

Account and access facility

Conditions of use

1 July 2024

Issued by Bank Australia Limited
ABN 21 087 651 607 AFSL 238431
Bank Australia
Locked Bag 2035
Collingwood VIC 3066 Australia
Telephone 132 888



Contents

1. Introduction	7
1.1 About this document	7
1.2 How our conditions of use become binding on you	7
1.3 We follow the Banking Codes of Practice	7
1.4 We comply with the ePayments Code	7
1.5 Privacy	7
1.6 Accessing copies of conditions of use	8
1.7 Financial claims scheme	8
1.8 How to contact us	8
2. Opening a Bank Australia account and access facility	9
2.1 What is the Bank Australia account and access facility?	9
2.2 How do I open an account?	9
2.3 Proof of identity required	9
2.4 Joint Accounts	10
2.5 Trust accounts	11
2.6 Accounts for children	11
2.7 Government Charges	11
2.8 What interest can I earn on my account?	11
2.9 What are the taxation consequences?	12
2.10 Tax File Number (TFN)	12
2.11 Third party access	12
3. Using a Bank Australia account and access facility	13
3.1 Making deposits to the account	13
3.2 Deposits using electronic equipment	13
3.3 Depositing cheques drawn on Australian banks	13
3.4 Withdrawing or transferring from the account	14
3.5 Over the counter withdrawals	14
3.6 Fraudulent payments into your accounts	14
3.7 Withdrawal limits	15
3.8 Periodic transfers to loan accounts	15
3.9 Overdrawing an account	15
3.10 Account statements	15
3.11 What happens if I change my contact details	16
3.12 What happens if I change my name?	16

3.13	Dormant accounts	16
3.14	Account combination	16
3.15	Closing accounts and cancelling access facilities	17
3.16	Notifying changes	17
3.17	How we send notices & statements	18
3.18	Cheque Clearance	18
3.19	Direct debits and Recurring Payments	19
3.20	PayPal	20
3.21	Direct credit	21
3.22	Complaints	21
3.23	The banking codes of practice we subscribe to	22
3.24	About our customer advocate	23
3.25	Financial difficulty	23
3.26	Information about your privacy	24
3.27	Use of our account and access facilities	24
4.	Electronic Banking	25
4.1	What type of transactions this section applies to	26
4.2	Information about our ePayment facilities	26
4.3	Visa Card	26
4.4	Passcode security requirements	27
4.5	Transactions	28
4.6	The access card	29
4.7	The digital card	30
4.8	Replacement of an access card	30
4.9	Round UPs	31
4.10	Using your access card details within a digital wallet	32
4.11	Using card controls on your access card	34
4.12	Using Visa outside Australia	36
4.13	Foreign currency conversion fee	37
4.14	Additional access card	37
4.15	Validity of access card	37
4.16	Cancellation of access card or access to internet banking service, Osko, PayTo or BPAY®	38
4.17	Consequences of suspension or termination	39
4.18	Exclusions of access card warranties and representations	40
4.19	Using internet banking	40
4.20	How to report loss, theft or unauthorised use of your access card, passcode or digital wallet	40

4.21	How to report unauthorised use of internet banking	41
4.22	Using BPAY®	41
4.23	Processing BPAY® payments	41
4.24	Future-dated BPAY® payments	43
4.25	Consequential damage for payments	43
4.26	Regular payment arrangements	44
4.27	Osko	44
4.28	Using Osko	45
4.29	Choosing a PayID and PayID Name	45
4.30	Transferring your PayID to another account	47
4.31	Transferring your PayID from another account	47
4.32	Locking your PayID	47
4.33	Closing your PayID	48
4.34	Processing Osko Payments	48
4.35	Notifications of Osko Payments	49
4.36	Mistaken or misdirected payments from your account	49
4.37	Mistaken or misdirected payments into your account	49
4.38	Future-dated Osko Payments	50
4.39	Consequential damage for Osko Payments	50
4.40	Changes to Osko	50
4.41	Privacy	51
4.42	Net Position View	51
4.43	Spend Tracker	51
4.44	Creating a PayTo Payment Agreement	52
4.45	Amending a Payment Agreement	53
4.46	Pausing your Payment Agreement	54
4.47	Transferring your Payment Agreement	54
4.48	Cancelling your Payment Agreement	55
4.49	Migration of Direct Debit arrangements	55
4.50	General	55
4.51	Privacy	58
4.52	Authority	58

5.	Other things you need to know	59
5.1	Third party payment services	59
5.2	Inward Telegraphic Transfers	59
5.3	Outward Telegraphic Transfers	59
5.4	When you are not liable for loss	61
5.5	When you are liable for loss	62
5.6	Liability for loss caused by system or equipment malfunction	63
5.7	Network arrangements	64
5.8	Mistaken internet payments	64
5.9	Money laundering and illegality	68
5.10	Request for Documents	69
5.11	Instructions to Us	69
6.	Specific terms applicable to accounts	70
6.1	Mortgage Offset Account	70
7.	Definitions	72

1. Introduction

1.1 About this document

This document, the Deposit Fees, charges and transaction limits brochure, and the Summary of accounts & availability of access facilities brochure, form your terms and conditions for your Account and Access Facility.

1.2 How our conditions of use become binding on you

As soon as you open an account or use an access facility you become bound by these conditions of use.

Other terms and conditions, including those implied by law, also apply. To the extent permitted by law, these terms and conditions shall prevail in the event of any inconsistency. If the law implies terms and conditions which cannot be excluded. Our liability under those implied terms and conditions will be limited to the maximum extent permitted by law.

1.3 We follow the Banking Codes of Practice

We are bound by the Customer Owned Banking Code of Practice.

We are also bound by the Australian Banking Association Code of Banking Practice which will apply to you if you are an individual, small business or guarantor (as defined in that Code).

Please see section 3.23 for further information about the Codes of Practice we subscribe to.

1.4 We comply with the ePayments Code

We warrant that we will comply with the ePayments Code.

1.5 Privacy

Please refer to section 3.26 in this document for details about:

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



1.6 Accessing copies of conditions of use

Please keep these conditions of use in a safe place so you can refer to it when needed. Alternatively, you can view and download our current conditions of use from our website at bankaust.com.au

1.7 Financial claims scheme

The Financial Claims Scheme (FCS) protects depositors through the provision of a guarantee on deposits (up to the cap of \$250,000) held in authorised deposit-taking institutions (ADIs) incorporated in Australia and allows quick access to their deposits if an ADI becomes insolvent.

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

1.8 How to contact us

Call 132 888

Overseas: +61 3 9854 4666

Email: mail@bankaust.com.au

Visit us in one of our branches

Secure mail through internet banking/Bank Australia app



2. Opening a Bank Australia account and access facility

2.1 What is the Bank Australia account and access facility?

The Bank Australia account and access facility is a facility that gives you transaction, savings and term deposit accounts as well as these facilities for accessing accounts:

- Visa Card
- Osko and BPAY® (registered to BPAY® Pty Ltd ABN 69 079 137 518)
- internet banking (including Bank Australia app)
- EFTPOS and ATM access
- direct debit
- PayTo
- Bank@Post™.

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

2.2 How do I open an account?

To open an account apply online at www.bankaustralia.com.au. Alternatively you can visit a branch or call us on 132 888 to open an account over the phone, internet banking or Bank Australia app.

Please first check the Summary of Accounts & Availability of Access Facilities brochure for the different account types available, any special conditions for opening, and the features and benefits of each account type.

2.3 Proof of identity required

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

In most cases you can prove your identity by showing us one of the following photo identity documents:

- current Australian driver's licence
- current Australian passport (or one that has expired within the last 2 years)
- a proof of age card which contains a photograph issued by an Australian State or Territory.

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

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

2.4 Joint Accounts

A joint account is an account held by two or more persons. If the option is available on the account, it's important for you to understand your responsibilities as a joint holder. They include:

- if one joint holder dies, the surviving joint holder(s) automatically takes ownership of the account, including any credit balance.
- each joint holder is individually liable for any amount owing and has the right to any credit balance in the account, jointly and severally with the joint holder.
- a joint account can be operated on an 'all to sign' or 'either/or to sign' basis:
 - 'all to sign' means all joint holders must instruct us to carry out an instruction on the account
 - 'either/or to sign' means any joint holder can operate the account independently of the other joint holder.

No matter which operation authority applies to the joint account, any joint holder acting on their own being able to:

- change the account from sole operation ('either/or to sign') to joint operation ('all to sign')
- change the delivery of account statements (i.e. from electronic to paper) in so far as it relates to them
- changing the account address in so far as it relates to them
- place a stop on the joint account.

Each joint holder may be able to see messages and notifications associated with payments to the joint account.

Unless we have specific instructions that the account is 'all to sign', it will be operated as 'either/or to sign'. This means all joint holders can access the account and transact independently of each other.



If we are notified of a dispute on a joint account, we may, in our absolute discretion:

- require all joint holders to operate the account. If this occurs, we may require all or specific future transactions to be authorised by all joint holders. We may also revoke or restrict access to services including for example, an Access Card or electronic banking.
- place a stop on the account. This means that joint holders will be unable to transact on the joint account and do, for example, the following things:
 - deposit money to the joint account;
 - withdraw money from the joint account; or
 - request any other changes to the account e.g. switching the account type.

We may, in our discretion, make exceptions to these rules from time to time.

2.5 Trust accounts

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

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

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

2.6 Accounts for children

Account holders aged 13 years and over may open an account. Please refer to the Summary of Accounts & Availability of Access Facilities brochure for available account types.

2.7 Government Charges

We will debit your primary operating account for all applicable government taxes and charges. These charges may vary according to State or Territory.

2.8 What interest can I earn on my account?

Our Interest Rates brochure provides information about our current deposit and savings interest rates. Our website also has information about our current deposit and savings interest rates. We may vary deposit or savings interest rates from time to time on all deposit accounts. Term Deposit interest rate is fixed at the time of the initial deposit and for the full term.

Our Summary of Accounts & Availability of Access Facilities brochure discloses how we calculate and credit interest to your account.



2.9 What are the taxation consequences?

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

2.10 Tax File Number (TFN)

Government legislation states that all accounts earning deposit interest in a tax year may be subject to Tax File Number (TFN) legislation. We will ask you whether you want to disclose your Tax File Number or exemption. If you disclose it, we will note your TFN or TFN exemption against any account you activate in line with the Privacy Act. Businesses may only quote their ABN instead of a TFN.

You do not have to disclose your TFN or ABN to us. For a joint account, each joint holder may quote their TFN and/or exemptions. If each joint account holder does not quote their TFN and/or exemptions, we may deduct Withholding Tax from interest paid on the account at the highest marginal tax rate (plus the Medicare levy).

If you reside outside Australia, you can disclose your non-resident tax status. Withholding Tax is then deducted at the rate of 10% of any interest earned.

2.11 Third party access

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

To appoint an authorised person you, together with the person you are authorising, will need to sign the relevant form. You can specify which of your accounts under the Account & Access Facility you give the authorised person authority to operate. You are responsible for all transactions your authorised person carries out on your account. You should ensure that the person you authorise to operate your account is a person you trust fully.

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

3. Using a Bank Australia account and access facility

3.1 Making deposits to the account

You can make deposits to the account:

- by cash at any branch
- by direct credit, e.g. from your employer for wages or salary – please note that we can reverse a direct credit if we do not receive full value for the direct credit
- by transfer from another account with us via internet banking or Bank Australia app
- by transfer from another financial institution
- by cash or cheque at a National Australia Bank branch using a specially encoded deposit book
- via Australia Post Bank@Post™
- by cash or cheque via Australia Post Bank@Post™

unless otherwise indicated in the Summary of Accounts & Availability of Access Facilities brochure. In processing deposits to your account, we will rely on your account number only. We will not check the account name received with the deposit instructions.

3.2 Deposits using electronic equipment

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

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

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

3.3 Depositing cheques drawn on Australian banks

NAB Deposit Books are no longer used, Bank@Post™ is the only way for customers to deposit cheques.



3.4 Withdrawing or transferring from the account

Unless otherwise indicated in the Summary of Accounts & Availability of Access Facilities brochure, you can make or authorise withdrawals from the account:

- over the counter at any branch
- by direct debit
- by Osko and PayTo
- via internet banking or Bank Australia app
- via BPAY® to make a payment to a biller
- at ATMs, if your account is linked to an access card
- via EFTPOS terminals, if your account is linked to an access card (note that merchants may impose restrictions on withdrawing cash).

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

3.5 Over the counter withdrawals

You can make over-the-counter withdrawals in cash. Please check:

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

3.6 Fraudulent payments into your accounts

Where a sending financial institution advises, or we reasonably believe, that a payment made into your account is a fraudulent, suspicious or illegal payment, you authorise us to, without further notice, deduct from your account an amount up to the original amount of the believed fraudulent, suspicious or illegal payment and return it to the original sending financial institution and we will incur no liability to you in doing so.

3.7 Withdrawal limits

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

These transaction limits are set out in the Deposit Fees & Charges and Transaction Limits brochure.

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

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

A contactless transaction made on a Visa Debit Access Card, may be processed as either an EFTPOS Transaction or Visa transaction. This is at the discretion of the Merchant. Non-cash transactions, including all purchases made via the EFTPOS network, do not count toward your daily cash withdrawal limit.

3.8 Periodic transfers to loan accounts

When you give us a periodic payment authority to transfer a loan repayment from an account to credit your loan account, you authorise us to increase or decrease the amount of the periodic payment to allow for any repayment variation we have notified you of in accordance with the loan contract.

3.9 Overdrawing an account

You must keep sufficient Cleared funds in your account to cover your transactions. If you do not, we can dishonour the transaction.

Alternatively, we can honour the transaction and overdraw your account.

We will charge you:

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

If we honour the transaction, the transaction will operate as your request to us to provide you with short term credit repayable within 7 days.

'Cleared funds' means the proceeds of cheque deposits to your account once the cheque is cleared, cash deposits and direct credits via Osko, Swifts and Telegraphic Transfer.

3.10 Account statements

We will send you account statements either monthly or quarterly, depending on your account. You can also ask us for an a statement at any time, however we may charge a fee for providing additional statements or copies: see the Deposit Fees, Charges and Transaction Limits brochure for more information.



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

For all other accounts, when we activate your internet banking account we will automatically set the delivery of your statements to electronic. You can request to change back to paper based statements at any time. We may charge you a fee for paper based statements: see the Deposit Fees, Charges and Transaction Limits brochure.

We recommend that you check your statement as soon as you receive it and immediately notify us of anything you think is wrong.

3.11 What happens if I change my contact details

If you change your address, phone number or email address, please let us know immediately, so that we can continue to contact you alternatively you can update address or phone number via Internet Banking. If you do not update your contact details any correspondence sent to your old address is still considered 'notice in writing'.

3.12 What happens if I change my name?

To update your name on your accounts you will need to visit a branch with your identification documents, and the details of your name change.

3.13 Dormant accounts

If no transactions are carried out on your account for at least 10 months (other than transactions initiated by Bank Australia, such as crediting interest or debiting fees and charges) we may write to you asking if you want to keep the account open. If you do not reply within 20 business days, we will treat your account as dormant.

Once your account becomes dormant, we may:

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

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

3.14 Account combination

If you have more than one account with us, and one of those accounts is overdrawn, over limit or in arrears, we may transfer money from one of your other accounts into this one to resolve this.

We will not combine accounts if to do so would breach the Code of Operation: Recovery of Debts from Customer Nominated Bank Accounts in receipt of Services Australia income support payments or Department of Veterans Affairs' payments, the ABA Banking Code of Practice or the Customer Owned Banking Code of Practice.

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

3.15 Closing accounts and cancelling access facilities

You can close your Bank Australia Account and Access Facility at any time. However, you will have to surrender your access card at that time. If you have not destroyed or returned your card to us, you will remain responsible for transactions you make where the merchant is not required to get authorisation.

We may defer closure and withhold sufficient funds to cover payment of outstanding electronic transactions and fees, if applicable.

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

We can where we consider it reasonably necessary for the prudent administration of the bank:

- close the Account and Access Facility in our absolute discretion by giving you at least 14 days' notice and paying you the balance of your account; or
- cancel any access facility for other reasons as set out in these Conditions of Use.

3.16 Notifying changes

We may change fees, charges, interest rates and other conditions. The following table sets out the minimum notice period we will provide to you prior to any change being implemented. Your use of the account after the expiry of the notice period is deemed acceptance by you of the changes contained in that notice.

Type of change	Minimum notice period
Increasing any fee or charge	30 days
Adding a new fee or charge	30 days
Reducing the number of fee-free transactions permitted on your account	30 days
Changing the minimum balance to which an account keeping fee applies	30 days
Changing the method by which interest is calculated	30 days
Changing the circumstances when interest is credited to your account	30 days
Changing deposit interest rates	on the day of change
Increasing your liability for losses relating to ePayments	30 days
Imposing, removing or changing any periodic transaction limit	30 days
Changing any other term or condition	on the day of change

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

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

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

We will always select a method(s) appropriate to the nature and extent of the change, as well as the costeffectiveness of the method of notification.

3.17 How we send notices & statements

We may send you notices and statements:

- by post, to the address recorded in our records or to a mailing address you nominate
- by fax
- by email
- by sms
- via digital banking, secure mail or Bank Australia App
- by advertisement in the media, for some notices only
- by other means we agree with you.

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

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

3.18 Cheque Clearance

Cheques are only accepted via Australia Post Bank@Post™ or National Australia Bank branches. You should allow 7 to 10 working days from the time you deposit the cheque in your account until the proceeds are available as cleared funds.

3.19 Direct debits and Recurring Payments

This section relates to Direct Debits under the BECS Procedures, and Recurring Payment Authorities. It does not apply to payments and arrangements under the PayTo service (for PayTo services see sections 4.44 to 4.52).

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.

A Recurring Payment is a payment that you have authorised to be taken directly from your Visa debit card or credit card. In order to authorise this, you will be required to sign a Recurring Payment Authority (RPA).

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

To cancel the RPA, you are required to contact the biller to arrange another payment option or cancel it all together. If you contact us we will promptly submit a request to stop the facility.

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

If you set up the payment on your access card via an RPA, please contact us directly about unauthorised or irregular debits.

If you have insufficient funds in your nominated account, we may dishonour your direct debit. However, we have discretion to allow the direct debit to be paid and to overdraw your account or transfer funds from another account in your name for this purpose. If you overdraw your account, we will charge you interest and fees. Please refer to section 3.9 for further information.

If the account information you provide is incorrect your direct debit may be rejected.

We can immediately cancel or suspend your direct debit facility (including any recurring payments you have authorised to be debited from your Visa debit card), as we reasonably consider appropriate in the circumstances if:

- three consecutive direct debit instructions are dishonoured
- we suspect any direct debit payments may be fraudulent
- for security reasons, where we suspect your account has been compromised or is at risk of being compromised
- your account is overdrawn and you have not corrected that overdrawn position in accordance with the terms and conditions of your account
- you are in default of the terms and conditions of your account and you have not rectified that default in the time specified in any notice to remedy the default
- we are required to by law
- you suffer an Insolvency event
- you or a joint account holder becomes deceased or
- your account becomes dormant.

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.

3.20 PayPal

When you use PayPal you are authorising PayPal to debit amounts from your account as a biller under Direct Debit. Please note that:

- you are responsible for all PayPal debits to your account
- if you dispute a PayPal debit, you can contact PayPal directly or ask us to do so
- we are not responsible for compensating you for any disputed PayPal debit, or for reversing any disputed PayPal debit to your account
- if you want to cancel your direct debit arrangement with PayPal, you can contact PayPal directly or ask us to do so
- when you ask us to pass on a disputed transaction to PayPal, or you request us to cancel your direct debit arrangement with PayPal, we will do so as soon as practicable but we are not responsible if PayPal fails to respond as soon as possible or at all.

Other third party payment services may operate in a similar way to PayPal.

3.21 Direct credit

You can arrange for a third party to electronically deposit (direct credit) funds to your Bank Australia account by providing your BSB (313-140) and account number.

Although the third party may request 'the account name', it will not be used to verify if the account details are correct. If the account information you provide is incorrect your direct credit may be rejected or credited to an incorrect account.

Bank Australia is not liable for any loss incurred as a result of:

- rejected direct credits due to incorrect account information being used by a third party,
- funds credited in error to accounts due to incorrect account information being used by a third party and subsequently recalled by the sending financial institution.

To change the direct credit you must contact the third party responsible for depositing funds to your account.

If you believe a direct credit has been incorrectly deposited to your account, you should notify Bank Australia immediately.

3.22 Complaints

At Bank Australia we want every experience you have with us to be a good one. So if we have fallen short of your expectations, please let us know and we will do what we can to fix it as quickly as possible. You can raise your complaint with our staff personally over the counter, by telephone, in writing by letter or email.

If a staff member is unable by reason of authority or experience to handle the matter, it will be referred to a more senior or experienced person. In the majority of cases, your complaint will be dealt with promptly and to your satisfaction, and you will not need additional assistance.

However, you may refer the complaint to our Resolution Team who will independently investigate and review your complaint. For further information on our resolution process, refer to our Complaints and Dispute Resolution Guide available at bankaust.com.au.

If you are not satisfied with the way in which we handle your complaint, you are entitled to have your complaint resolved free of charge by the Australian Financial Complaints Authority (AFCA).

AFCA can be contacted by:

Website: www.afca.org.au
Email: info@afca.org.au
Phone: 1800 931 678 (free call)
In writing to: Australian Financial Complaints Authority,
GPO Box 3, Melbourne VIC 3001



3.23 The banking codes of practice we subscribe to

The Customer Owned Banking Code of Practice (COBCOP)

Mutual banking delivers customer-focused, competitive services. Mutual banks, credit unions and mutual building societies are customer-owned financial institutions committed to putting their customers first.

The Customer Owned Banking Code of Practice, the code of practice for mutual banks, credit unions and mutual building societies, is an important public expression of the value we place on improving the financial wellbeing of our customers and their communities.

You can download a copy of the Customer Owned Banking Code of Practice from our website.

If you have a complaint about our compliance with the Customer Owned Banking Code of Practice you can contact:

Customer Owned Banking Code Compliance Committee

PO Box 14240 Melbourne VIC 8001
Phone: 1800 367 287
Email: info@codecompliance.org.au

Please be aware that the Committee is not a dispute resolution body and cannot provide financial compensation.

Australian Banking Association (ABA) Code of Banking Practice

Effective 1 July 2019, we are a subscriber to the revised Australian Banking Association (ABA) Code of Banking Practice.

This code sets standards of practice and service in the banking industry, when dealing with individual or small business customers, prospective customers and their guarantors.

The Code is underpinned by a statement of guiding principles which provide an ethical, customer orientated and sustainable framework. These principals include:

- Trust and confidence
- Integrity
- Service
- Transparency and accountability

Further information about the Code of Banking Practice is available at the Australian Banking Association website.

You can download a copy of the code from our website.

If you have a complaint about our compliance with the Code of Banking Practice, you can contact:

Banking Code Compliance Committee
PO Box 14240 Melbourne VIC 8001
Phone: 1800 931 678
Email: info@codecompliance.org.au



3.24 About our customer advocate

Our Customer Advocate is responsible for ensuring that customer complaints are responded to in a thorough, timely and fair manner. The Customer Advocate is independent from the Bank's dispute resolution team and works across the Bank to provide advice and identify where improvements can be made to help us meet our commitments to customers.

If you need to get in touch with our Customer Advocate, you can email customeradvocate@bankaust.com.au.

3.25 Financial difficulty

We understand that life is unpredictable and circumstances can change.

A variety of life events and changes to circumstance can put a significant strain on your finances and make it difficult to meet your financial obligations – but we're here to help.

If you get into financial difficulty, the sooner you let us know, the sooner we can work with you to help you get back on your feet.

We have a Hardship Assistance team who are available to help you. You can either:

- Call customer support on 132 888
- Talk to a consultant at any of our branches
- Visit our website <https://bankaust.com.au/hardship>



3.26 Information about your privacy

Your privacy is important to us. In handling your personal information, we are committed to complying with the *Privacy Act 1988* (Cth), the Australian Privacy Principles set out in the *Privacy Act 1988* (Cth) and the Banking Codes of Practice.

You may obtain a copy of our Privacy and Credit Reporting Policy by:

- visiting our website at bankaust.com.au
- calling us on 132 888
- asking at any of our branches.

Our Privacy and Credit Reporting Policy explains our commitment to the protection of your personal information and contains information about how you may complain about a breach of the *Privacy Act 1988* (Cth), and the process by which your complaint will be handled.

As a bank, we also have a general duty of confidentiality towards you, except in the following circumstances:

- where disclosure is compelled by law
- where there is a duty to the public to disclose
- where the interests of the bank require disclosure and
- where disclosure is made with your express consent.

3.27 Use of our account and access facilities

You and an authorised user may not use our access facilities to engage in conduct that, in our opinion:

- is offensive or inappropriate;
- is unlawful;
- is defamatory, harassing or threatening to any person;
- threatens, promotes or encourages physical or mental harm of any person;
- threatens, promotes or encourages violence against any person; or
- threatens, promotes or encourages terrorism.

4. Electronic Banking

Important information about protecting your access card and passcodes:

- sign the access card as soon as you receive it.
- familiarise yourself with your obligations to keep your access card and passcodes secure.
- familiarise yourself with the steps you have to take to report loss or theft of your access card or to report unauthorised use of your access card or through your account. Immediately report to us loss, theft or unauthorised use.
- if you change a passcode, do not select a passcode which represents your birth date or a recognisable part of your name.
- never write the passcode on the access card.
- never write the passcode on anything which is kept with or near the access card.
- never lend the access card to anybody.
- never tell or show the passcode to another person.
- use care to prevent anyone seeing the passcode being entered on a device.
- keep a record of the Visa card number and the Visa Card Hotline telephone number for your area with your usual list of emergency telephone numbers.
- check your account statements regularly for any unauthorised use.
- immediately notify us when you change your address, and ensure your contact details, including email address and mobile phone number, are correct and up to date at all times.
- always access internet banking only using the OFFICIAL URL addresses.
- NEVER access internet banking via a link in an email, SMS or other electronic message.
- if accessing internet banking on someone else's PC, laptop, tablet or mobile phone, ALWAYS DELETE your browsing history.
- always reject any request to provide or to confirm details of your passcode. We will NEVER ask you to provide us with these details.

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

These guidelines provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised payments. Liability for such transactions will be determined in accordance with the Conditions of Use and the ePayments Code.



4.1 What type of transactions this section applies to

This section applies to:

- payment, funds transfer and cash withdrawal transactions that are initiated using electronic equipment and not intended to be authenticated by comparing a manual signature with a specimen signature
- electronic card transactions, including ATM, EFTPOS, credit card and debit card transactions that are not intended to be authenticated by comparing a manual signature with a specimen signature
- bill payment transactions
- internet banking transactions, including pay anyone banking facility transactions
- online transactions performed using a card number and expiry date
- online bill payments (including BPAY®)
- direct debits
- PayTo
- transactions using mobile devices

Unless the account services are provided or referred to you by Bank Australia, Bank Australia does not authorise, promote or endorse the use of account services offered by third parties to access your Bank Australia accounts.

4.2 Information about our ePayment facilities

You should follow the guidelines set out in the grey box on the previous page to protect against unauthorised use of your access card and passcode. These guidelines provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised transactions. Liability for such transactions will be determined in accordance with this section 4, and the ePayments Code.

4.3 Visa Card

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

- check your account balances
- withdraw cash from your account
- transfer money between accounts
- deposit cash or cheques at Bank@Post™ outlets
- purchase goods and services.

We may choose not to give you a Visa Card if, in our reasonable opinion, your banking history with us is not satisfactory.

You may be able to reverse a transaction

Where you have used your access card to purchase goods or services, you may be entitled to reverse (chargeback) the transaction where you have a dispute with the merchant in certain limited situations. Strict timeframes apply to our ability to claim a chargeback on your behalf. You must notify us promptly if you believe you are entitled to reverse a transaction. If it is determined that you are entitled to reverse a transaction, we will credit your account for the amount initially debited for the transaction. You can also dispute any transaction that you did not authorise. Please see section 5.4 “When you are not liable for loss” for more information.

You should inform us as soon as possible if you become aware of circumstances which might entitle you to a chargeback and let us have the cardholder’s copy of the Visa transaction receipt in question.

4.4 Passcode security requirements

This section applies where one or more passcodes are needed to perform a transaction.

A user must not:

- voluntarily disclose one or more passcodes to anyone, including a family member or friend
- where a device is also needed to perform a transaction, write or record passcode(s) on a device, or keep a record of the passcode(s) on anything:
 - carried with a device
 - liable to loss or theft simultaneously with a device unless the user makes a reasonable attempt to protect the security of the passcode
 - where a device is not needed to perform a transaction, keep a written record of all passcodes required to perform transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the passcode(s).

Note: If you or another user breaches these passcode security requirements, we may not be required to indemnify you for loss arising from that breach. See section 5.5.



For the purpose of the above, a reasonable attempt to protect the security of a passcode record includes making any reasonable attempt to disguise the passcode within the record, or prevent unauthorised access to the passcode record, including (but not limited to) by:

- hiding or disguising the passcode record among other records
- hiding or disguising the passcode record in a place where a passcode record would not be expected to be found
- keeping a record of the passcode record in a securely locked container
- preventing unauthorised access to an electronically stored record of the passcode record.

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

An example of extreme carelessness is storing a user name and passcode for internet banking in a diary, computer or other personal electronic device that is not password protected.

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

- specifically instructed the user not to do so
- warned the user of the consequences of doing so.

The onus is on us to prove, on the balance of probability, that we have taken the actions mentioned in the above paragraph.

Where we expressly authorise particular conduct by a user, either generally or subject to conditions, a user who engages in such authorised conduct, does not breach our passcode security requirements. Where we expressly or implicitly promote, endorse or authorise the use of a service for accessing a facility (for example, by hosting an access service on our electronic address), a user who discloses, records or stores a passcode that is required or recommended for the purpose of using the service does not breach the passcode security requirements set out above. For these purposes, we are not taken to have promoted, endorsed or authorised a user's use of a particular service merely because we have chosen to use the service for our own purposes or have not actively prevented the user from accessing a service.

4.5 Transactions

When you or any other authorised user make a transaction with electronic equipment, it is your responsibility to tell us the correct amount you wish to pay or transfer and the correct account you wish to have the payment or transfer credited to. The 'account name' will not be used to verify if the account details are correct.

If you directed us to pay or transfer an amount that was greater than what was required, you cannot make a claim upon us. You must contact the recipient to obtain a refund.

If the account you told us to make a payment or transfer was incorrect, you can contact the recipient to obtain a refund, or contact us. We will attempt to recover the funds on your behalf (see section 4.36 “Mistaken or misdirected payments from your account’.)

If the amount you direct us to pay or transfer was less than the amount required, you can make another payment or transfer to the same recipient to make up the difference.

4.6 The access card

Subject to:

- each user having an Australian residential address when an Access Card is issued to them; and
- the Linked Account permitting it, we will issue an Access Card to you and may, at your request and in accordance with section 4.14, issue an Access Card to any Additional Cardholder you nominate.

We are a member of CUSCAL which is the principal member of Visa through which we can provide the Card.

You are liable for all Charges incurred where an Access Card is used in respect of your Linked Account, including any Charges that are incurred by an Additional Cardholder.

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

We will advise you from time to time:

- what transactions may be performed using your access card
- what ATMs of other financial institutions may be used; and
- what the daily cash withdrawal limits are.

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

If you have been issued with an access card with contactless functionality, that is identifiable by the contactless symbol, you will be able to make a transaction by holding or tapping your access card within 4cm of an electronic terminal without having to insert or swipe the card. Transactions using the contactless functionality can only be made at a participating merchant outlet and if it is under AU\$100.

If your transaction is equal to or over AU\$100, you’ll still need to enter your PIN. The same conditions apply to your contactless transactions as your other access card transactions.

You agree that the access card always remains our property.

4.7 The digital card

Subject to section 4.6 and each user having a valid electronic address when a Digital Card is issued to them, we will issue a Digital Card to you and may, at your request and in accordance with clause 4.14, issue a Digital Card to any Additional Cardholder you nominate.

If you are issued a Digital Card, the active status of your Physical Card will be the same as your Digital Card (even if you have not received your Physical Card).

A Digital Card is valid when it is issued to you, unless you are required to activate it – in which case the Digital Card will be valid when it has been activated by you.

To prevent fraudulent or unauthorised use of your Linked Account, a Digital Card will be issued with card controls in place to restrict its use. You can change these card controls but must ensure that you maintain the security of your User Device or account through which your Digital Card can be viewed or accessed.

You agree that a Digital Card is our property at all times. You must deactivate a Digital Card, remove the Card Details from any Digital Wallet to which they are registered, or remove the Digital Card from any User Device or account through which it can be viewed or accessed if we reasonably ask you to do so.

You must not modify, encode, encrypt or otherwise interfere with any Digital Card.

You agree that the Digital Wallet software is to be used solely for the purposes of registering and using a Digital Card in a Digital Wallet. You will not use the Digital Wallet software for any other purpose or distribute the Digital Wallet software in any way.

4.8 Replacement of an access card

Except where you are in breach of these terms and condition, we may at our discretion issue:

- a replacement Card to you prior to the Expiry Date shown on your current Access Card; and
- a replacement Additional Card to each Additional Cardholder prior to the Expiry Date shown on the Additional Card held by that Additional Cardholder.

We will order a replacement Card 5 weeks prior to the Expiry Date shown on the current Card. If the User has not completed a PIN authorised transaction on the Card within the 6 months prior to us ordering the replacement Card, we are under no obligation to provide a replacement Card upon expiry of the current Card.

The use of any replacement Card will at all times be subject to these Terms and Conditions.

If we issue a replacement Card you or any Additional Cardholder must ensure that the current Card and Card Details are removed from any Digital Wallet to which they are registered. In order to use the replacement Card to make payments through the Digital Wallet, the replacement Card and Card Details must first be registered on that Digital Wallet.

If you do not wish to receive a replacement Card, either for yourself or for an Additional Cardholder, you must notify us in writing 6 weeks before the Expiry Date on the current Card.

4.9 Round UPs

Round UP is an optional feature that offers an easy way to set up automatic debits of small amounts from one account and the credit that same amount into a secondary account, usually a savings account.

Example

Jane buys her weekly groceries with her Visa Debit Card, spending \$51.05. She activated Round UP to \$1.00 to help her save for her Christmas holidays. Based on that grocery shop, \$0.95 will be transferred from her Everyday Access Account to her mySaver account, replacing the old trick of putting loose change into a coin jar.

Once you have activated Round UP, every time an eligible purchase is made with your access card (including the information printed on it or a digital card), the difference between the purchase amount and the nearest \$1, \$5, \$10 (rounded up) is transferred into a secondary account that you nominate.

The access card transactions which are eligible for round up are as set out below so long as the merchant processes a contactless transaction as a Visa transaction.

Access Card Function	Is this an eligible transaction for Round UP?	Things you should be aware of in relation to Round UPs:
In-store transactions	✓	
payWave	✓	
Digital wallet	✓	
International	✓	
Online transactions	✓	
ATM Withdrawals (international)	✗	
ATM withdrawals (domestic)	✗	
BPAY®	✗	
Transfers between accounts or Fee transactions	✗	
Reversals	✗	The transfer of the Round UP amount will not be reversed
Overdraft or Unavailable funds	✗	The Round UP amount will be \$0.00 for a transaction that causes you to use an approved Overdraft Limit or exceed your available funds.

The accounts which can:

- support a round up amount debit; and
- receive a round up amount credit,

are detailed in the Summary of Accounts & Availability of Access Facilities brochure.

You (or in the case of an Account held jointly, each or either of you) can activate Round UP by accessing the Round UP menu item in your Bank Australia App. The account to receive the Round UP amount credit must be in the same name of the account which has Round UP activated, or for joint accounts, can be in either or both names of the account holders. Round UP is not available on two-to-sign accounts.

To activate Round UP you will need to nominate an account which Round UP amounts will be debited and a different account which Round UP amounts will be credited. By activating Round UP, you authorise us to debit the Round UP amount from your nominated account as a separate transaction which will ordinarily occur on the same day as the underlying purchase transaction, or in the case of a Visa transaction held as pending, on the day after it remitted and credit the Round UP amount to your nominated account as a separate transaction.

You can disable Round UP at any time via the Bank Australia App.

We may disable Round UP if your eligible Round UP account is closed or you are in material breach of these Terms. We will notify you when these events occur. This may occur by email, SMS or secure message via Internet Banking or in a manner we deem appropriate.

You can change the account which receives Round UP amount credits at any time via the Bank Australia App by first disabling Round UP then activating Round UP with your new instructions.

We may provide you the option to change the Round UP amount, at our discretion.

4.10 Using your access card details within a digital wallet

You may use a digital wallet to make contactless payments using your access card.

There may be additional terms and conditions imposed by the digital wallet provider, or the provider of a device or telecommunications service, and you are also required to comply with them.

Your ability to register an access card into a digital wallet is at our reasonable discretion. We will provide reasons if we will not or cannot register an access card into a digital wallet.

We do not guarantee that any or all merchants will accept payment using the digital wallet.

We are not liable for any loss or inconvenience incurred as a result of the refusal of any merchant to accept payment in this way.

We are not the provider of the digital wallet, and are not responsible for its use or function, including any disruption, failure, malfunction or unavailability or any security breach affecting information stored in or sent from the digital wallet. You should contact the digital wallet provider if you have questions or concerns about the digital wallet.

If you access a User Device using biometric recognition, such as a fingerprint, no passcodes will be required in order for you to make payments through the digital wallet on that User Device. To protect your linked account(s), you should ensure that:

- only your biometrics are stored in that User Device and
- that User Device, and your biometrics used in connection with that User Device, remain secure at all times.

If you, or an additional card holder:

- allow another person's biometric identifier to remain, or be, registered on a User Device; or

- share any PIN or other pass code registered to the User Device with any person,

then you are taken to have authorised that person to carry out transactions using an access card in a digital wallet on that User Device and you will be responsible for their use of the access card in the digital wallet.

We do not charge any fees for the use of a digital wallet in addition to the fees and charges that already apply to the use of an access card. Third party fees and charges may apply to the use of a digital wallet, such as those imposed by a telecommunications service for data usage and text messaging.

We can suspend or cancel the ability to use an access card to make payments using a digital wallet.

We may do so reasonably and at any time, for example, if we suspect fraud with the access card, if there is an overdue or negative balance on the access card account, if applicable laws change, if we cease to permit access cards to be used with any digital wallet, or if we are directed to do so by the digital wallet Provider or the applicable card scheme. We will notify you if we do so.

You may remove an access card from a digital wallet at any time by following the digital wallet provider's procedures for removal.

Your User Device may be linked to other devices by a common account. If so, when an access card is added to a digital wallet using the User Device, that access card may also be accessible through a digital wallet on a linked device, which may permit users of the linked device to see the access card details and make payments with that access card.

4.11 Using card controls on your access card

You must be a Bank Australia access cardholder that is registered for Internet Banking in order to access the card controls service within internet banking and within the Bank Australia app.

You may be able to use card controls in order to do the following:

Function	How the card control service works in Australia	How the card control service works Internationally	Things you should be aware of:
In-store transactions	Disabling Australian in-store transactions on your access card will block transactions made where the physical card is presented at a domestic electronic terminal at the time of processing the transaction (excluding ATMs). This will also decline Australian payWave transactions.	Disabling International in-store transactions on your access card will block transactions made where the card is physically presented at an international electronic terminal at the time of processing the transaction (excluding ATMs). This will also decline International payWave transactions.	This won't affect: <ul style="list-style-type: none"> • Digital wallet transactions • online transactions
Online transactions	Disabling Australian online transactions on your access card will block transactions processed in Australia where the card is not present. This could include (but is not limited to) online, phone, or mail order transactions where the merchant processes the transaction domestically.	Disabling International online transactions on your access card will block transactions processed by overseas merchants and transactions made in Australia (such as on Australian websites, mail orders and over the phone) where the merchant processes the transaction overseas.	This won't affect purchases made with your access card in store or with payWave.
ATM withdrawals	Disabling Australian ATM withdrawals on your access card will block cash withdrawals or cash transfers at an Australian ATM.	Disabling International ATM withdrawals on your access card will block cash withdrawals or cash transfers made at an ATM overseas.	This won't affect staff assisted or non-ATM self-service cash withdrawals/transfer made on your access card at a branch.
payWave	Disabling Australian payWave transactions on your access card will block transactions made by 'tapping' or 'waving' the card within a small distance of the domestic electronic terminal.	Disabling International payWave transactions on your access card will block transactions made by 'tapping' or 'waving' the card within a small distance of the international electronic terminal.	This won't decline transactions that are made by either inserting or swiping your access card. You will also be able to make Digital wallet transactions (i.e. using your phone to tap and pay).
Digital wallet	Disabling Australian digital wallet will block the ability to make a payment via Apple Pay, Google Pay and Samsung Pay or any other service we may offer as a mobile payment system (i.e. when you use your phone to Tap & Pay) or any other service we may offer as a digital payment system such as payment via Garmin and Fitbit or via other wearables, at a domestic electronic terminal, inside apps and on websites where the merchant processes the payment within Australia.	Disabling International digital wallet will block the ability to make a payment via Apple Pay, Google Pay and Samsung Pay or any other service we may offer as a mobile payment system (i.e. when you use your phone to Tap & Pay) at international electronic terminal, inside apps and on websites where the merchant processes the payment outside Australia.	

Function	How the card control service works both in Australia and Internationally	Things you should be aware of
Report a Card lost or stolen	By reporting your access card lost or stolen, rather than just applying a temporary block, you are irrevocably notifying Bank Australia that you wish for the access card to be cancelled. Once an access card has been reported lost or stolen the same card cannot be reactivated.	A new access card will not automatically be issued to you. A replacement card can be ordered by contacting us on 132 888, visiting a branch or sending us a secure email.
Change PIN	This refers to the access card PIN and enables you to change the PIN.	The change occurs immediately.
Temporary Card Block	Blocking your access card enables you to temporarily disable all card control indicators on the card except digital wallet. You may choose to use this card control when you have misplaced your physical access card.	Digital wallet transactions will not be blocked unless digital wallet have been set to disable after temporarily blocking your access card.

When you receive a new or renewed access card, we recommend that you use the Bank Australia app or logon to Internet Banking to confirm the card controls that you would like applicable to that access card.

All available control indicators will be set to the default position when the card control service is accessed for the first time. The default position for each control is “enabled” – meaning that the card control will not block any transactions.

When you set a card control for an access card it applies to every account linked to that access card.

If you are a primary cardholder of an access card with an additional cardholder and your card number is different to the additional cardholder’s card number, the card control you set for your card will not apply to the additional cardholder’s card. In addition, we don’t notify the additional cardholder of any control set by you.

We rely on the information about a transaction that a merchant provides us in order to decline transactions based on card controls that you have set. We cannot decline a transaction if we receive an authorisation request which does not match one of the transaction types you have blocked.

When you have enabled a card control or a temporary block on your access card, we will not decline the following transactions and they will be charged to the relevant account:

- transactions made under a Recurring Payment Authority (i.e. those payments flagged by the system as ‘recurring’) and
- transactions on the account your access card is attached to made via a Bank Australia branch/internet banking/app, including:
 - transfers to other accounts
 - bill payments (including BPAY®) and
 - assisted cash withdrawals via our branches.

- transactions that are not sent to us for authorisation, e.g. some contactless payments or transactions processed when there is a system interruption; and
- transactions that we consider should be allowed for your convenience.

We will make every effort to decline transactions that match one of the card controls you have set. However, we cannot guarantee that all such transactions will be declined. We are not responsible for any loss you suffer if a transaction:

- authorised by you or any additional cardholder is charged to your account even though it matches one of the card controls you have set
- is declined because it matches one of the card controls you have set, including any subsequent loss of goods/services if a merchant is unable to process the transaction to the account.

If you enable an international transaction, we recommend that you check your transaction history to confirm the transaction has appeared on your account before disabling that transaction type. This is because some merchants may not process your transaction immediately (i.e. the merchant may not process the transaction until the goods are dispatched).

Some or all card controls may not be effective in some cases, including where there are disruptions to computer and/or telecommunications systems or electronic terminal service failures. Disruptions to these systems may result in the card control service being unavailable from time to time.

A temporary lock doesn't report your card as lost or stolen. If your card is lost or stolen or you're unable to locate it, you must report it as soon as possible via Internet Banking, the Bank Australia app or by calling us. You should also tell us if there's been any fraudulent activity such as unauthorised transactions.

We may change the functionality of card controls at any time without giving prior notice to you. Any changes to card controls will show if and when you download an updated version of the Bank Australia app.

4.12 Using Visa outside Australia

All transactions made overseas on a 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 overseas on the Visa Card are subject to a conversion fee payable to CUSCAL, the principal member of Visa Worldwide under which we provide you with the Visa Card. Please refer to the Deposit Fees & Charges and Transaction Limits brochure for the current conversion fee.

Some overseas merchants and ATMs 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.

4.13 Foreign currency conversion fee

We will charge you with a foreign currency conversion fee (also known as foreign currency transaction fee) for each of the following types of transactions:

- transactions made overseas, to be converted into \$AUD
- transactions made in a foreign currency, to be converted into \$AUD
- 'card-not-present' transactions in Australian dollars with merchants located overseas
- transactions in Australian dollars with financial institutions located overseas or
- transactions in Australian dollars (or any other currency) that is processed by an entity outside Australia (together referred to as Overseas Transactions in Australian Dollars).

Please note that even though an online shopping website with a domain name that ends in '.com.au' might appear to be an Australian business, they or their bank might be located overseas. This means you could still be charged an international transaction fee.

4.14 Additional access card

You may authorise us, if we agree, to issue an additional access card to an additional cardholder provided this person is over the age of 13 (unless we agree to a younger age) for the purpose of accessing the linked account.

You will be liable for all transactions carried out by this cardholder. We will give each additional cardholder a separate passcode.

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

To cancel the additional access card you must notify us by telephone, in person at any branch or in writing (including electronically).

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

4.15 Validity of access card

A card is valid when it is issued to you until its Expiry Date, unless you are required to activate it. An access card which requires activation will be valid from when it is activated (and, if required in the case of a Physical Card, signed) until its Expiry Date.

You must not use your access card:

- before the valid date or after the expiration date shown on the face of the access card or
- after the access card has been cancelled.

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



4.16 Cancellation of access card or access to internet banking service, Osko, PayTo or BPAY®

You may request to cancel any access facility in person, online or over the phone.

We may cancel or suspend any access facility at any time for:

- security reasons
- where we suspect on reasonable grounds that you or someone acting on your behalf is being fraudulent
- where we suspect on reasonable grounds that your account or access method has been compromised or is at risk of being compromised
- if you breach any part of section 4. of these Conditions of Use in a manner which is capable of remedy but is not remedied within 20 business days of receiving a notice from us specifying the breach and requiring the breach to be remedied
- if you breach any obligation under any part of section 4. of these Conditions of Use which is incapable of remedy or
- if you suffer an Insolvency Event.

In the case of your access card, we may cancel the access card by recapturing the access card at any ATM.

We may also refuse to complete a transaction, cancel or suspend any access facility at any time without notice where you or an authorised user use an access facility or any services associated with it, to engage in conduct that, in our reasonable opinion,:

- is offensive or inappropriate;
- is unlawful;
- is defamatory, harassing or threatening to any person;
- threatens, promotes or encourages physical or mental harm of any person;
- threatens, promotes or encourages violence against any person; or
- threatens, promotes or encourages terrorism.

We may also refuse to complete a transaction, cancel or suspend any access facility at any time without notice where you or an authorised user use an access facility or any services associated with it, to engage in conduct that, in our reasonable opinion,:

- for security reasons where we reasonably suspect your account has been compromised or is at risk of being compromised
- your account is overdrawn and you have not corrected that overdrawn position in accordance with the terms and conditions of your account
- you are in default of the terms and conditions of your account and you have not rectified that default in the time specified in any notice to remedy the default
- we are required to by law, directed to by a payment scheme (or similar payment authority), banking regulator or where Bank Australia is no longer a participant in a payment scheme
- you suffer an Insolvency Event
- you or a joint account holder becomes deceased or
- your account becomes dormant.

In the case of your internet banking, BPAY®, Osko or PayTo, we may cancel or suspend the facility:

- if our membership to the BPAY® Scheme or our subscription to Osko is suspended, ceased or is cancelled (as the case may be) for any reason
- where we suspect on reasonable grounds that you are using Osko in a manner that will or is likely to affect our ability to continue providing Osko to you or our other customers
- where we believe on reasonable grounds that it is necessary to do so to prevent loss to Bank Australia or you, including where we suspect that the facility is being used or will be used for fraudulent purposes
- temporarily for the purpose of performing system maintenance or upgrades.

Without limiting the above, we will block Gambling Transactions on credit cards accounts. You agree that we may do this on your credit card account without us incurring any liability. There will be instances where we are unable to block a gambling or gaming transaction, in which case you will still be responsible for those gambling or gaming transactions.

4.17 Consequences of suspension or termination

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

- we notify you that we have cancelled your access card or your access method to the account with us
- you close the last of your accounts with us to which the access card applies or which has internet banking, BPAY®, PayTo or Osko access
- you alter the authorities governing the use of your account or accounts to which the access card applies or which has internet banking, BPAY®, PayTo or Osko access (unless we agree otherwise).

In the case of your access card, you will be liable for any transactions you make using your access card before the access card is cancelled but which are not posted to your account until after cancellation of your access card. We will credit to you any refund or other credit payments that occur prior to cancellation but are received by us after cancellation.

We may demand the return or destruction of any cancelled access card.

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



Termination or suspension of your rights to use Osko does not:

- prejudice any claims either party may have against the other in respect of any then subsisting breaches of these Conditions of Use or
- otherwise affect the accrued rights and remedies of either party.

4.18 Exclusions of access card warranties and representations

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

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

We are not responsible for any defects in the goods and services you acquire through the use of the access 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.

4.19 Using internet banking

We do not warrant that:

- the information available to you about your accounts through our internet banking service is always up to date
- you will have 24 hours a day, 7 days per week, access to internet banking
- data you transmit via internet banking is totally secure.

4.20 How to report loss, theft or unauthorised use of your access card, passcode or digital wallet

If you believe your access card has been misused, lost or stolen or the passcode has become known to someone else, you must contact us immediately on **132 888** from within Australia. If you're calling outside of business hours, listen to the message for directions and contact the after hours service number provided on the message.

You should take the same actions if any access card or device holding a digital wallet into which an access card has been registered or through which a digital card can be viewed, has been lost, stolen or used without authorisation, a passcode has become known to someone else, any security credentials on any device are otherwise compromised, or a user suspects that unauthorised transactions have been made on your linked account.

If the Contact Centre is not operating when you attempt notification and you are not able to contact the after hours service, 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 Contact Centre 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.



If the loss, theft or misuse, occurs OUTSIDE AUSTRALIA you must notify an organisation displaying the Visa sign and also then confirm the loss, theft or misuse of the card with us by telephone, priority paid mail or secure mail as soon as possible.

You should also immediately implement appropriate card controls (such as temporary card block), which you can do through Internet Banking or the Bank Australia app.

4.21 How to report unauthorised use of internet banking

If you believe that your passcodes for internet banking transactions have been misused, lost or stolen, or, where relevant, your passcode has become known to someone else, you must contact us immediately and change your passcode on 132 888 from within Australia or +61 3 9854 4666.

4.22 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 (found on your bill), your Customer Reference Number (eg. your account number with the biller), the amount to be paid and the account from which the amount is to be paid.

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

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

4.23 Processing BPAY® payments

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

- you become aware of any delays or mistakes in processing your BPAY® payment
- you did not authorise a BPAY® payment that has been made from your account or
- you think that you have been fraudulently induced to make a BPAY® payment.

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

A BPAY® payment instruction is irrevocable.

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

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

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

Please note that you must provide us with written consent addressed to the biller who received that BPAY® payment. If you do not give us that consent, the biller may not be permitted under law to disclose to us the information we need to investigate or rectify that BPAY® payment.

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

- on the date you direct us to make it, if we receive your direction by the cut off time on a banking business day, that is, a day in Sydney or Melbourne when banks can effect settlements through the Reserve Bank of Australia and
- otherwise, on the next banking business day after you direct us to make it. Please note that the BPAY® payment may take longer to be credited to a biller if you tell us to make it on a Saturday, Sunday or a public holiday or if another participant in BPAY® does not process a BPAY® payment as soon as they receive its details.

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

- there is a public or bank holiday on the day after you instruct us to make the BPAY® payment
- you tell us to make a BPAY® payment on a day which is not a banking business day or after the cut off time on a banking business day or
- a biller, or another financial institution participating in BPAY®, does not comply with its BPAY® obligations.

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

- advise you of this
- credit your account with the amount of the BPAY® payment and
- take all reasonable steps to assist you in making the BPAY® payment as quickly as possible.

You must be careful to ensure you tell us the correct amount you wish to pay.

If you make a BPAY® payment and later discover that:

- the amount you paid was greater than the amount you needed to pay, you must contact the biller to obtain a refund of the excess or
- the amount you paid was less than the amount you needed to pay, you can make another BPAY® payment for the difference between the amount you actually paid and the amount you needed to pay.

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

4.24 Future-dated BPAY® payments

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

You may arrange BPAY® payments up to 60 days in advance of the time for payment.

If you use this option you should be aware of the following:

- you are responsible for maintaining, in the account to be drawn on, sufficient cleared funds to cover all future-dated BPAY® payments (and any other drawings) on the day(s) you have nominated for payment or, if the account is a credit facility, there must be sufficient available credit for that purpose
- if there are insufficient cleared funds or, as relevant, insufficient available credit, the BPAY® payment will not be made and you may be charged a dishonour fee
- you are responsible for checking your account transaction details or account statement to ensure the future-dated payment is made correctly
- you should contact us if there are any problems with your future-dated payment
- you must contact us if you wish to cancel a future-dated payment after you have given the direction but before the date for payment. You cannot stop the BPAY® payment on or after that date.

4.25 Consequential damage for payments

This section does not apply to the extent that it is inconsistent with or contrary to any applicable law or code of practice to which we have subscribed (including the ePayments Code and the Customer Owned Banking Code of Practice). If those laws would make this section illegal, void or unenforceable or impose an obligation or liability which is prohibited by those laws or that code, this section is to be read as if it were varied to the extent necessary to comply with those laws or that code or, if necessary, omitted.

We are not liable for any consequential loss or damage (including any loss of profit) you suffer as a result of your use of any access method (such as BPAY®, Osko, PayTo, EFTPOS, access card and direct debits) for sending or receiving, or arranging to send or receive any payments from your account, other than loss due to our negligence or in relation to any breach of a condition or warranty implied by the law of contracts for the supply of goods and services which may not be excluded, restricted or modified at all, or only to a limited extent.

In respect of any warranty or consumer guarantee which is unable to be excluded under any relevant law, our liability in respect of a breach of that warranty or guarantee relating to your use of account is limited to the re-supply of the services or the payment of the cost of having the services supplied again at your discretion.



4.26 Regular payment arrangements

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

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

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

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

4.27 Osko

We subscribe to Osko under the BPAY® Scheme.

Osko is available to all customers who have set up internet banking services with us.

Osko allows you to make and receive Osko Payments to other Osko users located within Australia in near real-time.



4.28 Using Osko

You can use Osko to make and receive Osko Payments using a PayID instead of account details. Limits apply; please refer to our Deposit Fees, Charges and Transaction Limits brochure.

When you tell us to make an Osko Payment, you must tell us:

- the payee's PayID, or if you elect not to use PayID, the details of the payee's account(s) to be credited with the amount of the Osko Payment
- the amount to be paid and
- the account from which the amount is to be paid from.

You should ensure that all information you provide in relation to an Osko Payment is correct as we will not be able to cancel an Osko Payment once it has been processed.

When initiating an Osko Payment, you might direct the Osko Payment to an incorrect account if you get the PayID wrong. To try and avoid this, we will ask you to verify that you have the right PayID by presenting you with the associated PayID Name of the payee as an additional confirmation of the intended recipient before you submit a Payment Direction.

In order to better provide you with the services under Osko, we may retain certain information relating to PayIDs you have used. For example, we may retain information relating to PayIDs you provide us in order to facilitate scheduled payments.

We cannot effect an Osko Payment if:

- the payee's financial institution does not support the New Payments Platform Payment service and/or
- the payee's account is locked.

Depending on the settings you choose for your PayID, other account holders on your account may be able to see messages and notifications associated with Osko Payments addressed to your PayID.

4.29 Choosing a PayID and PayID Name

You do not have to register PayID but any PayID created must be in a PayID Type that we support. The following is the full list of PayID types that we support:

- a BSB and account number issued by us to you (note: this is the default PayID that will be assigned to your account)
- a valid email address
- a mobile phone number issued in Australia and
- for business customers, their ABN, ACN, ARBN or ARSN.

In establishing a PayID, you represent and warrant that:

- you own or are authorised to use the PayID you have created
- the PayID is current, accurate and complete and
- you agree to the PayID you have established being registered in the PayID Service.

You may choose to create more than one PayID for your account.



You must first satisfy us that you own or are authorised to use your chosen PayID before you can use it. This means we may ask you to provide evidence to establish this to our satisfaction, whether you are already registered for any other mobile or online banking or online payment services with us or not. We may reject your use of any PayID where in our reasonable opinion you are not the owner or authorised to use that PayID. We can also refuse your request to create a PayID where:

- we have not verified your identity
- we are required to do so by law or by the New Payments Platform operator or
- the PayID is already in existence.

If you have other authorised users on your account, each authorised user can create a unique PayID for the account.

If you have nominated a joint account to participate in Osko, you and each other joint account holder can create a unique PayID for the account.

Once a PayID is created and linked to your account, you may not use the same PayID in relation to any other account with us or with any other financial institution.

We may restrict some PayID Names or PayID Types if they:

- are identical to another PayID in the service
- restricted for use only by business customers and organisational payers
- likely to mislead or deceive a payer into sending you Osko Payments intended for another payee or
- for any other reason which, in our reasonable opinion, is inappropriate.

If you have attempted to create a PayID for your account and have been informed that it is identical to another PayID in the service, you can contact us to discuss the duplicate PayIDs but we will not be able to disclose details of any personal information in connection with the duplicate PayID.

Depending on the payer's financial institution, your PayID Name may be displayed to payers who send Osko Payments to you. At the same time you create your PayID Name, we will either enable you to:

- confirm your selection of a PayID Name for display to payers or
- select an alternative PayID Name, such as your business name, for display.

We will not permit the choosing a PayID Name that we consider could reasonably mislead or deceive a payer into sending you an Osko payment intended for another payee.

4.30 Transferring your PayID to another account

You can request a transfer of your PayID at any time. However, a locked PayID cannot be transferred.

You can transfer your PayID to another account with us, or to an account with another financial institution, by submitting a request to us online (via our internet banking site or our mobile app), by visiting a branch or over the phone by calling us on 132 888.

A transfer of your PayID to another account with us will generally be effective immediately, unless we notify you otherwise.

To transfer your PayID to another financial institution, you must ask us to put your PayID into a transfer state and tell your new financial institution to complete the transfer.

Until the transfer is effected, all Osko payments to your PayID will be directed to your current linked account with us.

If the new financial institution does not complete the transfer within 14 days, the transfer will be deemed to be ineffective and your PayID will remain attached to your linked account with us. This means Osko Payments to your PayID will continue to be directed to your account with us. You can request to transfer your PayID again at any time.

If the PayID you transfer to another financial institution is linked to a PayTo Payment Agreement, the Payment Agreement will not automatically transfer with the PayID. You will need to either link the Payment Agreement to another account with us or transfer the Payment Agreement to the other financial institution (see section 4.47 "Transferring your Payment Agreement"). We may refuse to transfer a PayID to another financial institution until you have taken appropriate steps, as we reasonably determine, in relation to any linked Payment Agreements.

4.31 Transferring your PayID from another account

You can transfer a PayID that you have created for an account with another financial institution to your account with us by initiating the transfer process with the other financial institution and notifying us once this has been done so that we can complete the transfer process.

If the PayID you transfer to an account with us is linked to a PayTo Payment Agreement, the Payment Agreement will not automatically transfer with the PayID. You will need to take additional steps if you wish to transfer the Payment Agreement to your account with us (see section 4.47 "Transferring your Payment Agreement").

4.32 Locking your PayID

We monitor PayID use to manage PayID misuse and fraud.

You acknowledge and agree to us locking your PayID if we reasonably suspect misuse of your PayID or where your PayID has been used to procure Osko Payments fraudulently.

You will need to contact us to unlock a locked PayID.

4.33 Closing your PayID

You can submit a request to close your PayID by submitting a request to us online (via our internet banking site or our mobile app), by visiting a branch or over the phone by calling us on 132 888. We may refuse to close a PayID until you have taken appropriate steps, as we reasonably determine, in relation to any PayTo Payment Agreements linked to the PayID.

You must keep your PayID details current, accurate and complete.

You must notify us immediately if you no longer own or have authority to use your PayID.

We can close your PayID where:

- we are not reasonably satisfied that you own or are otherwise authorised to use that PayID
- we reasonably suspect that the PayID is or has been used for a fraudulent purpose
- your PayID has remained locked for a period that we reasonably consider to be excessive or
- we are required to do so by law or by the operator of the New Payments Platform.

We will automatically close your PayID if the Linked Account for that PayID is closed.

4.34 Processing Osko Payments

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

- you become aware of mistakes in processing your Osko Payment
- you did not authorise an Osko Payment that has been made from your account or
- you think that you have been fraudulently induced to make an Osko Payment.

An Osko payment direction is irrevocable. Our ability to recover payments is limited as set out in sections 4.34, 4.35 and 4.36.

You cannot stop an Osko Payment once you have instructed us to make it and we cannot reverse it.

We will treat your Osko payment direction as valid if, when you give it to us, you comply with these Conditions of Use in relation to making Osko Payments, subject to applicable laws including, where applicable, the ePayments Code.

Where you direct us to make an Osko Payment and the payee's PayID is a BSB and account number, we will, in the first instance endeavour to send the payment as an Osko Payment. If, for any reason the payment cannot be effected via Osko we will attempt to send the payment as a direct credit on your behalf and you authorise us to do this. In these circumstances the terms and conditions in respect of direct credits will apply to the payment. A direct credit will not be effected in real time.



4.35 Notifications of Osko Payments

We will inform you when:

- we confirm and validate each Osko payment direction you give us
- an Osko payment direction is successfully completed
- an Osko payment direction has failed for any reason.

If we are advised that an Osko Payment you have attempted to send from your account cannot be processed for whatever reason, we will:

- advise you of this
- when appropriate, credit your account with the failed amount of the Osko Payment and
- take all reasonable steps to assist you in making the Osko Payment as quickly as possible.

Where we are able to do so we will tell you:

- if there are delays in processing Osko Payments
- when Osko Payments are likely to be completed and
- give you the opportunity to cancel an Osko Payment that is delayed.

4.36 Mistaken or misdirected payments from your account

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

If you make an Osko Payment and later discover that:

- the amount you paid was greater than the amount you needed to pay, you must contact the payee if you wish to obtain a refund or
- the amount you paid was less than the amount you intended to pay, you can make another Osko Payment for the difference between the amount you actually paid and the amount you needed to pay.

If you are responsible for a mistaken Osko Payment, we will make reasonable attempts at recovering the amount from the person who received it. However, if we are unsuccessful at recovering the amount from the person within 20 business days, you will be liable for that payment. In the event we recovered some or part of the mistaken Osko Payment after the 20 business day period, we will credit the amount received to you less any relevant fee, tax or charge payable in respect of that Osko Payment.

4.37 Mistaken or misdirected payments into your account

Where we and the sending financial institution determine that an Osko Payment made to your account is either a mistaken payment or a misdirected payment, we may, without your consent, deduct from your account an amount up to the original amount of the mistaken payment or misdirected payment, subject to complying with any other applicable terms and conditions.

We will notify you if a mistaken payment or misdirected payment has been made.

4.38 Future-dated Osko Payments

Please note that this section is only operative if Bank Australia notifies you that future dated payment functionality for Osko payments is available. Bank Australia does not warrant that it will make future dated payment functionality available.

You may arrange Osko Payments in advance of the time for payment. If you use this option you should be aware of the following:

- you are responsible for maintaining, in the account to be drawn on, sufficient cleared funds to cover all future-dated Osko Payments (and any other drawings) on the day(s) you have nominated for payment or, if the account is a credit facility, there must be sufficient available credit for that purpose
- if there are insufficient cleared funds or, as relevant, insufficient available credit, the Osko Payment will not be made and you may be charged a dishonour fee
- you are responsible for checking your account transaction details or account statement to ensure the future-dated payment is made correctly
- you should contact us if there are any problems with your future-dated payment
- you must contact us if you wish to cancel a future-dated payment after you have given the direction but before the date for payment. You cannot stop the Osko Payment on or after that date.

4.39 Consequential damage for Osko Payments

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

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

In respect of any warranty or consumer guarantee which is unable to be excluded under any relevant law, our liability in respect of a breach of that warranty or guarantee relating to your use of Osko is limited to the re-supply of the services or the payment of the cost of having the services supplied again at your discretion.

4.40 Changes to Osko

We may change the way you use Osko where the change is reasonably necessary to:

- comply with any law
- accommodate changes in the operation of the BPAY® Scheme or Osko
- comply with BPAY®'s or our security policies and procedures.

We will notify you of these changes when they occur.

4.41 Privacy

By creating your PayID you acknowledge that you authorise:

- us to record your PayID, PayID Name and account details (including full legal account name) (PayID Record) in the PayID Service
- Osko participants which are payers' financial institutions to use your PayID information for the purposes of construction Osko Payment messages, enabling payers to make Osko Payments to you, and to disclose your PayID Name to payers for Osko Payment validation and
- us, in order to provide you the Osko services, to disclose your personal information (within the meaning of the Privacy Act 1988 (Cth) and including any updates of your personal information notified to us) to BPAY®, its service providers and such other participants involved in Osko. If we do not disclose your personal information to BPAY® and its service providers, we will not be able to provide you with services under Osko.

You must notify us of any changes to your relevant personal information that may be contained in a PayID Record.

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 Act 1988(Cth) you acknowledge and agree that you consent to that disclosure, storage and use.

4.42 Net Position View

'Net Position View' allows you to see a summary of your assets and liabilities.

Using the Net Position View, you can see the credit balance you hold in accounts with Bank Australia and liabilities you owe to Bank Australia.

The 'Net Position View' is the figure that is calculated via the difference between your total liabilities and total assets in your Bank Australia accounts. It will not take into account other information such as the value of the asset against which the liability is secured and as such, may not be an accurate reflection of your 'net worth'. The information is based on transactions that have cleared your account.

4.43 Spend Tracker

'Spend Tracker' allows you to track cleared payments from eligible accounts (as are detailed in the Summary of Accounts & Availability of Access Facilities brochure) in the Bank Australia app. This includes card transactions made in person, online or over the phone, mobile wallet transactions (such as Apple Pay or Google Pay), recurring transactions, Pay Anyone payments, BPAY® payments, direct debits, PayTo transactions, international money transfers and fees or charges on your account.

Spend Tracker is only an indicator of your spending and will not restrict your spending or saving that is linked to your Bank Australia accounts.



4.44 Creating a PayTo Payment Agreement

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

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

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

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

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

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 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.

This section 4.44 does not apply to Migrated DDR Mandates.

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

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

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 instruct us to amend your name or transfer the Payment Agreement to another Account you hold with us. If you wish to transfer the Payment Agreement to an account with another financial institution, you may, when available, give us a transfer instruction (see section 4.47 "Transferring your Payment Agreement"). We may decline to act on your instruction to amend your Payment Agreement if we are not reasonably satisfied that your request is legitimate. You may not request us to amend the details of the Merchant or Payment Initiator, or another party.

4.46 Pausing your 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. While the Payment Agreement is paused, we will not process payment instructions in connection with it. We are not liable for any loss that you or any other person may suffer as a result of you pausing a Payment Agreement.

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

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

4.47 Transferring your Payment Agreement

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

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

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.

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

4.48 Cancelling your 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 cancelling a Payment Agreement.

You may remain liable to the Merchant or Payment Initiator for payments that would otherwise have been paid under the Payment Agreement, including for any cancellation fees.

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

4.49 Migration of Direct Debit arrangements

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

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

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

4.50 General

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

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



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

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

You are responsible for ensuring that you have sufficient funds in your Account to meet the requirements of all your Payment Agreements. We are not responsible for any loss that you suffer as a result of your Account having insufficient funds to meet a payment instruction under a Payment Agreement. See section 3.9 "Overdrawing an account" for our rights if there are insufficient funds in your Account.

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 your Payment Agreements are accurate and up to date. You must promptly respond to any such request. Failure to respond may result in us pausing the Payment Agreements.

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

You are responsible for ensuring 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; and
- (iii) any passwords/PINs needed to access the facilities we provide are kept confidential and are not disclosed to any other person.

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



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

- (i) modifications to Our Intellectual Property by or on behalf of you in a manner that causes the infringement;
- (ii) use of any item in combination with any hardware, software or other products or services in a manner that causes the infringement and where such combination was not within the reasonable contemplation of the parties given the intended use of the item;
- (iii) your failure to use corrections or enhancements to Our Intellectual Property that are made available to you (except where the use of corrections or enhancements would have caused a defect in PayTo or would have had the effect of removing functionality or adversely affecting the performance of PayTo); and
- (iv) your failure to use Our Intellectual Property in accordance with this agreement.

We may cancel or suspend your use of PayTo in accordance with our rights under section 4.16 "Cancellation of access card or access to internet banking service, Osko, PayTo or BPAY®".

We may amend the terms and condition relating to PayTo in accordance with our rights under section 3.16 "Notifying changes". If you do not accept our amendments, you may cease using PayTo.

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 in the Mandate Management Service.

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

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

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

4.51 Privacy

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

4.52 Authority

Your instructions in relation to a Payment Agreement must be provided in accordance with the account operating instructions for the Account that is, or is intended to be, linked to the Payment Agreement. This includes instructions to confirm or decline a Payment Agreement or the Merchant's or Payment Initiator's amendments to a Payment Agreement, or to amend, pause, resume, cancel or transfer a Payment Agreement. For example, instructions to confirm a Payment Agreement linked to a joint account operated on an 'all to sign' basis must be provided by all the joint holders. Any changes to your account operating instructions for the Account may result in a pause of the Payment Agreement. While the Payment Agreement is paused, we will not process payment instructions in connection with it. We are not liable for any loss that you or any other person may suffer as a result of you pausing a Payment Agreement.



5. Other things you need to know

5.1 Third party payment services

Bank Australia provides outward and inward telegraphic transfer services to our customers through our business partner Convera Australia Pty Ltd trading as Convera ACN 150 129 749; AFSL 404092. All telegraphic transfers you initiate through Bank Australia will be sent to beneficiaries account via Convera. Fees & charges and terms & conditions apply.

5.2 Inward Telegraphic Transfers

Funds forwarded from outside of Australia may pass through other financial institutions before being credited to your Bank Australia account.

Each institution involved in the transfer process may deduct a processing fee from the amount being remitted before on-forwarding the funds. Bank Australia does not charge any fees but will pass on any fee charged by other financial institutions involved in the transfer.

Bank Australia will credit telegraphic transfer funds to your account within 1 to 2 business days once the payment has been received by Bank Australia.

Provided all information supplied on the request is complete and correct, funds transferred from major overseas currencies generally take 3-5 business days to be received, however this is an estimate only and cannot be guaranteed. Funds transferred from minor overseas currencies generally take 7-10 working days, however this is an estimate only and cannot be guaranteed.

The conversion of foreign amounts into Australian Dollars is performed by our international payments provider before the funds are received at Bank Australia for processing.

Telegraphic transfer funds can only be credited to a transaction account and funds received for other accounts will be credited to your Bank Australia transaction account.

5.3 Outward Telegraphic Transfers

Requests to transfer funds via telegraphic transfer will be processed within 1-2 business days.

Telegraphic transfers are manually processed and will pass through at least one, and up to four other institutions before being credited to the receiving account.

Please be aware that all international money transfers are monitored by government agencies for the purpose of detecting terrorist and criminal activity. For this reason and the possibility of incorrect information being provided when remitting funds, our international payments provider may require further information or details from you before the international transfer can be processed, and you agree that all information may be passed on by Convera to third parties as appropriate.



Provided all information supplied on the request is complete and correct, funds transferred to major overseas currencies generally take 3-5 business days to be received, however this is an estimate only and cannot be guaranteed. Funds transferred to minor overseas currencies generally take 7-10 working days, however this is an estimate only and cannot be guaranteed.

Each institution involved in the transfer process may deduct a processing fee from the amount being remitted before on-forwarding the funds.

Bank Australia cannot lodge a trace on international telegraphic transfers until 5 business days after telegraphic transfer has been lodged.

You are responsible for the completeness and accuracy of the details you provide to us in relation to a telegraphic transfer. We are not responsible to you or a beneficiary for any direct or consequential loss as a result of:

- any error or omission in the details you provide when requesting a telegraphic transfer
- any error, omission or negligence of Convera or
- any delay in payment to the Beneficiary, other than loss due to our negligence or in relation to any breach of a condition or warranty implied by the law of contracts for the supply of goods or services which may not be excluded, restricted or modified at all, or only to a limited extent.

Requests to recall or change the detail on international telegraphic transfers may be charged a fee or have penalties to exchange rates applied. If you think you have made a mistake when providing details in relation to the telegraphic transfer, you should contact us immediately. However, we cannot and do not warrant that we will be able to stop or correct a telegraphic transfer that you have authorised. Convera can lodge an amendment on transfers should this be necessary. Amendments can take up to 10 business days to be acknowledged by the overseas financial institution and actioned.

If it becomes necessary to recall funds or if funds are returned due to incorrect or incomplete details being supplied, Convera will apply the buying rate on the day funds are received, which may vary to the original rate and result in a loss. Funds returned to Convera may be less than the original amount transferred due to overseas bank charges. Please note that while Convera can lodge a request to recall funds, this would require debit authorisation from the beneficiary for any release of funds. Should the beneficiary choose not to give a debit authority, the recall will not be successful.

If a telegraphic transfer is rejected and fails or further information is required to process your payment, we will use our best endeavours to contact you. You will be liable for our fees and charges notwithstanding that the telegraphic transfer has been rejected.

If you complete a telegraphic transfer through internet banking your acceptance of a quote by selecting the 'Confirm Transfer' button will constitute your instruction and authorisation to us to immediately debit the value of your telegraphic transfer request (in Australian dollars) from the account you have nominated when using the facility (including the applicable fees and charges payable to us in relation to the telegraphic transfer as stated in our 'Deposit Fees, charges and transaction limits' document) and to transfer funds to the account of the beneficiary.

A transaction confirmation does not signify that the telegraphic transfer has been received into the account of the beneficiary.

5.4 When you are not liable for loss

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.

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

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

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.

5.5 When you are liable for loss

You may only be made liable for losses arising from an unauthorised transaction in the circumstances specified in this section.

Where we can prove on the balance of probability that a user contributed to a loss through fraud, or breaching our passcode security requirements:

- 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:
 - incurred on any one day that exceeds any applicable daily transaction limit
 - incurred in any period that exceeds any applicable periodic transaction limit
 - that exceeds the balance on the facility, including any pre-arranged credit
 - 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.
- Where:
 - more than one passcode is required to perform a transaction and
 - we prove that a user breached our passcode security requirements for one or more of the required passcodes, but not all of the required passcodes you are liable under this section only if we also prove on the balance of probability that the breach of our passcode security requirements was more than 50% responsible for the losses, when assessed together with all the contributing causes.

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

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

Where we can prove, on the balance of probability, that a user contributed to losses resulting from an unauthorised transaction by unreasonably delaying reporting the misuse, loss or theft of a device, or that the security of all passcodes has been breached, you:

- are liable for the actual losses that occur between:
 - 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
 - when the security compromise was reported to us.
- are not liable for any portion of the losses:
 - incurred on any one day that exceeds any applicable daily transaction limit
 - incurred in any period that exceeds any applicable periodic transaction limit
 - that exceeds the balance on the facility, including any pre-arranged credit
 - 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 if you were the user who contributed to the loss, or if a different user contributed to the loss.

Where a passcode was required to perform an unauthorised transaction, and the preceding paragraphs of this section do not apply, you are liable for the lower 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 pre-arranged 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.

In deciding whether on the balance of probabilities we have proved that a user has contributed to losses as stated in the preceding paragraphs of this section 5.5:

- 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 our 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.

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 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, chargeback 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.

5.6 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 to complete a transaction accepted by the system or equipment in accordance with a user's instructions.

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

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

5.7 Network arrangements

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

- we are a party to a shared electronic payments network
- another party to the network caused the failure to meet the obligation.

We must not require you to:

- raise a complaint or dispute about the processing of a transaction with any other party to a shared electronic payments network
- have a complaint or dispute investigated by any other party to a shared electronic payments network.

5.8 Mistaken internet payments

In this section:

- **Mistaken Internet Payment** means a payment by a user through a pay anyone banking facility and processed by an authorised deposit-taking institution (ADI) where funds are paid into the account of an unintended recipient because the user enters or selects a Bank/State/Branch (BSB) number and/or identifier that does not belong to the named and/or intended recipient as a result of:
 - the user's error, or
 - the user being advised of the wrong BSB number and/or identifier.

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

- **Receiving ADI** means an authorised deposit-taking institution whose customer has received an internet payment.
- **Unintended Recipient** means the recipient of funds as a result of a mistaken internet payment
 - when you report a mistaken internet payment, we must investigate whether a mistaken internet payment has occurred
 - if we are satisfied that a mistaken internet payment has occurred, we must send the receiving ADI a request for the return of the funds.

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

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

- acknowledge the request for the return of funds, and
- advise us whether there are sufficient funds in the account of the unintended recipient to cover the mistaken internet payment.

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



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

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

- are not satisfied that a mistaken internet payment has occurred
- have not complied with the processes and timeframes set out in the preceding paragraphs of this section 5.8, or as described in the box below.

When we receive a complaint we must:

- deal with the complaint under our internal dispute resolution procedures
- not require you to complain to the receiving ADI.

If you are not satisfied with the outcome of a complaint, you are able to complain to AFCA. Refer to the Complaints section for further details.

If you receive a mistaken internet payment into your account and we are required under the ePayments Code as receiving ADI to return the funds to the payer's ADI then we will, without seeking your consent, transfer the funds from your account.

If there are insufficient funds in your account you must co-operate with us to facilitate repayment of the funds.

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

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

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

- Process where sufficient funds are available & report is made within 10 business days:
 - if satisfied that a mistaken internet payment has occurred, the receiving ADI must return the funds to the sending ADI, within 5 business days of receiving the request from the sending ADI if practicable or such longer period as is reasonably necessary, up to a maximum of 10 business days
 - if not satisfied that a mistaken internet payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder
 - the sending ADI must return the funds to the holder as soon as practicable.
- Process where sufficient funds are available & report is made between 10 business days & 7 months:
 - the receiving ADI must complete its investigation into the reported mistaken payment within 10 business days of receiving the request.
 - if satisfied that a mistaken internet payment has occurred, the receiving ADI must:
 - (i) prevent the unintended recipient from withdrawing the funds for 10 further business days, and
 - (ii) notify the unintended recipient that it will withdraw the funds from their account, if the unintended recipient does not establish that they are entitled to the funds within 10 business days commencing on the day the unintended recipient was prevented from withdrawing the funds.
 - if the unintended recipient does not, within 10 business days, establish that they are entitled to the funds, the receiving ADI must return the funds to the sending ADI within 2 business days after the expiry of the 10 business day period, during which the unintended recipient is prevented from withdrawing the funds from their account.
 - if the receiving ADI is not satisfied that a mistaken internet payment has occurred, it may seek the consent of the unintended recipient to return the funds to the holder.
 - the sending ADI must return the funds to the holder as soon as practicable.

- Process where sufficient funds are available and report is made after 7 months:
 - If the receiving ADI is satisfied that a mistaken internet payment has occurred, it must seek the consent of the unintended recipient to return the funds to the user.
 - If not satisfied that a mistaken internet payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder.
 - If the unintended recipient consents to the return of the funds:
 - (i) the receiving ADI must return the funds to the sending ADI, and
 - (ii) the sending ADI must return the funds to the holder as soon as practicable.
- Process where sufficient funds are not available
 - where the sending ADI and the receiving ADI are satisfied that a mistaken internet payment has occurred, but there are not sufficient credit funds available in the account of the unintended recipient to the full value of the mistaken internet payment, the receiving ADI must exercise discretion, after appropriate weighing of interests of the sending consumer and unintended recipient and information reasonably available to it about the circumstances of the mistake and the unintended recipient, in deciding whether it should pursue return of the total value of the mistaken internet payment, pursue the return of a partial amount of the mistaken internet payment, or not pursue any return of funds.
 - The above processes where sufficient funds are available will also apply where insufficient funds are available, but only in relation to the value of the insufficient funds available.

5.9 Money laundering and illegality

So that we can meet our legal and regulatory obligations, we must exercise a level of control and monitoring over accounts and access facilities opened with Bank Australia. This means that we may delay, freeze, block or refuse to make or receive any payment using the services detailed in these Conditions of Use if we believe on reasonable grounds that making, receiving or crediting the payment may breach any law in Australia or any other country, and we will incur no liability to you if we do so. We are not liable for any loss you suffer (including consequential loss) howsoever caused in connection with any action or omission undertaken by us which we reasonably considered was necessary or prudent in order for us to comply with:

- our internal policies and guidelines
- any law or lawful direction
- any industry code to which we subscribe or
- any payment scheme rule applicable to the respective payment.

You provide Bank Australia the following undertakings and indemnify Bank Australia against any potential losses arising from any breach by you of such undertakings:

- that you will not initiate, engage in or effect a transaction that may be in breach of any Australian law or sanction (or any law or sanction of any other country) and
- the underlying activity for which any deposit account is being provided does not breach any Australian law or sanction (or any law or sanction of any other country).

To discharge our regulatory and compliance obligations, we may require that you provide us with additional information. You should be aware that where we are obliged to do so we will disclose the information gathered to regulatory and/or law enforcement agencies, other banks, payment system participants, service providers and other third parties.

5.10 Request for Documents

We will, at your request, give you a copy of your documents in our possession including:

- A contract – including terms and conditions, standard fees and charges and interest rates;
- Any mortgage or other security document;
- A statement of account; and
- Any notice we previously gave to you which is relevant to us exercising our rights.

However, we do not have to give you a copy of either of the following documents under the above paragraph:

- A notice requiring you to take action if you ask for the copy more than two years after the contract to which the notice relates was discharged or ended; or
- A statement of account within three months after we gave you a copy of the same statement of account.

If we are giving you a copy of a document under the above paragraph, then we will do so within 14 days where the original came into existence no more than one year ago or otherwise 30 days.

We may charge you a reasonable fee for providing you with a copy of a document under this section. However, in certain circumstances we may waive or refund that fee.

5.11 Instructions to Us

Subject to the provisions of this section 5, you are responsible for all instructions given in relation to your accounts which are authorised by a user's use of their password, authentication service or otherwise undertaken by another person with the user's knowledge or consent. For the avoidance of doubt, this includes instructions given after a user has allowed remote access to a device used for internet banking or provided access to secure codes which a person has used to provide instructions. Such instructions are valid, irrevocable authorities to us to follow the instructions.



6. Specific terms applicable to accounts

6.1 Mortgage Offset Account

This Section 6.1 applies if we have agreed to allow you to link a Mortgage Offset Account to your Home Loan Account. Not all loan accounts may be linked to a Mortgage Offset Account. Please refer to our Summary of Accounts and Availability of Access Facilities brochure as to the specific home loans which are eligible and you may apply to be linked to a Mortgage Offset Account.

Eligibility criteria

We will link your Mortgage Offset Account to an eligible Home Loan Account when each of the following criteria has been satisfied:

- You have an eligible Home Loan Account that can be linked to your Mortgage Offset Account.
- You have asked us to link your Mortgage Offset Account to the eligible Home Loan Account.
- The Mortgage Offset Account is not currently linked to another loan account.
- If the eligible Home Loan Account has a fixed rate of interest, it does not already have another Mortgage Offset Account linked to it.
- The Mortgage Offset Account holder is a party to the Home Loan Account to which the Mortgage Offset Account is being linked.

Time to link accounts

It may take us up to 5 Business Days to link the Mortgage Offset account to the Loan once all eligibility criteria have been satisfied.

Calculation of interest

The interest charges calculated on your home loan account for each day will be reduced by the Offset Amount on that day. No reductions by Offset Amounts will apply until the Mortgage Offset Account and Home Loan Account have been linked.

During any fixed rate period under your linked Home Loan Account, the Offset Amount is capped at \$20,000 ("Offset Cap").

No interest paid on a Mortgage Offset account

Bank Australia will not pay interest on the balance, or any part of the balance, of your Mortgage Offset Account. This includes any portion of the balance of your Mortgage Offset Account that exceeds either the unpaid balance of your linked Home Loan Account or the Offset Cap.

Transfer of funds to another account

We may in our discretion transfer any amount in excess of the Offset Cap to either:

- Another Mortgage Offset Account in your name (except to the extent that it is also capped).
- An Everyday Access Account in your name.

If you do not already have such an account, you authorise us to open one for you.

Number of offset accounts

An eligible Home Loan Account with a variable rate of interest can have an unlimited number of Mortgage Offset Accounts linked to it. An eligible Home Loan Account with a fixed rate of interest can only have one Mortgage Offset Account linked to it. Each Mortgage Offset Account can only be linked to one eligible Home Loan Account.

Conversion of Mortgage Offset Account to Everyday Access Account

When any of the following circumstances occur:

- the Mortgage Offset Account is not or ceases to be linked to an eligible Home Loan Account, or
- the Home Loan Account to which it is linked is paid out and closed,

you acknowledge and agree that we may convert the Mortgage Offset Account to an Everyday Access Account unless you have requested that the Mortgage Offset Account be closed before that time. Before we do this, we will write to you to confirm your instructions. If we don't hear from you within 30 days, we will convert your Mortgage Offset Account to an Everyday Access Account.

De-linking of Accounts

We may de-link your Home Loan Account from your Mortgage Offset Account, and treat your Mortgage Offset Account in the same manner as set out above in "Conversion of Mortgage Offset Account to Everyday Access Account" in any of the following circumstances:

- when you instruct us to do so;
- if the Home Loan Account is paid out or closed for any reason; or
- if you have converted your Home Loan Account to an ineligible Home Loan Account.

Our right to block access to your Mortgage Offset Account

If you default on your Home Loan Account, we can, and without giving you notice, use all or part of the balance in your Mortgage Offset Account to pay off all or part of the Loan.

Where the Mortgage Offset Account holder is a joint party to the loan

Where the Home Loan Account has multiple borrowers or guarantors, but the Mortgage Offset Account has been provided by only one of those parties, you acknowledge and agree that the other borrowers/guarantors may be able to see messages and notifications associated with payments and other messages addressed to a PayID which is linked to the Mortgage Offset Account, or details about the credit balance which is held in the Mortgage Offset Account. We only offset or combine where able to do so under the Code of Operation for Centrelink Direct Credit Payments, the ABA Banking Code of Practice and Customer Owned Banking Code of Practice (COBCOP).



7. Definitions

Access Card means an ATM card, debit card or credit card and includes our Visa card.

Account means an account you hold with us.

Additional Cardholder means a person 13 years or older nominated by you and authorised by us to operate your linked account(s) alone.

ADI means an 'authorised deposit-taking institution' as that term is defined in the Banking Act 1959 (Cth).

Adjustment in relation to Osko Payments means a transaction initiated by us or you to adjust or reverse an Osko Payment which has already been cleared and settled.

AFCA means the Australian Financial Complaints Authority.

ATM means automatic teller machine.

Authorised User means the user and any person the user has authorised to operate the account.

BECS Procedures means the Bulk Electronic Clearing System Procedures as existing from time to time.

BPAY® means BPAY® Pty Ltd (ABN 69 079 137 518).

BPAY® Scheme means the scheme operated by BPAY® which governs the way in which we provide Osko to you.

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 an Access Card or Digital Card (as the case may be).

Card Controls means the control functions available for any access card which is not expired, blocked, suspended or cancelled.

Card Details means the information printed on the access card, or displayed on the digital card, and includes, but is not limited to, the card number and expiry date.

Closed in relation to a PayID means a PayID which is removed from the PayID Service, and which you will no longer be able to use to make and receive Osko Payments.

Conditions of Use means these Account and Access Facility Conditions of Use.

Contactless means transactions made by holding or tapping an access card (which is capable of making a contactless transaction) in front of an electronic terminal without having to insert or swipe the card.

Contract means an agreement or arrangement under which you incur or owe obligations to us or under which we have rights against you and includes a guarantee and a mortgage.

Credit Card Accounts means any credit card we have issued to you including a Bank Australia Visa Credit Card, Low Rate Visa Credit Card, Commercial Visa Credit Card, Platinum Rewards Visa Credit Card, Secured Visa Credit Card and Credicard.

Device means a device we give to a user that is used to perform a transaction.

Examples include:

- ATM card
- debit card or credit card, whether physical or virtual
- token issued by us that generates a passcode

Digital Card means a digital Visa Debit Card or Visa Credit Card we issue to you or to any additional cardholder to access your linked account, the details of which will, at any time, be identical to the details of a physical card.

Digital Wallet means a mobile application which enables a user to make transactions using their access card or card details through a device, including contactless payments at an EFTPOS Terminal and online purchases.

Digital Wallet Provider means the person operating a digital wallet, for example Google (Android Pay).

Direct Debit means a "Direct Debit Request" as defined in the BECS Procedures.

EFTPOS means electronic funds transfer at the point of sale – a network for facilitating transactions at point of sale.

Electronic Terminal means the electronic equipment, electronic system, communications system or software controlled or provided by or on behalf of us or any third party for use with an access card and PIN to conduct a transaction and includes, but is not limited to, an ATM or point of sale terminal.

ePayments Code means the ePayments Code published by ASIC and available at asic.gov.au.

Facility means an arrangement through which you can perform transactions.

Gambling Transaction means any transaction identified by us as being for gambling or gaming purposes. Generally, we are only able to identify a transaction with a merchant as a gambling transaction based on information (including the type of business conducted by the merchant) provided by the merchant and the relevant intermediary financial institution (i.e. the financial institution with which the merchant has entered into an agreement, enabling the merchant to accept payment for goods and services by credit card). Accordingly, certain transactions made with certain merchants may be identified by us as gambling transactions, even though such transactions are not for gambling or gaming purposes. Similarly, we may not identify a transaction as a gambling transaction, even though the transaction is for gambling or gaming purposes.

Home Loan Account means the account we keep in your name with which we debit the Loan or any part of the Loan.

Identifier means information that a user:

- knows but is not required to keep secret and
- must provide to perform a transaction. Examples include an account number or PayID. An identifier also includes a token generated from information that would otherwise be an identifier.

Insolvency Event means any of the following:

- a person is or states that the person is unable to pay from the person's own money all the person's debts as and when they become due and payable
- a person is taken or must be presumed to be insolvent or unable to pay the person's debts under any applicable legislation
- an application or order is made for the winding up or dissolution or a resolution is passed or any steps are taken to pass a resolution for the winding up or dissolution of a corporation
- an administrator, provisional liquidator, liquidator or person having a similar or analogous function under the laws of any relevant jurisdiction is appointed in respect of a corporation or any action is taken to appoint any such person and the action is not stayed, withdrawn or dismissed within seven days
- a controller is appointed in respect of any property of a corporation
- a corporation is deregistered under the Corporations Act 2001 (Cth) or notice of its proposed deregistration is given to the corporation
- a distress, attachment or execution is levied or becomes enforceable against any property of a person
- a person enters into or takes any action to enter into an arrangement (including a scheme of arrangement or deed of company arrangement), composition or compromise with, or assignment for the benefit of, all or any class of the person's creditors or members or a moratorium involving any of them
- a petition for the making of a sequestration order against the estate of a person is presented and the petition is not stayed, withdrawn or dismissed within seven days or a person presents a petition against himself or herself
- a person presents a declaration of intention under section 54A of the Bankruptcy Act 1966 (Cth) or
- anything analogous to or of a similar effect to anything described above under the law of any relevant jurisdiction occurs in respect of a person.

Linked Account means an account nominated by you that we authorise you to access using an access card. If there is more than one account holder and/or more than one signatory, each account holder and each signatory must be authorised by us to operate the account alone.

Loan means the credit we give you under a Contract.

Locked in relation to a PayID means a PayID which we have temporarily disabled in the PayID Service.

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



Manual Signature means a handwritten signature, including a signature written on paper and a signature written on an electronic tablet.

Merchant means a retailer or any other provider of goods or services.

Migrated DDR Mandates has the meaning given in section 4.49.1.

Misdirected Payment means an Osko Payment erroneously credited to the wrong account because of an error in relation to the recording of the PayID or associated account information in the PayID Service.

Mistaken Payment in relation to a PayID means an Osko Payment, made by a user which is erroneously credited to the wrong account because of the user's error.

Mortgage Offset Account means the account that you have with us that we agree to be linked to your Home Loan Account so that we can offset interest in the manner set out under Section 6.1.

NPP means the New Payments Platform operated by NPP Australia Limited.

NPP Payments means electronic payments cleared and settled by participating financial institutions via the NPP.

Offset Amount means the amount calculated by multiplying the credit balance of your Mortgage Offset Account by the daily percentage rate applicable to your linked Home Loan Account. We calculate it as follows:

Step 1: We calculate the credit balance of the Mortgage Offset Account (after all transactions made).

Step 2: We ascertain the interest rate that currently applies to your linked home loan account.

Step 3: We multiply the balance of the Mortgage Offset Account determined in step 1 by the interest rate determined in step 2 and divide the result by 365 (being the number of days in the year) and in the case of a leap year, by 366.

Organisational Payer means a payer who is any of the following:

- an individual acting in their capacity as a trustee, sole trader or partner of a partnership
- a body corporate in its personal capacity or as a trustee
- a government agency
- an unincorporated body or association or
- a firm or partnership.

Osko means the Osko payment service provided by BPAY®.

Osko Payment means a payment made by or on behalf of a payer to a payee using Osko.

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
- code generated by a physical security token
- code provided to a user by SMS, email or in a mobile application.

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

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

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

PayID means a smart address for Osko Payments, composed of a permitted PayID Type linked to your nominated account.

PayID Name means the name we give you or the name that you choose which reasonably and accurately identifies you to payers when your PayID is used to make an Osko Payment.

PayID Service means the payment addressing service for sending and receiving Osko Payments.

PayID Type means a piece of recognizable and memorable information you select for receiving Osko Payments, which may be your telephone number, email address, Australian Business Numbers or other organisational identifications.

Payment Agreement means an agreement established by you and an approved Merchant or Payment Initiator, by which you authorise us to make payments from your Account. Other than in section 4.44 "Creating a PayTo Payment Agreement", it includes a Migrated DDR Mandate.

Payment Direction in relation to an Osko payment means a direction from a payer to effect an Osko Payment or Adjustment.

Payment Initiator means an approved payment service provider who, whether acting on behalf of you or a Merchant, is authorised by you to initiate payments from your Account.

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.

Recurring Payment Authority means either a recurring or an instalment payment agreement between you (the cardholder) and a Merchant in which you have preauthorised the Merchant to bill your account at predetermined intervals (eg. monthly or quarterly) or at intervals agreed by you. The amount may differ or be the same for each transaction.

Round UP is a phrase used to describe an optional feature on selected transaction and offset accounts that works by debiting the round up amount from one account and crediting it into a secondary account, usually a savings account.

Round UP Amount means the difference between the purchase amount of an eligible transaction made with an Access Card (including the information printed on it or a Digital Card) and the nearest \$1, \$5, \$10 (rounded up).

Service Provider in relation to Osko means a person engaged by BPAY® to provide goods or services to BPAY® in connection with Osko.

Transaction means a transaction to which the ePayments Code applies or which was processed through the new payments platform operated by NPP Australia Limited.

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 a user. It does not include any transaction that is performed by you or another user, or by anyone who performs a transaction with the knowledge and consent of you or another user..

User means you or an individual you have authorised to perform transactions on your account, including:

- a third party signatory to your account and
- a person you authorise us to issue an additional card to.

User Device means a mobile device capable of connecting to the internet which is compatible with a Digital Wallet application, and includes a smartphone, tablet or watch.

We, us and our means Bank Australia Limited (ABN 21 087 651 607).

You and your means the person or persons in whose name an account and access facility is held.

