 - Transferring your payment agreement**). We may decline 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.

6.9.3. Pausing your PayTo payment agreement

- 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. We will not process payment instructions under a Payment Agreement that is paused. We are not liable for any loss that you or any other person may suffer as a result of the pausing of a Payment Agreement that is in breach of the terms of an agreement between you and the relevant Merchant or Payment Initiator.

- 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 are not liable for any loss that you or any other person may suffer as a result of the pausing of a Payment Agreement by the Merchant or Payment Initiator.

6.9.4. Transferring your PayTo payment agreement

- When available, you may ask us to transfer 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.
- 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.
- 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.
- 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.

6.9.5. Cancelling your PayTo payment agreement

- 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.
- 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.

6.9.6. Migration of direct debit arrangements

- 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. You will not be required to confirm or decline a Migrated DDR Mandate. 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.
- Once the migration is completed it is the responsibility of the Merchant or Payment Initiator to cancel the existing Direct Debit arrangement.

6.9.7. General PayTo provisions

- A Payment Agreement can only be linked to an account that has the PayTo Facility.
- 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.
- 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.
- 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.
- 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.
- 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. Refer to **section 7.2 – Overdrawn accounts**. Fees may be payable to third parties in accordance with their terms and conditions.
- 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.
- 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.
- 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.
- 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 passcodes and PINs are kept confidential and are not disclosed to any other person.
- All intellectual property, including but not limited to the PayTo trademarks 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.
- We may cancel or suspend your use of PayTo at any time and at our absolute discretion.
- You must comply with all applicable laws in connection with your use of PayTo.
- We will accurately reflect all information you provide to us in connection with a Payment Agreement (including a Migrated DDR Mandate) in the Mandate Management Service.
- 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.

- 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.
- 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.
- We accept no liability for delayed or failed payments caused by service interruptions to PayTo or other NPP services.
- 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. This must be done separately.
  - closing your PayID will cause payments under the linked Payment Agreement to fail. This must be done separately.

6.9.8. Privacy – PayTo

- 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.

6.10. Unauthorised payments

An unauthorised transaction is a transaction that is not authorised by a user. This does not include transactions carried out by the account holder or an authorised user, or by anyone who performs a transaction with the knowledge or consent of the account holder or any authorised user.

6.10.1. When you are not liable for loss

A. You are not liable for loss arising from an unauthorised transaction if the cause of the loss is any of the following:
   - fraud or negligence by our employee or agent, a third party involved in networking arrangements, or a merchant or their employee or agent
   - a device, identifier or passcode which is forged, faulty, expired or cancelled
   - 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)
   - a transaction being incorrectly debited more than once to the same facility
   - 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.

B. You are not liable for loss arising from an unauthorised transaction that can be made using an identifier without a passcode or device. When 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.

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

D. In a dispute about whether a user received a device or passcode:
   - there is a presumption that the user did not receive it, unless we can prove that the user did receive it
   - we can prove that a user received a device or passcode by obtaining an acknowledgement of receipt from the user
   - 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.

6.10.2. When you are liable for loss

If the **section 6.10.1 - When you are not liable for loss** does not apply, you may only be made liable for losses arising from an unauthorised transaction in the circumstances specified in this section.

A. When we can prove on the balance of probability that a user contributed to a loss through fraud, or breaching the passcode security requirements (refer to **section 2 – Protecting your accounts**):
   - 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
   - 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.

B. When:
   - more than one passcode is required to perform a transaction, and
   - we prove that a user breached the passcode security requirements for one or more of the required passcodes, but not all of the required passcodes, you are liable under **section 6.10.2 (A)** only if we also prove on the balance of probability that the breach of the passcode security requirements under **section 2 – Protecting your accounts** was more than 50% responsible for the losses, when assessed together with all the contributing causes.

C. 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.

D. When 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:
   - 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.
   - 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 this section if you were the user who contributed to the loss, or if a different user contributed to the loss.

E. When a passcode was required to perform an unauthorised transaction, and **sections A to D** above do not apply, you are liable for the least of:
   - $150, or a lower figure determined by us
   - 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

- 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.

F. In deciding whether on the balance of probabilities we have proved that a user has contributed to losses under **section A to D**:
   - we must consider all reasonable evidence, including all reasonable explanations for the transaction occurring
   - 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
   - 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.

G. 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 this section 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 section 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 section for a greater amount than would apply if we had exercised those rights.

6.11. Liability for loss caused by system or equipment malfunction

- 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.
- When 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:
  - correcting any errors
  - refunding any fees or charges imposed on the user.

7. Managing your accounts

7.1. Account statements

Statements will be automatically issued quarterly. We may provide account statements electronically for you to retrieve via internet or mobile banking, your data sharing dashboard or in some instances via email unless:

- you request that statements be sent in paper form
- you have not registered for internet or mobile 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.

Paper statements are not available for the Online Saver product. When we provide paper statements, you may be charged a fee. Refer to our Fees & Charges Schedule.

We recommend that you check your account statement as soon as you receive it. Immediately contact us to report any unauthorised transactions or errors.

7.2. Overdrawn accounts

There is no overdraft facility on our accounts, with the exception of our Legacy Overdraft account, and you must not overdraw your account. You must keep sufficient cleared funds in your account to cover any fees or charges, direct debit, PayTo or other scheduled payments and any fees. If you do not, we can dishonour the transaction and charge dishonour fees. Refer to our Fees & Charges Schedule.

If your account is overdrawn and you have multiple accounts with us, we may apply a deposit balance from another account to clear the overdrawn amount. We'll let you know if we do this (but we do not need to provide notice in advance).

7.3. Inactive accounts

If no transactions are carried out on your account for at least 12 months (other than transactions initiated by Australian Military Bank, such as crediting interest or debiting fees and charges) we may charge an inactive fee (refer to the Fees and Charges Schedule for details).

7.4. 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 (refer to the Fees and Charges Schedule for details)
- stop paying interest or reduce the amount of interest,
- close your account (or combine it with other accounts in your name).

If your account remains dormant for 7 years (excluding accounts for minors), we have a legal obligation to remit balances exceeding $500 to the Australian Securities and Investment Commission (ASIC) as unclaimed money. We can assist you in making a claim for return of unclaimed monies which have been remitted to ASIC from your account.

7.5. Closing or suspending accounts

You can close an account at any time. Before closing an account you are responsible for ensuring:

- the account balance is $0.00,
- you cancel any scheduled payments or direct debits to or from the account, and

- you don't have outstanding transaction charges pending.

You will have to surrender any Visa Card at the time. We may defer closure and withhold sufficient funds to cover payment of outstanding transactions costs and fees, if applicable.

We may close or suspend an account or access service (such as your Visa Card, internet and mobile banking, BPAY, Osko or PayTo) if:

- you breach these Terms and Conditions,
- the account is considered dormant due to lack of activity or it has a negative balance,
- we suspect fraud or other security concerns
- you, or someone acting on your behalf, is being fraudulent
- we suspect that you are using an access facility in a manner that is likely to affect our ability to continue providing the service to you or our other members.

We will generally provide you at least 14 days notice if we are closing an account and will pay you the balance of your account. However, in some circumstances we may close or suspend an account (including limiting account facilities, delaying or not processing transactions) without notice when it is reasonable, such as to protect you from potential harm or loss (e.g. scams) or comply with our legal and regulatory obligations (including our own policies). When we suspend your account it means that you will not be able to transact on your account.

Alternatively, we may block a proposed transaction (or type of transaction) on your account, rather than stopping all transactions on your account, or suspend your card. We may place a stop on your account, suspend your card or block a transaction (or type of transaction) if:

- you breach, or we suspect you have breached, these terms and conditions in a manner we reasonably consider involves a material risk to us
- a third party you have appointed to access your account breaches, or we suspect they have breached, these terms and conditions or the terms of their appointment conditions in a manner we reasonably consider involves a material risk to us or to you
- you do not provide us with any information that we have reasonably asked you to provide and we reasonably consider creates a material risk to us or prevents us from complying with our legal or regulatory obligations or compliance policies
- we are notified of your death, bankruptcy, insolvency or loss of capacity
- you are the recipient of a mistaken payment into your account, however, limited to preserving funds in the account to the value of the mistaken payment
- we reasonably believe it necessary in order to prevent the occurrence of fraud or unlawful transactions
- we reasonably believe your account or PayID is being used in a way that may cause loss to you or us (including, without limitation, where unauthorised transactions have been reported on the account)
- we know, or reasonably suspect, or you advise us that, your Card, Card Details, PayID, Device, Passcode, Account and/or PIN are no longer secure, or are being or will be used for fraudulent or unlawful transactions
- your account has a negative (debit) balance
- we become aware of any dispute which we reasonably believe has a bearing on the account until this dispute has been resolved to our reasonable satisfaction (for example, a dispute as to who may operate or owns the account)
- we become aware of a technical issue with your account, card or card details, which requires us to cease any transaction on the account and/or to close your account
- you behave in a way towards our staff, our service providers or other customers that we reasonably consider to be inappropriate
- we are entitled to under, or required to by, law (including, without limitation, any Anti-Money Laundering or Counter-Terrorism Financing laws and sanctions) or a court order.

8. Communicating changes

We may change fees, charges, interest rates (other than fixed term deposit rates) and other conditions from time to time. The following table sets out the notice period we'll provide you before making a change.

Type of change	Notice provided
Introducing a new fee or increase an existing one	30 days in advance
Changing the minimum balance to which an account keeping fee applies	30 days in advance
Reducing the number of fee-free transactions permitted on your account	30 days in advance
Interest rate changes	On the day of change
Changing they way in which interest is calculated, charged or applied to your account	20 days in advance
Increasing your liability for losses relating to electronic transactions	30 days in advance
Electronic daily transaction limits	20 days in advance
Changing or removing an account special feature	20 days in advance
A change required because of an immediate need to restore or maintain the security of a system or an individual account, including the prevention of criminal activity	When we next communicate with you
Cancelling your Visa card, access to internet and mobile banking, BPAY®, Osko or PayTo for any reason (which does not need to be specified)	30 days in advance
Closing an account (initiated by us)	14 days
Changing any other terms and conditions	When we communicate with you next

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

Depending on the change, we may notify you by:

- internet or mobile banking notification
- email to the email address you've provided
- letter by post to the address you've provided us
- SMS to the mobile phone number you've provided
- a notice on your next account statement
- a notice on our website and/or
- a notice in a national or local newspaper.

You must let us know immediately if you change your name or contact details (including email address or mobile phone number). You can update your details using internet and/or mobile banking, when visiting a branch or by calling us.

9. 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.

There is no fee for making a complaint.

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 (Monday to Friday, 8am to 6pm, Sydney time)
In person: at any one of our branches
In writing: Member Resolution Team, 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 at **australianmilitarybank.com.au/disclosuredocuments**.

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: 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: cobccc.org.au
Email: info@codecompliance.org.au
Telephone: 1800 931 678

10. Definitions

access facility means an arrangement through which you can perform transactions on an account
account means your account with us
account holder means the person or persons in whose name the account is held
additional cardholder means a person other than the account holder who has been nominated by an account holder to operate the account by Visa card
AFCA means the Australian Financial Complaints Authority
ATM means automatic teller machine
business day means a day that is not a Saturday, a Sunday or a public holiday or bank holiday in the place concerned
card means the Visa Card you can access your account via an ATM or point of sale terminal
device means a device we give to a user that is used to perform a transaction. Examples include:

- ATM card
- Visa Card, whether physical or digital
- token issued by a subscriber that generates a passcode
- contactless devices

digital wallet provider is the service provider who enables you to access your Visa Card to make purchase through your device such as Apple Pay, Google Pay, etc.
EFTPOS means electronic funds transfer at the point of sale—a network for facilitating transactions at point of sale
identifier means information that a user:

- may know but is not required to keep secret, and
- 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.

lock in relation to a PayID, means the temporary suspension of a PayID in the PayID Service.
manual signature means a handwritten signature, including a signature written on paper and a signature written on an electronic tablet
mandate management service means the central, secure database operated by NPP Australia Limited of Payment Agreements
merchant means a merchant with which you have established, or would like to establish, a Payment Agreement
NPP means the New Payments Platform operated by NPP Australia Limited.
NPP payment means an electronic payment cleared and settled by participating financial institutions via the NPP
one time passcode (OTP) 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 to that account holder by their preferred communication method such as SMS or email
Osko payment means an NPP Payment made through the Osko payment service offered by BPAY Pty Ltd.
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
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:

- personal identification number (PIN)
- internet banking password
- mobile banking passcode
- secret question
- code generated by a physical security token
- code provided to a user by SMS, email or in a mobile application
- one-time passcodes

A passcode does not include a number printed on a device (e.g. a security number printed on a Visa Card).

PayID means the identifier that you choose in order to receive NPP Payments into your Account.
PayID name means the name we give you to identify you to payers (for example, your full name or entity name).
PayID service means the service, provided via the NPP, through which NPP Payments can be made and received by use of a PayID.
PayID type means the type of PayID you select, which, subject to availability, may be your mobile number, email address, Australian company number, Australian business number or Organisation ID.
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
pay anyone banking facility means a facility when 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
privacy law means the Privacy Act 1988 (Cth) and any regulations made under that Act.
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
unauthorised transaction means a transaction that is not authorised by you and occurs when a transaction has been made without your knowledge or consent. 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.
we, us or our means Australian Military Bank Limited
you, your or yours means you as the account holder (or any additional signatories / cardholders for your account).

Australian Military Bank

Contact us

- 1300 13 23 28
- Visit your local branch
- service@australianmilitarybank.com.au
- australianmilitarybank.com.au

AMB-202-290324

ABN 48 087 649 741 | AFSL and Australian Credit Licence No. 237 988