Account and Access Facilities Terms and Conditions

Effective 11 June 2026

This document must be read together with the Fees and Charges Schedule and the Summary of Account and Access Facilities. Together these documents form the Conditions of Use for your Account and Access Facilities.

1300 364 400 www.unity.bank mail@unity.bank

Unity Bank Limited ABN 72 087 650 637 | AFSL & Australian Credit Licence 238311

Unity Bank

Unity Bank

Table of Contents

Introduction 4

About this document 4

Customer Owned Banking Code of Practice 4

ePayments Code 4

Privacy 4

About these Terms and Conditions 4

Accessing copies of Terms and Conditions 5

Financial Claims Scheme 5

How to contact us 5

Lost and stolen card hotlines 5

Definitions 5

Part A – Opening and operating your deposit accounts 6

What is an account and access facility? 6

How do I open an account? 6

Member numbers 7

Proof of identity requirements 7

Electronic & biometric verification 7

Joint accounts 7

Trust accounts 8

Accounts for children 8

Transitioning Accounts 8

Closing Children Accounts 9

Non-individual accounts 9

Fees and charges 9

Monthly account fee 9

What interest can I earn on my account? 9

Tax File Numbers (TFN) 10

Tax residency status 10

Third party access 10

Authorised Signatory 10

Power of Attorney (POA) 10

Confidentiality 11

Using an account or access facility 11

Deposit accounts 11

Transaction Accounts 11

Savings Accounts 11

Pensioner Plus Account 11

Term Deposits 11

Interest on Term Deposits 11

What happens at maturity? 11

Withdrawal Restrictions 12

Making deposits to an account 12

Depositing using electronic equipment 13

Depositing cheques 13

Withdrawing or transferring from an account 13

Over the counter withdrawals 13

Withdrawals using bank cheques 13

Cheque security 14

Stopping a bank cheque payment 14

Overdrawing an account 14

Transaction limits 14

Direct debits 14

Recurring payments 15

PayPal 15

Direct credits 15

Periodical payments 16

Account Statements 16

Change of name or address 16

Dormant and inactive accounts 17

Account combination 17

Sweep Facilities 17

Blocking transactions and access to your account 17

Closing accounts and cancelling facilities 18

Member Initiated Closure 18

Bank Initiated Closure 18

Notifying you about changes 18

Notices and electronic communication 19

Complaints and feedback 19

What to do if you have a complaint 19

Details of your complaint 20

What we will do if you have a complaint 20

What to do if you are not satisfied with the resolution 20

Customer Owned Banking Code Complaint 20

Feedback and compliments 20

Financial Hardship 20

Financial Abuse 21

Consumer Data Right 21

Part B – Electronic Banking and ePayments Conditions of Use 21

Section 1 – Information about your ePayment facilities 21
Visa card 22
Using your Visa card 23
Cancellation of a Visa card by us 23
Cancellation of a Visa card by you 23
When a Visa card has been cancelled 24
Visa Secure 24
Contactless transactions using payWave 24
Visa Click to Pay 25
Digital wallets 26
Section 2 – Definitions 27
Section 3 – Account and Transactions 30
Section 4 – When you are not liable for loss 30
Section 5 – When you are liable for loss 31
Section 6 – Passcode security requirements 32
Section 7 – Liability for loss caused by system or equipment malfunction 33
Section 8 – Network arrangements 33
Section 9 – Mistaken internet payments 33
Section 10 – Using Online Banking or Mobile App 35
Section 11 – How to report a loss, theft or unauthorised use of your Visa card or passcode 38
Section 12 – How to report unauthorised use of Online Banking or Mobile App 38
Section 13 – Using your Visa card for foreign currency transactions 38
Section 14 – Additional cardholder 38
Section 15 – Use after cancellation or expiry of Visa card 39
Section 16 – Exclusions of Visa card warranties and representations 39
Section 17 – Cancellation of Visa card or access to electronic banking or BPAY 39
Section 18 - Using BPAY payments facility ("BPAY") 39
Section 19 – Processing BPAY payments 40
Section 20 – Future-dated BPAY payments 41
Section 21 – Consequential damage for BPAY payments 41
Section 22 – Using Osko 41
Section 23 – Processing Osko payments 41
Section 24 – Scheduled and recurring Osko payments 42
Section 25 – Regular payment arrangements 42
Section 26 – PayTo 42
Section 27 – Confirmation of Payee 46
Other things you need to know 46
Request for Documents 46
Third party payment services 47
Inward Telegraphic Transfers 47
Outward Telegraphic Transfers 47
Account switching 48
Account verbal password 48
Money laundering and illegal activity 48
Comprehensive Credit Reporting 48
Collection and disclosure of information 49
Access to personal information 49
Accuracy and Correction 49
Instructions to us 49

Unity Bank

Introduction

About this document

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

These Terms and Conditions operate in conjunction with any additional terms and conditions which apply to accounts or facilities accessed by use of the service.

Other terms and conditions, including those implied by law, may also apply. To the extent permitted by law, these Terms and Conditions shall prevail in the event of any inconsistency.

Customer Owned Banking Code of Practice

We commit to complying with the Customer Owned Banking Code of Practice as varied from time to time, when it applies to an account or facility provided to you.

The Customer Owned Banking Code of Practice, the code of practice for customer owned financial institutions, is an important public expression of the value we place on improving the financial wellbeing of our individual members and their communities.

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

The Customer Owned Banking Code of Practice will apply if you are an individual or a small business (as defined in the Code).

You may obtain a copy of the Customer Owned Banking Code of Practice on request or download a copy from our website.

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

Phone: 1800 931 678
Mail: PO Box 14240, Melbourne VIC 8001
Email: info@codecompliance.org.au

ePayments Code

The ePayments Code may apply to the use of electronic payment facilities to make payments or withdraw funds from, or transfer funds to, your account.

Where it applies, we will comply with the ePayments Code. You can obtain a copy of the ePayments Code from ASIC's website www.asic.gov.au.

Privacy

In order to service you, we will collect personal information about you. We will handle it in accordance with our Privacy Policy and Privacy Notice.

We are committed to protecting your privacy. Our Privacy Policy contains information about how you:

- can request us to provide you access to any personal information about you,
- can seek correction of personal information we hold about you,
- may complain about a breach of an Australian Privacy Principle and how we will deal with such a complaint.

Our Privacy Policy is available on our website, on request by calling us, or at any of our Service Centres. We may make changes to our Privacy Policy from time to time for any reason. For this reason, we recommend that you review it on a regular basis.

You may request that we provide you with access to your personal information held by us in relation to your account by contacting our Privacy Officer, refer to the 'How to contact us' section.

About these Terms and Conditions

This introduction to these Terms and Conditions applies to both our deposit and credit products.

PART A - Opening and operating your deposit accounts, governs the use of our deposit accounts including transaction accounts, savings accounts and term deposits and cheque facilities associated with these accounts.

PART B - Electronic Access Facilities and ePayments Conditions of Use, governs the use of our electronic access facilities for all of our accounts including both deposit and credit accounts by:

- Visa card (including use of your card via digital wallets and contactless transactions)
- BPAY
- Electronic banking (online banking or mobile app)
- eftpos and ATM access
- Osko payments (including using PayID)
- PayTo
- Direct debit
- Direct credit

- Periodical payments

Accessing copies of Terms and Conditions

Please keep these Terms and Conditions in a safe place so you can refer to them when needed. Alternatively, you can download this document from our website.

Financial Claims Scheme

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

Funds are protected to a maximum of $250,000 for each account holder per institution. In the case of joint accounts, each account holder is entitled to a maximum of $250,000.

Unity Bank Limited is an ADI. Depositors with Unity Bank Limited may be entitled to receive a payment from the Financial Claims Scheme, subject to a limit per depositor.

For further information about the FCS, visit the website at www.fcs.gov.au

How to contact us

Visit us at any of our Service Centres (locations available on our website), send us a secure message within Online Banking, or by:

Phone: 1300 364 400

Mail: PO Box A253, Sydney South NSW 1235

Email: mail@unity.bank

Website: www.unity.bank

Lost and stolen card hotlines

If you believe your card has been misused, lost or stolen or your password or passcode has become known to someone else, you must contact us immediately on:

In Australia	1300 364 400 or 1800 648 027 – 24 hours a day, every day (7 days)
From overseas	+61 2 9307 5400 or +61 2 8299 9101
Visa Global Customer Assistance	+1 303 967 1090 (international)

Please contact us before you travel overseas to let us know you are travelling and for the current Visa hotline details.

To report any other unauthorised transaction or the loss of other access facilities, contact us directly.

Definitions

In these Terms and Conditions, these terms have the following meanings:

ABN	means an Australian Business Number issued by the Australian Taxation Office
Access facility	methods for you to access your account
Account	an account you hold with us
AFCA	the Australian Financial Complaints Authority
Apple Pay, Samsung Pay or Google Pay	mobile payment apps and/or digital wallet with the corresponding names that enables access to your cards
Bank@Post	the banking service provided at Australia Post Offices through which you can make withdrawals, deposits and balance enquiries
Biometric identifier	refers to any physical characteristic of an individual which assigns their unique identification (such as fingerprints or facial images)
BPAY payment	is an easy and secure way to make bill payments from within online banking. BPAY® is a trademark of BPAY Pty Ltd ABN 69 079 137 518
Card	a card includes our Visa Debit or Visa Credit card and any digital representation of those cards, including in a Digital Wallet (commonly called 'virtual cards') issued by us.
Cash advance	a debit to your Visa Credit card account (whether or not your Visa Credit card account is in credit or debit), which results in you receiving physical cash (whether at a Service Centre or via electronic equipment or by other means) or cash substitutes and includes: ▪ purchase of quasi-cash items such as cheques or travellers cheques; ▪ BPAY payments; ▪ any other transaction we reasonably consider to be a cash

	advance
Clear funds	The proceeds of: a) cheque deposits to your account (once the cheque is cleared); b) direct debits against non-Bank accounts (once the proceeds of the direct debit are cleared); c) cash deposits and direct credits; and d) Card credits and/or refunds that are processed using your card once those funds are no longer pending, less any outstanding card transactions.
Contactless transaction	a way to pay for a purchase by tapping your card or card/device on a payment terminal without having to sign or enter a PIN.
Consumer Data Right (CDR) Policy	the Consumer Data Right Policy (CDR Policy) explains how you may access and correct certain types of information that we hold about you, how to make a complaint, and how we deal with CDR complaints. The CDR Policy only relates to our obligations under the CDR Regime.
Credit limit	the credit limit for a Visa Credit card account set out in the Letter of Offer, and if varied, the credit limit as varied
Digital wallet	facility that enables the storage and use of a digital representation of your card
Fees and Charges Schedule	is our schedule specifying fees and charges that apply to the account available on our website
Interest Rate Schedule	is our schedule specifying interest rates that apply to the accounts available on our website
Member	someone who holds membership (by way of paid or unpaid shares) with Unity Bank Limited
Member number	your unique number we give you when you become a member. We generally allocate one member number regardless of the number of accounts you hold
Mobile App	our mobile app that allows you to bank electronically using your smartphone or tablet
Online Banking	online banking facility that enables you to access your account via an internet connection.
We, Us, Our or the Bank	Unity Bank Limited
You	the person or persons in whose name a Visa card or Account and Access Facility is held

Note: Within Part B – Electronic Banking and ePayments Conditions of Use, there are further defined terms used in the Code.

Part A – Opening and operating your deposit accounts

This Part A governs our deposit accounts, which includes transaction accounts, savings accounts, and term deposits.

What is an account and access facility?

Our account and access facilities include transaction and savings accounts and term deposits as well as these facilities for accessing accounts:

- Visa card (including use of your card via digital wallets and contactless transactions)
- Osko payments
- Online Banking or Mobile App
- BPAY
- eftpos and ATM access
- Direct debit
- Direct credit
- PayTo
- Periodical payments
- Bank@Post

Please refer to the Summary of Accounts and Access Facilities for available account types and the access methods attached to each account type.

How do I open an account?

You will need to become a member of the Bank before we can open an account for you. To become a member, you will need to:

- complete an application (this can be done in person at a Service Centre or via our website); and
- have a member share allocated

If you are unsure or have any questions about opening an account, please contact us.

Member numbers

When you join us, we give you a unique member number.

All of your accounts and payment services with us are linked to your member number. This means you will receive a regular statement for your membership which shows all of your savings and loan accounts.

Each account type also has a nine digit alternate reference number which can be located within your account listing in Online Banking and used for reference to transfer funds directly into a specific account.

Proof of identity requirements

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, attorney or an additional cardholder.

You'll be unable to operate any account until we have verified your identity. We are also required to identify you when you are transacting with us via a Service Centre and over the phone to confirm that we are dealing with the right person.

As a minimum, we require proof of your name and address on two separate documents, and in most cases, two of the following documents will provide proof of your identity:

- a State or Territory driver's licence;
- a photo identification document issued by a State or Territory;
- a current Australian passport or one that has expired within the last two years;
- a photo driver's licence issued by a foreign government;
- a passport issued by a foreign government, the United Nations or a United Nations agency;
- a national ID card with a photo and signature, issued by a foreign government, United Nations or a United Nations agency.

If you do not have a photo ID, please contact us to discuss what other forms of identification may be acceptable.

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

Electronic & biometric verification

We may use electronic and biometric verification to confirm proof of your identity. The Privacy Act and Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act authorise the use and disclosure of personal information contained in a credit information file by and between a credit provider (the Bank) and a credit reporting body for the purpose of verification of identification information.

This method of verification is permitted by amendments to the AML/CTF Act and the Privacy Act.

Biometric verification relies on advanced technology and government records. We collect, use and share your biometric information for the sole purpose of verifying your identity. In order to perform biometric verification, the following is required:

- A digital camera device to scan your Australian driver's licence or Australian Passport or any other specified identification document;
- A photo of yourself which will be used to match the photo on your identification document which you will be required to provide.

There may be some instances where you're unable, or do not consent, to verify your identity through biometric or electronic identification. In certain circumstances, we may permit you to provide certified copies of your ID to verify your identity or be identified in person at one of our Service Centres.

The law does not allow you to open an account using a false name or an alias. A false name is any name other than a name you are legally known by.

Joint accounts

If you open an account jointly with someone else, you authorise us to act on any instruction given by either of you, unless you both agree that all account owners must provide the instruction before we act on it. The default method of operation when setting up a joint account is 'any to sign' unless we are notified otherwise.
If you open a joint account, it can be operated by:

- All to sign – meaning that all joint owners must instruct us to operate the account (for example, all parties must sign a withdrawal slip, bank cheque request, etc), or
- Either to sign – means that you and your joint account owner can operate the account independently of each other and instructions about your account can be given by either of you (for example, only one party has to sign a withdrawal slip, bank cheque request, etc).

While all account owners must consent to make the account either to sign, any one joint account owner can cancel this arrangement, making it all to sign.

Any one joint account owner can also suspend the account to resolve any dispute between the joint account owners. Once a dispute is resolved, or in cases of separation, we can

convert an account from joint names to individual names following consent from both account owners. If a joint account owner is a victim survivor of financial abuse, we may remove them from a joint account without requiring other account owners to agree to this change.

If a card or electronic banking is required for a joint account, then the account must be operated by either to sign.

Irrespective of the method of operation on the account, all joint account owners will need to provide instructions to:

- close the account;
- withdraw or redeem a term deposit prior to maturity;
- appoint a third-party signatory to the account;
- change the address for delivery of statements or notices in relation to the joint account.

Other important things you need to know about joint accounts are:

- Credit balance – The credit balance is held jointly by all account owners;
- Survivorship – if one joint account owner passes away, we treat the balance of the account as belonging to the living account owner (for business accounts different rules may apply – see note below);
- Authority/Disputes – A joint holder may only make a withdrawal on the terms of any authority to operate on the account. If we become aware of a potential dispute between joint account owners or bankruptcy, we may decide to restrict the account and only permit operation of the account when all parties have signed the necessary authority;
- Joint and several liability – for all withdrawals and purchases and if the account is overdrawn, each joint account owner is individually liable for the full amount owing;
- Cheque payees – we may accept a cheque into a joint account which is payable to any one or more of the joint account owners.

Note: The right of survivorship does not automatically apply to joint business accounts, such as partnerships. A partner's interest in a business joint account would normally pass to beneficiaries nominated in the partner's will or next of kin if there is no will.

If you are operating a business partnership joint account, you should obtain legal advice to ensure your wishes are carried out.

Trust accounts

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

- we are not taken to be aware of the terms of the trust; and
- 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.

Accounts for children

Notwithstanding any other provisions in these Terms and Conditions, the following conditions apply to children's accounts:

- "child" or "children" means an individual or individuals under the age of 18 years;
- where an account is opened for a child, the child is the account owner and legal and beneficial owner of the funds in the account, irrespective of whether they are a signatory to the account, unless the account is set up with the objective of being a trust account;
- we do not open formal trust accounts with a child as beneficiary;
- we may set rules for the operation of children's accounts.

We may set an age under which a child who is an account owner cannot act as a signatory on their account. Where a child account owner is under 12 years old, the only signatory permitted is an adult relative.

Where a child who is an account owner attains an age at which we determine the child may act as a signatory:

- the child may be added as a signatory to their account; and
- the existing adult relative signatory on the account may remain as such until the child attains the age of 18 years, unless, prior to the child's 18th birthday, the adult relative is removed as a signatory.

Transitioning Accounts

From the time of opening their account until their 18th birthday, we may transition children through different account types, access facilities (including cards) and modes of account operation.

Where a child who is an account owner attains the age of 18 years:

- the child (then adult) member becomes the sole signatory on the account;
- any adult relative who is a signatory ceases to be such and no longer has any operating or access rights on the

account.

Closing Children Accounts

A child's account may be closed either by:

- the child, provided they are a signatory on their account; or
- an adult relative, where they are a signatory on the account; or
- both of the above.

Non-individual accounts

For non-individual entities, you must show us details of your certificate of incorporation, partnership agreement or other constitution documents. You must notify us if there are any changes to these documents.

We may enquire about the nature of the entity, including the likely types of transaction activity and volume of transactions.

We are required to verify the identity of each individual beneficial owner and controller of a non-individual entity. You'll not be able to use an account until all required individuals and entities have been identified.

Fees and charges

We charge service and administration fees for our products and services including:

- real time gross settlement payments
- dishonours
- paper statements
- dormant and inactive accounts
- card-related fees
- foreign currency transactions

Our current fees and charges (as well as government fees and charges) are set out in our Fees and Charges Schedule, which can be found on our website.

Monthly account fee

Members are exempt from the monthly account fee if they either:

- have held their membership for less than three months
- are under 25 years and over 65 years
- maintain the minimum combined balances of all savings, investments and drawn loans within the one membership over $5,000 for the whole calendar month

Business memberships are exempt from the monthly account fee if they maintain a minimum combined balance of $10,000 at all times throughout the month.
We may vary our fees and charges from time to time. If we do, we will make sure you are notified in accordance with the table in the 'Notifying you about changes' section.

We will debit your primary account for any fees and charges or applicable government taxes and charges.
From time to time, we may waive any of our fees or charges on an individual basis for members in financial hardship or with special needs. However, this doesn't mean that we will waive them in the future.

We will also deduct relevant government taxes and charges from your account. We won't be able to waive these. Please note that the government can change these without notice.

What interest can I earn on my account?

Please refer to our Interest Rate Schedule for current interest rates payable, which can be found on our website.

We calculate interest daily by applying the daily interest rate to the balance of cleared funds in your account at the end of the day. The daily interest rate is the relevant annual interest rate divided by 365. The end of the day is the time we set for our end of day transaction processing on your account.

Unless your account is a term deposit (please refer to the 'Term Deposits' section for more information), interest will be credited to your account on or about the last day of each month.

Tiered interest rates, where applicable, are based on ranges of dollar amounts. Generally, the higher the tier means the higher the interest rate.

Bonus interest is applied to certain account types on top of the base rate where the conditions specified in the Interest Rate Schedule are met.

We may change interest rates, the method of calculation or the frequency of interest payments by giving you prior notice of the change, however interest rates on Term Deposits remain fixed for the agreed term of the deposit.

For more information on how we give you notices in relation to interest rate changes, please see our 'Notifying you about changes' section.

If we make any changes to the interest rate, we will act reasonably and in accordance with our principles as a mutual organisation.

Interest earned on your savings and term deposit accounts must be declared for income tax purposes and may impact your income tax or any government benefits you receive.

Please refer directly to the Australian Taxation Office for information relating to income tax.

Certain thresholds may relate specifically to children's accounts. Refer to the Australian Taxation Office for information relating to these thresholds and quoting a Tax File Number (TFN) on a child's account.

Tax File Numbers (TFN)

When we issue you with a bank account and access facility, we will ask you for your TFN or an exemption. If provided, we will apply your TFN to each account and access facility you hold. You are not obliged to disclose your TFN to us. However, if you do not, we are obliged to deduct withholding tax from any interest you earn at the highest rate.

For a joint account, all holders must quote their TFNs and/or exemptions, otherwise withholding tax applies to the whole of the interest earned on the joint account.

The deduction of withholding tax may form part of your normal income tax, just as when your employer deducts tax from your salary or wages. When you fill out your tax return, including your interest earned, along with your regular income, you may be able to claim the withholding tax paid on the interest as tax already paid together with the tax your employer deducts from your salary or wages.

If you give us your TFN, we will not deduct withholding tax from interest that you earn on your account. However, you may still be required to disclose interest as income when you complete your tax return at the end of the financial year.

For business accounts and charities, you need only quote your Australian Business Number (ABN) instead of your TFN.

Tax residency status

When applying for a membership with us, you need to tell us your tax residency status. If you declare that you have tax obligations in another country, you must provide the relevant Tax Identification Number (TIN).

You also need to notify us of any changes to your tax residency status.

Third party access

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

Authorised Signatory

An authorised person can operate on all the accounts you have nominated them to have access to. You are responsible for all transactions your authorised person carries out on your accounts.

You should ensure that the person you authorise to operate on your accounts is a person you trust fully.

You can nominate the method of operating the account to be:

- any account owner or signatory to sign/either to operate (this is the default method unless stated otherwise). For example, you or your signatory can operate the account by signing for withdrawals;
- all account owners and signatories to sign (i.e. you and your signatory must both sign to operate the account by both signing for withdrawals etc), or another method which you specify and is acceptable to us.

Authorised signatories can operate the account but cannot manage the account. For example, an authorised signatory cannot:

- open or close accounts;
- receive statements;
- change an account owner's address details, or
- appoint other signatories.

These are the types of instructions only an account owner can provide. If we believe there is a dispute on the account, we may restrict the account and refuse to allow operation on the account until all parties have signed the necessary authority or instruction.

We can stop the authorisation at any time, as long as you send us a cancellation of your authorisation in writing.

Otherwise, the authority will remain in force until we receive and process a cancellation of authorisation in writing or written notice of the death of the person granting the authority.

Notice of cancellation must be signed by all surviving account owners. We may require a new Authority to Operate before we allow further operation of the account. An Authority to Operate will lapse if the account owner loses mental capacity.

If a card or electronic banking is required, then the account must be operated by either to sign.

For business accounts please contact us about applicable signatory options.

Power of Attorney (POA)

If you have appointed an attorney under a Power of Attorney (POA) to manage and operate your accounts, you can let us know and once we are satisfied of the validity of the POA and have verified to our satisfaction the identity of the attorney, we will accept all instructions from the attorney as if the instruction was made by you. This means your attorney will

have the same ability to manage your accounts and make transactions to and from the account as you have (subject to any restrictions you placed on their terms of appointment).

The limitations of an authorised signatory described previously don't apply to your attorney, although the attorney won't be able to delegate their powers to another person and won't be able to authorise others to deal with or operate your accounts. Your attorney's ability to manage your accounts is only limited in the same manner as you are limited, that is, by these Terms and Conditions, and by the terms of the appointment as your attorney.

If you revoke your attorney's appointment, you must tell us immediately in writing. Otherwise, we won't know, and they will continue to be able to access and operate your accounts.

Confidentiality

We will take reasonable steps to maintain the confidentiality of your account and personal details. However, there may be circumstances when we are obliged to disclose your account details or other personal information, for example when:

- you have given us your consent to do so;
- the law compels us to disclose your account details; or
- you have, by your conduct (but without actually telling us), released us from our duty to maintain the confidentiality of your account details.

Our Privacy Policy sets out how we do this. You should read our Privacy Policy which is available on our website. You can also contact us to request a copy.

Using an account or access facility

Deposit accounts

Transaction Accounts

We call our main at call savings account an Access Account (S1) or a BusiAccess Account (S82) for businesses. These accounts are usually opened when you become a member and are primarily designed as transaction accounts. If you have a loan, an offset account (where applicable) will be opened as your transaction account and then transferred to an Access Account once the loan has been paid out or discharged.

If you would like to earn higher interest on your savings, you should consider some of our other deposit accounts which provide a range of services and facilities. Refer to the Summary of Accounts and Access Facilities for more information.

Savings Accounts

We have a number of at call savings accounts including online savings accounts and reward based accounts with tiered interest rates or bonus interest when certain conditions are satisfied.

These accounts can be kept separate to your transaction accounts to assist with saving. Refer to the Summary of Accounts and Access Facilities for more information.

Pensioner Plus Account

If you receive an eligible government pension or allowance, or are a self-funded retiree, and over 55 years of age, then you may be able to open a Pensioner Plus Account.

Term Deposits

The minimum amount that can be invested in a Term Deposit is $1,000. Terms range from one month to five years.

To service your Term Deposit, we need you to open an accompanying Access Account in the same name(s) as your Term Deposit. It will be used to add or withdraw funds from the Term Deposit. If you don't have an accompanying Access Account to facilitate this, we will open an Access Account for you in the same name(s) as your Term Deposit.

Interest on Term Deposits

The interest rate on a Term Deposit is fixed for the term of the deposit. If we quote an interest rate for a Term Deposit, the rate may differ if the deposit is not made on the same day.

When you invest in a Term Deposit, you can elect for interest to be paid as follows:

- for Term Deposits of 12 months or less, interest can be paid monthly or at maturity;
- for Term Deposits of more than 12 months, interest can be paid monthly, annually and at maturity (the minimum interest payment frequency is annually).

Interest is calculated on closing daily balances. The daily interest rate is the relevant annual rate divided by the number of whole days in the year. We will not change the method of interest calculation or payment during the term of the deposit. Interest will be credited to your savings account, an external account or you can choose to reinvest it into your term deposit.

What happens at maturity?

You will receive an email or letter advising that your Term Deposit is maturing soon and to contact us to provide maturity instructions.

At maturity you may choose to withdraw or transfer your term deposit or it may be reinvested. You will also be able to increase or decrease the amount of your deposit if desired.

If you don't tell us before maturity that you don't want to re-invest your deposit, we will automatically re-invest your deposit for the same or similar term and the interest rate which applies at that time. In this case, you have up to 10 days after the maturity date (the "Grace Period") to tell us if you don't want this to happen:

- If you tell us during the Grace Period that you don't want to re-invest the Term Deposit or to make some other type of change, we will not charge an interest adjustment or apply a notice of withdrawal period.
- If you tell us within the Grace Period that you want to withdraw a partial amount from your Term Deposit or change the term, we will update your deposit with the new amount from the date of maturity.

If you decide not to re-invest your Term Deposit, the funds must be paid to an account in identical names to the Term Deposit, or as directed in the instructions you provided to us when opening the Term Deposit.

Withdrawal Restrictions

You cannot withdraw or transfer funds from a term deposit account prior to maturity unless you give us thirty one days' notice. The notice period commences on the first business day after you give us notice. If you believe you may need access to your funds prior to maturity, you should consider a shorter term or another deposit product.

Where you give us notice of early withdrawal and the maturity date is less than thirty one days from the date of notice, we will not release the funds until maturity.

Upon early withdrawal or transfer, we will reduce the interest payable. An adjustment may be required where we have paid interest to you prior to you making an early withdrawal. Where an adjustment is required, we will deduct the applicable amount from the deposit balance paid to you.

The reduced interest rate is calculated as follows:

Percentage of term elapsed	Adjustment to be applied as a % of the interest rate
0% to less than 20%	90%
20% to less than 40%	80%
40% to less than 60%	60%
60% to less than 80%	40%
80% to less than 100%	20%

For example, if your term deposit has been invested for 50% of the agreed term, then the interest rate adjustment to be applied will be 60%. Therefore, if the interest rate at the commencement of the term was 4.00% per annum, the interest rate that you will earn on the amount that you have withdrawn early will be 40% of the interest rate agreed at commencement of the term. The interest rate you would earn on the withdrawal amount is:

4.00% (p.a) – (4.00% x 60%) = 1.60% pa.

In special circumstances or emergencies, we may permit you to withdraw all or part of the funds lodged prior to the maturity date, without applying the interest rate reduction. No interest reduction shall apply where the Term Deposit is released early due to death of a depositor.

In the case of partial redemptions, the amount remaining will continue to earn the interest rate originally agreed until the date of maturity.

If the amount remaining is less than the minimum allowed for that type of Term Deposit, the whole balance must be redeemed and penalty interest will apply.

Making deposits to an account

You (or other people) can make deposits to your account by multiple means where those services are available on your account (refer to Summary of Accounts and Access Facilities):

- Electronic banking (Online Banking or Mobile App)
- Osko payments
- Service Centre
- Periodical payments
- Transfer from an account with the Bank or another financial institution
- Direct credit
- Bank@Post at participating Australia Post outlets

We try to process payments into your account promptly. Where possible, this will occur on the date of receipt. When we credit payments into your account, we use the account number specified by the sending bank. We don't use the account names, so please make sure that anyone depositing money into your account uses the correct account number.

To receive direct payments to your account from sources within Australia you must either use:

- BSB number (659 000), and your member number;
- BSB number (659 000), and your nine digit account reference number; or
- a registered PayID

Payments from overseas are unable to be received as a direct credit. You'll need to use a Telegraphic Transfer, Real Time Gross Settlement (RTGS) payment or an International NPP transaction.

Payments received by us with invalid account details will be reviewed and either credited to the correct account, where the account can be identified, or returned to the sender. A fee may apply for manual processing of this transaction.

Deposits can be made at any Australia Post outlet offering the Bank@Post service.

To make Bank@Post deposits you need your Visa card linked to a savings account. Deposits can be cash, cheques or a combination of both. For cash deposits, note that Australia Post may limit the amount of cash you can deposit each day using the Bank@Post service and may refuse to deposit excessive coins or small denomination notes.

Depositing using electronic equipment

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

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

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

Depositing cheques

You can only access the proceeds of a cheque when it has cleared.

Funds will be made available as follows:

- a cheque drawn on an Australian financial institution – three business days
- a cheque drawn on an overseas financial institution – forty five business days
- when a cheque is deposited via Bank@Post, – ten business days

We have a discretion to allow you to withdraw the funds of a cheque deposited to your account before it is cleared, but if the cheque is then dishonoured:

- we will debit the account for the amount of the cheque
- if this overdraws the account or exceeds any credit limit you have, you will need to bring the account back into credit or under the credit limit.

We may accept a cheque into a joint account which is made payable to one of the account holders, however we do not accept cheques into an individual account if the cheque is payable to joint payees, even if one payee has endorsed the cheque to the other. We do not accept cheques payable to a third party which have been endorsed to the account holder.

Withdrawing or transferring from an account

You can access your money by using the following services, where those services are available on your account (refer to Summary of Accounts and Access Facilities):

- Electronic banking (Online Banking or Mobile App)
- Osko payments
- Service Centres
- Visa Card
- Periodical payments
- Direct debit
- PayTo payments
- eftpos and ATM
- BPAY
- Bank@Post at participating Australia Post outlets

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.

Over the counter withdrawals

Generally, you can make over the counter withdrawals in cash or by having a bank cheque issued. Where a teller service is available at our Service Centres, cash withdrawals are limited to $3,000 per day. Larger amounts may be available with 24 hours notice, however we can decline any such requests at our discretion.

Withdrawals using bank cheques

This is a cheque we draw payable to the person you nominate and may incur a fee, see the Fees and Charges Schedule.

If a bank cheque is lost or stolen, you can ask us to stop payment on it which may incur a fee, see the Fees and Charges Schedule.

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

Cheque security

Stopping a bank cheque payment

You can stop payment on a bank cheque by:

- ringing us with sufficient particulars to identify the bank cheque; we may insist on written confirmation; or
- writing to us, again, with sufficient particulars to identify the bank cheque.

You must, of course, do this before the bank cheque has been paid. You may be charged a stop payment fee in accordance with our Fees and Charges Schedule.

You should tell the bank cheque payee that the bank cheque is stopped and not to present the bank cheque. If the bank cheque is presented after a stop payment has been placed on it, the bank cheque will be dishonoured by us and cheque dishonour fees will be charged and payable by you.

Overdrawing an account

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

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

- Interest at our current overdraft rate. We calculate interest daily by applying the daily interest rate to the balance of cleared funds in your account at the end of the day. The daily interest rate is the relevant annual interest rate divided by 365. Interest will be debited to your account on or about the last day of each month; or
- A fee for each direct debit presented whilst your account has insufficient cleared funds, see the Fees and Charges Schedule; or
- A fee where your account remained overdrawn or overlimit for 1 day or more during a calendar month, see the Fees and Charges Schedule.

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

If your account remains overdrawn for 60 days or more, we may need to report it to a credit reporting body. This could impact your credit score and your ability to obtain credit in the future.

Transaction limits

We limit the amount of daily withdrawals or payments you may make, either generally or in relation to a particular facility. These transaction limits are set out in the Summary of Accounts and Access Facilities. You may vary your transaction limits at any time through Online Banking, subject to any maximums or minimums set by us. Your daily limit will remain at the increased amount until you reduce it through Online Banking. Increasing these limits may increase your liability for unauthorised transactions.

We may, on application from you, agree to vary a transaction limit temporarily or permanently. We may, at our discretion, reduce the daily transaction limit or any other transaction limit applying to your accounts or payment type, or set it to zero for security reasons.

If we assist you through the Contact Centre and agree to a temporary or permanent limit increase, we will tell you the maximum number of days that your limit will remain in place. For limit increase requests, we may require additional information relating to the request to assess possible risks or potential scams, or require other security measures to be completed before processing the request, these may include passwords, SMS One Time Passwords, security codes or other measures we deem appropriate. A limit increase may increase your liability in the case of unauthorised transactions, including any requests for limit increases on Business memberships.

A contactless transaction made on a Visa 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.

Direct debits

You can authorise a participating remitter to debit amounts directly from your account, as and when you owe those amounts to the remitter.

The remitter will provide you with a Direct Debit Request (DDR) Service Agreement for you to complete and sign to provide them with this authority.

To cancel the DDR Service Agreement, you can contact either the remitter or us. If you contact us, we will promptly process your instruction to cancel the remitter's authority. However, we suggest that you also contact the remitter.

If you believe a direct debit initiated by a remitter is wrong, you should contact the remitter to resolve the issue. Alternatively, you may contact us. If you give us the information we require, we will forward your claim to the remitter. However, we are not liable to compensate you for the remitter's error.

You can also provide us with direct debit instructions yourself

to make periodical payments from your account. You must give us at least three business days' notice in writing to stop any direct debit you have instructed us to make.

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.

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

We can immediately cancel or suspend your direct debit facility as we reasonably consider appropriate in these 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
- your account becomes dormant.

If we do this, remitters 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 remitter may charge you a fee for each dishonour of their direct debit request.

Recurring payments

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

If you set up a recurring payment on your Visa card it will be processed as a Visa payment, not a direct debit and will be processed in accordance with the Visa Scheme rules.

To cancel or update a recurring payment on your Visa card you will need to contact the merchant or service provider directly. You should always consider any terms and conditions the merchant or service provider may have regarding cancelling a recurring payment.
If your Visa card expiry dates change, it's your responsibility to tell the merchant or service provider.

The above sections on direct debits and recurring payments relate to transactions under the BECS procedures and does not apply to payments and arrangements under the PayTo service (see section 26).

PayPal

When you use PayPal you are authorising PayPal to debit amounts from your account as a remitter 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.

Direct credits

Electronic credits to your account are credited in accordance with our obligations under the rules, regulations and procedures of the payment or funds transfer system that the electronic credit was received through.

Direct credits (which do not include Osko Payments received for your account) received daily are processed no later than 9am the next working day.

Osko Payments received for your account will be credited to your account as soon as reasonably practicable.

We are not liable for any delay in the crediting of your payment to your nominated account.

Payments made to accounts in error may be recalled by the remitting institution. We do not accept liability for funds credited in error to accounts due to incorrect account number and/or account name being supplied by the remitter.

- Where there are sufficient funds to cover the recalled amount, we will debit the account credited for the

amount of the incorrect credit

- Where there are insufficient funds to cover the recalled amount, you agree to incur and repay the debt up to the amount of the recalled amount and any associated fees incurred in retrieving these funds where the amount exceeds the balance of the account credited.

Payments received with invalid account details will be either credited to the correct account, where the account can be identified, or returned to the remitter.

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 us immediately.

Periodical payments

If you set up periodical payments, the order in which we process the payments is at our absolute discretion.

Where reasonably necessary, or if instructed by you, we can stop any periodical payment arrangements at our discretion. Similarly, we can continue to effect periodical payments until you advise us otherwise.

We will normally debit your account on the date nominated. You must have enough cleared funds available in your account to cover processing of the periodical payment on the day it is due.

If you have set up periodical payments on a loan provided by us from an internal savings account, we will make a number of attempts to debit loan repayments from your nominated account on the due date. This will include the full amount of the periodical payment if sufficient cleared funds are held in the source account or partial payment up to the account balance if there are insufficient funds available.

While we will generally debit your account on the day you have nominated, you should allow sufficient time for your periodical payment to reach the destination account. Your periodical payment may be delayed:

- where additional time is required to process your request (for example, because of the payment system rules);
- in circumstances beyond our control; or
- where we reasonably consider it necessary or prudent.

Where your payment is delayed due to one or more of the circumstances listed above, we accept no responsibility for the delay, and we shall not incur any liability due to late payment.

If three successive periodical payments fail, the authority will normally be cancelled automatically.

However, this may not be the case if a periodic payment has been established to meet a minimum loan repayment.

Any request to stop a payment may be required in writing. Alternatively, you are also able to adjust or cancel periodical payments in Online Banking or through our Mobile App.

Amendments will not be accepted to the payee account details. To amend the payee account details, the current authority must be cancelled, and a new authority given advising us of the account details. A cancellation of any request may be arranged at a Service Centre, over the phone, through our Mobile App or via Online Banking.

Account Statements

We will send you account statements either monthly or at least every six months depending on your account. However, we will not give you a statement of account or may give you statements of account less frequently where permitted under applicable law, the ePayments Code and for accounts that are dormant. You can also ask us for a statement at any time, however we may charge a fee for providing additional statements or copies, see the Fees and Charges Schedule for more information.

Statements are provided electronically through Online Banking as part of our eStatement facility unless you:

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

Where we are required to provide you with paper statements we may charge a fee, see the Fees and Charges Schedule.

For joint accounts, only the first named owner will receive a statement for that account. The first named owner agrees to act as agent for all other joint account owners in receiving these statements. Other joint owners can request a separate statement.

You can nominate someone else to receive statements on your behalf and in doing so, you agree that they act as your agent in receiving those statements.

You should check your account statement as soon as you receive it and immediately tell us of any unauthorised transactions or errors.

Change of name or address

If you change your name or address, please contact us

immediately or update your details through Online Banking.

If your name changes, you must provide us with a certified copy of your marriage or change of name certificate. We may ask you to present your documents at a Service Centre.

Dormant and inactive accounts

If no transactions are carried out on your account for at least 12 months (other than transactions initiated by us, such as crediting interest or debiting fees and charges) we may write to you asking if you want to keep the account open or to reactivate the account by making a transaction. If you don't reply, we will treat your account as inactive.

Once your account becomes inactive, we may charge an inactive fee each year and/or stop paying interest or reduce the amount of interest.

If you wish to reinstate your accounts and membership we will require copies of identification documents.

If your account remains inactive for seven years, we will treat your account as dormant. We have a legal obligation to remit dormant balances exceeding $500 to the Australian Securities and Investment Commission (ASIC) as unclaimed money.

We can assist you in making a claim for unclaimed monies which have been remitted to ASIC from your account with us.

Account combination

We may set off the credit balance of any of your deposit accounts against any debt owing by you to us from time to time.

We reserve the right to transfer funds from any of your deposit accounts to another, where the accounts are held in the same name. This may be necessary if, for example, one of your accounts becomes overdrawn, or in payment of any amount overdue on any loan account held in the same name. We will have regard to any dispute between joint account holders or any circumstances of financial hardship of which it is aware when considering transferring of funds.

However, this transfer of funds will not occur where we know the funds are not held in the same capacity.

Further, where we are bound by a specific code, there may be limits on the extent to which funds from your various accounts may be transferred.

Consistent with the Customer Owned Banking Code of Practice, we will, where possible, advise you if it has been necessary to transfer funds between your accounts. However, we are under no obligation to tell you of our intentions prior to transferring funds between your accounts. Furthermore, you should not assume that we will automatically transfer funds to an overdrawn account from an account which is in credit.

Sweep Facilities

We currently have existing sweep facilities on legacy products where you may nominate an account (the first account) which is to have either a nominated minimum balance or to be maintained in credit. You may then nominate a second account, which authorises us to transfer, automatically, sufficient funds to keep the first account at its nominated balance or in credit. However, we are not obliged to transfer funds if there are insufficient funds in the second account to draw on. This facility offering is no longer available.

Blocking transactions and access to your account

We can delay, block, freeze or refuse a transaction or suspend an account, or suspend access to an account, without prior notice to you, where we believe:

a) the transaction may breach a law or sanctions;

b) the transaction involves fraudulent or illegal activity;

c) a payment was sent to your account in error;

d) doing so will protect you or us from incurring a loss;

e) the funds involved in the transaction may directly or indirectly be applied for the purposes of criminal or unlawful conduct;

f) there is significant risk to our business which exceeds our internal policies or risk appetite;

g) the transaction is not in the Account Holder's interest, (for example: where we think the Account Holder is in a vulnerable position due to illness, cognitive impairment, financial illiteracy, domestic violence, elder abuse, financial abuse or other similar circumstance);

h) security concerns (for example, if we know or suspect that your payment device and/or security details have been compromised or misused;

i) behaviour by you was offensive, threatening, controlling, intimidating, abusive or caused harm to another person (including our staff); or

j) the action is otherwise reasonably necessary to protect our legitimate interests (which includes our legitimate business needs, reputation, prudential requirements, material changes to our business or systems, security requirements or to manage regulatory risk).

If a transaction is delayed, blocked or refused for any of the above reasons, we are not liable to you for, and you indemnify us against, any and all loss incurred by you or any other person arising from such delay, block or refusal of a transaction or application.

Visa Credit Cards cannot be used for any gambling, lottery or gaming transactions and authorisations will be declined.

These transactions are identified by us based on the merchant category code. The category is based on information provided by the merchant and their financial institution and in some circumstances may not characterise all transactions correctly. The most common types of merchants where this may occur are newsagencies that sell lottery tickets. There will be instances where we are unable to block a gambling or gaming transaction, in which case you are still responsible and liable for those transactions.
From time to time, we are required under Australian law to obtain additional information from you. If you don't provide the information within a reasonable timeframe, your account may be blocked, suspended or frozen.

We are not liable to you for, and you indemnify us against, any loss or damage caused (including consequential loss) as a result of us blocking, suspending or freezing your account in these circumstances.

Closing accounts and cancelling facilities

Member Initiated Closure

You can close your account or an access facility at any time. However, you will have to surrender any member deposit book and any Visa cards at the time. We may defer closure and withhold sufficient funds to cover payment of outstanding bank cheques, EFT transactions and fees, if applicable.

You can cancel any access facility on request at any time. However, for direct debit:

- you can contact your remitter or us to cancel any Direct Debit you have given a remitter; and
- you have to give us at least three business days notice to cancel any Direct Debit Authority you give us.

To close a joint account, we need consent from all account holders. Any one signatory cannot close a joint account.

Bank Initiated Closure

We can cancel any access facility for security reasons or may close your account under these Terms and Conditions if that account is in credit. If we do so, we will act fairly and reasonably towards you and we:

a) will, if appropriate, give you reasonable notice of the closure;

b) will pay you the amount of the credit balance; and

c) may charge you an amount that is our reasonable estimate of the costs (fees and/or interest) outstanding upon closing your account.

We can close your account immediately and without notice if any of the following occur:

- your account has been operated in a manner we reasonably consider is unsatisfactory or inconsistent with these Terms and Conditions;
- you engage in behaviour that is illegal;
- your account may be being used unlawfully including fraudulently or as part of a possible scam or in any way that might otherwise cause you, us or a third-party to lose money;
- your behaviour is unreasonable or improper for example you act in a threatening, defamatory, harassing, controlling or violent manner towards staff;
- you promote or encourage physical or mental harm of any person (including use of payment descriptions and/or references);
- we reasonably suspect you have used our products to perpetrate financial abuse on another person; or
- you do not provide us with any document or information we reasonably request from you.

We can also, at our discretion, terminate your membership in certain circumstances (including where you have no products with us). Our Constitution sets out when memberships can be terminated.

Notifying you about changes

We may change fees, charges, interest rates and other conditions at any time. We may use various methods, and combinations of methods, to notify you of these changes, such as:

- by post;
- electronically through email, SMS or secure messaging within Online Banking;
- publishing it on our website;
- on or with your next statement of account;
- on or with the next newsletter;
- advertisements in the local or national media;

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

The minimum notice period we will give you for a change is as follows:

Type of change	Notice
Increasing any fee or charge	20 days
Adding a new fee or charge	20 days
Changing interest rates	Day of change
Changing the method by which interest is calculated	20 days
Changing the minimum balance to which an account keeping fee applies	20 days
Changing the circumstance when interest is debited or credited to your account	20 days
Increasing your liability for losses in relation to EFT transactions	20 days
Imposing, removing or adjusting daily or periodic limits in relation to EFT transactions	20 days
Changing any other term or condition	Day of change

We are not required to provide advanced notice for the following changes:

- the reduction or cancellation of daily card limits for cash withdrawals, purchases and transfers using electronic banking by holders or users, or
- other changes to terms and conditions, required to immediately restore or maintain the security of a system or an individual facility, including the prevention of systemic or individual criminal activity, including fraud.

Notices and electronic communication

We may give you notices and other communications and documents relating to your account and access facilities and these Conditions of Use in any way allowed by law, the Customer Owned Banking Code of Practice and the ePayments Code (where those codes apply).

Subject to any applicable legal requirements and any applicable provisions of the Customer Owned Banking Code of Practice and the ePayments Code, you agree that we may give you written notices and other communications and documents:

- by post, to the address recorded in our membership records or to a mailing address you nominate; or
- electronically through email, SMS or secure messaging within Online Banking;
- publishing it on our website;
- on or with your next statement of account;
- on or with the next newsletter;

You may elect to receive notices and other communications and documents we are required to give you in writing in paper form by post at any time by changing your communication preference by contacting us by telephone. If you make this election, you will also be taken to have elected to receive statements of account for all your deposit accounts and credit contracts, except credit card contracts, in paper form by post and the Paper Statement Fee specified in the Fees and Charges Schedule will apply.

If you have not given us electronic contact details, we may treat you as having elected to receive notices and other communications and documents in paper form by post until you provide electronic contact details to us.

Even when you have elected to receive notices and other communications and documents in paper form by post, we may also give them to you electronically. We may also send you notices and statements by some other way that you have agreed to.

If you agree, we may, instead of sending you a notice or statement, post notices or statements to our website for you to retrieve.

You can vary your nominated email address, or cancel arrangements to receive notices or eStatements at any time.

Complaints and feedback

If we can improve our services, we welcome your feedback. If you have any issues, suspect an error, or have any concerns about your accounts, we genuinely want to help resolve them.

We have a dispute resolution system to deal with any complaints you may have in relation to your account and access facility or transactions on your account. Our dispute resolution policy requires us to deal with any complaint efficiently, promptly and sympathetically.

What to do if you have a complaint

You can access our complaint resolution service in the following ways:

Phone: 1300 364 400

Mail: PO Box A253, Sydney South NSW 1235 (attention to the Complaints Officer)

Email: mail@unity.bank

Website: www.unity.bank

Online form through our website or through

secure messaging in Online Banking

Our staff have a duty to deal with your complaint under our dispute resolution policy. Our staff must also advise you about our complaint handling process and the timetable for handling your complaint.

We also have an easy-to-read guide to our complaints and dispute resolution process available to you on request and on our website.

Details of your complaint

To help us resolve your concerns it's important to give us all the information you have, such as account information, contact details, detailed information regarding your complaint and how you would like your complaint to be resolved.

If we receive everything, we will be able to properly investigate your complaint and work towards a resolution.

What we will do if you have a complaint

Once your complaint is made to us, we will acknowledge your complaint (generally by the next business day), give you a reference number, and let you know the name and contact details of the person who's handling it as soon as we can.

Our aim is to have your complaint resolved as soon as practical, although we may need up to 30 calendar days. In exceptional circumstances, a resolution may take longer than 30 calendar days, in which case we will keep you informed of the progress of our investigations and provide you with notification of the delay as well as an explanation.

If your complaint is related to hardship, it will be referred to a specialist in this area, and we will aim to respond to you within 21 calendar days.

What to do if you are not satisfied with the resolution

If you are not satisfied with the way in which we resolve your complaint or the speed at which we respond, please raise this with our Complaints Officer.

If your complaint is still unresolved after 30 days, you can lodge a complaint with the Australian Financial Complaints Authority (AFCA), which is an independent external dispute resolution body that is free to consumers. You can contact AFCA at:

Phone: 1800 931 678

Mail: GPO Box 3, Melbourne, VIC 3001

Email: info@afca.org.au

Website: http://www.afca.org.au

AFCA requires you to contact us in the first instance to try to resolve your complaint.

Customer Owned Banking Code Complaint

If you have a complaint about our compliance with the Code which does not involve financial loss, you can contact them through:

Email: info@codecompliance.org.au

Website: www.cobccc.org.au/for-consumers/resolving-complaints/

Mail: Customer Owned Banking Code
Compliance Committee
PO Box 14240
Melbourne VIC 8001

The Code Compliance Committee (CCC) is an independent committee established in accordance with the Code, to ensure that subscribers to the Code meet the standards of good practice set out in the code. The CCC investigates allegations that the Code has been breached and monitors compliance with the Code through compliance activities such as mystery shopping, surveys and compliance visits.

Please be aware that the CCC is not a dispute resolution body.

Feedback and compliments

If you have any other feedback, or would like to give us a compliment, please speak to our staff at any Service Centre, through our contact centre, website or via email.

Financial Hardship

If your financial circumstances change due to unexpected life events such as job loss, accidents, illness, relationship breakdown, or natural disasters which make it difficult for you to manage your debts and to make repayments, please call us as soon as possible to discuss the situation and your options.

We have a centralised financial hardship team and our approach is to actively assist any member experiencing financial difficulty.
Knowing early increases our ability to work with you and assess your situation on a case by case basis.

We will work with you to tailor a suitable plan and will suggest solutions based on the nature of your financial hardship (short term, where restoring your financial position is possible in a few months, or long term, where it may take longer than a few months). Depending on the nature of your circumstances, we offer a range of options to help best suit your needs, including:

- deferral of repayments for an agreed period of time
- tailored payment arrangements, such as reducing the amount of each payment due
- short-term concessional interest rates
- providing interest-only repayment options on loans
- providing fee waivers
- reducing the limit available on credit contracts; and
- suspending recovery processes to allow you time to get back on your feet

To enable us to better assess your situation, we may need additional information or documentation from you relating your situation, current and projected financial position.

We also understand that at times you may like to have a friend, relative or third-party representative such as a financial counsellor deal with us, on your behalf. Should this be the case, we require written authority to discuss your personal and account information first to maintain your privacy and then can work together to get you back on track.

If you are in a tough situation financially, please call us on 1300 364 400 or refer to our website at https://www.unity.bank/financialhardship for more information.

Financial Abuse

Financial abuse occurs when a trusted individual manipulates or compromises the financial decision-making of an individual. It is a serious form of domestic and family violence or elder abuse and often involves misusing or taking control of a partners or family members' money, financial resources, property or assets, without their knowledge, consent or understanding.

Financial abuse includes, but is not limited to:

- behaviour such as taking control of, or spending a person's finances without their knowledge or consent;
- restricting someone's access to their own money;
- refusing access to view statements;
- withholding someone's card from them;
- coercing someone to apply for credit or provide guarantees; or
- abusing Power of Attorney or Authority to Operate privileges.

You must not use your account, card or any other facility we provide, in a manner that is intended to control, threaten, harass, humiliate or cause harm to another individual, including through financial abuse.

A bank account is no place for abuse and has serious impacts on victim survivors. We are committed to monitoring account activity for possible warning signs where intervention and assistance may be required. In accordance with our Terms and Conditions section 'closing accounts and cancelling facilities' we will close your account without notice if we reasonably suspect improper conduct or offensive, threatening or controlling behaviour or that you have used our products to perpetrate financial abuse on another person. Where warranted, we will also report suspicion of financial abuse to law enforcement.

For joint accounts, where we reasonably believe that a joint account holder is experiencing financial abuse (or other harm), we will take appropriate measures to safeguard that person. This may include refusing to execute a transaction, removing access to functionality, freezing the account, or closing the account entirely.

If you are impacted by domestic or family violence, please contact us and we can work with you to provide tailored support, changes to your account access or assistance in opening a new membership, if required. We will discuss safe ways to contact you and refer you to external specialist support providers if appropriate.

Consumer Data Right

Consumer Data Right (CDR) gives our members the ability to share banking data with third parties that have been accredited by the Australian Competition and Consumer Commission (ACCC).

Management of your CDR Data is performed via the Data Sharing Dashboard in Online Banking.

For further information about CDR, please refer to the Consumer Data Right Policy, which is available on our website.

Part B – Electronic Banking and ePayments Conditions of Use

Section 1 – Information about your ePayment facilities

You should follow the guidelines in the box below to protect against unauthorised use of the mobile app, online banking or your Visa card and passcode. These guidelines provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised ePayments.

Liability for such transactions will be determined in accordance with these ePayments Conditions of Use and the ePayments Code.

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

- Visa card (including use of your card via digital wallets and contactless transactions)
- BPAY
- Electronic banking (Online Banking or Mobile App)
- Eftpos and ATM access
- Osko payments (including using PayID)
- Direct debit
- Direct credit
- PayTo payments
- Periodical payments

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

Important information about protecting your cards, devices and passcodes

- Make reasonable attempts to protect your passcode such as hiding or disguising it among other records or in an unexpected place, keeping it in a securely locked container, password protecting it if electronically stored.
- Do NOT act with extreme carelessness in protecting the security of your passcode.
- Familiarise yourself with your obligations to keep your Visa card and passcodes secure.
- Familiarise yourself with the steps you have to take to report loss or theft of your Visa card or to report unauthorised use of your Visa card, BPAY, Online Banking or Mobile App.
- Immediately report loss, theft or unauthorised use.
- If you change a passcode, do not select a passcode which represents your birth date or a recognisable part of your name.
- Never write the passcode on the Visa card.
- Never write the passcode on anything which is kept with or near the Visa card.
- Never lend the Visa 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 our phone number with your usual list of emergency telephone numbers.
- Check your statements regularly for any unauthorised use.
- Immediately notify us when you change your address.
- ALWAYS access Online Banking or Mobile App services only using the OFFICIAL phone numbers and URL addresses.
- If accessing Online Banking or Mobile App on someone else's computer, 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 Visa card, access facility and passcodes or you fail to promptly tell us about a security breach on your account you may increase your liability for unauthorised transactions.

Visa card

A Visa card allows you to make payments at any retailer displaying the Visa logo, anywhere in the world. You can also withdraw cash from your account, anywhere in the world, using an ATM displaying the Visa logo. We will provide you with a Personal Identification Number (PIN) to use with your Visa card or the option to select your own PIN through Online Banking or our Mobile App. Your Visa card allows you to:

- check your account balances;
- withdraw cash from your account;
- transfer money between accounts;
- purchase goods and services
- deposit cash or cheques into your account (at select ATMs only)

All cards are issued at our discretion and we may determine the level of functionality made available in our cards.

We may choose not to provide you with a card if your banking history with us is not satisfactory or due to age restrictions. The use of a Visa Credit Card is subject to Credit Card Terms and Conditions and the terms of your loan contract.
We may also provide you with a digital copy of your Visa card that is embedded into our Mobile App. You can use your digital Visa card just like your physical Visa card to shop

online, pay bills, make in-app purchases and set up your recurring card payments or add it to your digital wallet.

Using your Visa card

You must not use a Visa card for any unlawful purpose, including the purchase of goods or services prohibited by the laws of the jurisdiction of purchase.

The maximum daily cash advance amount for an account is AUD$2,000.

Cash advances from ATMs will only be available upon entry of the correct PIN in conjunction with the use of the Visa card.

We may, where we think it's reasonably prudent, put temporary or permanent blocks on a merchant, group of merchants or a geographical region that will prevent you from using your Visa card with those merchants or in that region. We may do this without notice to you. Usually we will only do this where we believe there is a high risk of fraud or criminal activity associated with those merchant(s) or region, a customer or we are exposed to an unacceptable risk, or where we are obliged by law to take such action.

Authorisations

Before any transaction is made, the merchant or other person involved in the transaction may obtain an authorisation for the transaction. This authorisation is for the purpose of establishing that there are sufficient funds available for the transaction.

Once the authorisation is obtained, we may reduce the amount of available funds in the Visa card account. If the purchase or other transaction is not completed, the amount of available funds in the Visa card account may continue to be reduced until the merchant charges your card for the purchase and clears the authorisation or cancels the authorisation as the purchase is not proceeding.

We may choose at any time not to authorise a transaction. We shall not be liable to you or anyone else for any loss or damage resulting from our refusal to authorise a transaction.

You agree that we can debit the Visa card account with all transactions authorised by you.

Transactions can be authorised by:

- using your Visa card, alone or together with your PIN, at any electronic terminal; or
- providing the Visa card account details to a merchant or to any other party to whom payment is to be made, either directly or via a third party, in a manner acceptable to us, for example, over the phone or online.

You can authorise a transaction for either a particular amount or for particular goods or services. For example, if you hire a car, you may authorise a transaction for both the rental and any additional costs, such as the cost of any damage to the vehicle.

When you authorise a transaction:

a) you are confirming the validity of the amount of the transaction, that is, the transaction correctly represents
   - the purchase price of the goods or services obtained; or
   - the amount of the cash advance;

b) you agree to pay (in Australian dollars) the amount of that transaction; and

c) you agree that, when transacting with a Visa Credit card, we provide you with credit equal to the amount of the transaction on the date on which you make the transaction.

Cancellation of a Visa card by us

Visa cards remain our property at all times. We will not cancel any individual Visa card(s) without good reason.

We reserve the right to cancel any Visa card at any time without prior notice if:

- we believe that use of the Visa card or the card account may cause loss to you or to us (for example, if you are in default under a Credit Card loan contract or under the Conditions of Use applicable to another credit facility provided by us to you);
- the Visa card account is an inactive account;
- the Visa card account has been closed; or
- a Visa Credit Card credit limit has been exceeded. (Note that we may elect not to close a Visa Credit card account for this reason, but the fact that we have elected not to do so on one or more previous occasions does not stop us from closing a Visa Credit card account whenever the credit limit has been exceeded).

If the Visa card account is closed, all Visa cards issued in relation to that Visa card account will also be cancelled.

Cancellation of a Visa card by you

You may close the Visa card account at any time by making a written request to us for closure of the account. If the Visa card account is closed, all Visa cards issued in relation to that account will also be cancelled.

You may cancel any Visa card linked to the account (including any additional card) at any time at a Service Centre, over the

phone or by making a written request to us for cancellation of that Visa card. You will not be liable for any losses resulting from unauthorised use of the subsidiary card following cancellation.

When a Visa card has been cancelled

When we cancel a Visa card or we receive instructions from you to cancel a Visa card:

- we will confirm the cancellation details with you; and
- the Visa card (and any additional card) must not be used. To reduce the risk of identity fraud, please securely destroy the card. You should take all reasonable steps to retrieve additional cards from an additional cardholder.

If the Visa card account has a credit balance when the card account is closed, we will:

- credit the credit balance to any other account held by you with us;
- transfer the credit balance by direct entry to another financial institution nominated by you; or
- send you a bank cheque for the closing credit balance of the account.

You will continue to be liable for any of the following transactions on your account:

- transactions made before we process your termination request; and
- any transactions debited to the Visa card account in accordance with any regular payment or any other authorised link to the account until the regular payment or authority is cancelled; and
- in the case of Visa Credit Cards, you must continue to make payments to the Visa Credit Card account in accordance with the Credit Card loan contract while a balance remains outstanding.

Upon receipt of your request for closure we will immediately cancel the card.

Any regular payment arrangement must be cancelled directly by you with the other party.

Visa Secure

The Visa Secure service is designed to provide you with improved security when your Visa card is used to make a purchase online. We encourage you to join the growing number of users who enjoy additional security by using the Visa Secure service and by shopping at participating Visa Secure online merchants.

These Terms and Conditions govern the Visa Secure service and form the agreement between you and us regarding the use of the service, so please read them carefully.

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

By completing or attempting to complete a Visa Secure transaction, you are deemed to accept the Visa Secure Terms and Conditions and you are bound by these each time you use Visa Secure.

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

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

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

Contactless transactions using payWave

If your physical Visa card has the payWave logo displayed on the card that means that your Visa card is enabled to make contactless transactions at eftpos terminals. You do not need to swipe and enter your PIN or sign your name to perform transactions under the relevant authorisation limit. You can simply tap your Visa card on the eftpos terminal.

Limits for contactless transactions apply as set by the relevant card schemes (e.g. Visa). We may at our discretion apply a lower or higher daily transaction limit to contactless transactions performed via certain:

- types of cards;
- card/devices; or
- third party payment services/digital wallets.

If you exceed your payWave maximum limit for the day, you'll still be able to use your card by entering a PIN.

Important information about disputed transactions for your Visa card

If you believe a Visa card transaction was:

- unauthorised
- for goods or services and the merchant did not deliver them and a refund or credit was not offered or provided by the merchant; or
- for goods and services which did not match the description provided by the merchant and a refund or credit was not offered or provided by the merchant,

then you can ask us to lodge a dispute and seek a reversal of the transaction (sometimes referred to as 'chargeback'), by reversing the payment to the merchant's financial institution. If the transaction was processed through the eftpos network, your chargeback will be processed in accordance with the rules applying to eftpos transactions. If the transaction was processed through the Visa network, your chargeback will be processed in accordance with the rules applying to Visa transactions.

You should tell us as soon as possible, but no later than 120 days after the date of the transaction and provide us with any information we may require.

You are not able to reverse a transaction authenticated using Visa Secure unless we are liable as provided in the ePayments Conditions of Use.

We may in good faith chargeback some or all of the amount disputed. However, if we do chargeback the transaction, and Visa, the merchant or the merchant's financial institution subsequently declines to chargeback the transaction, we will deduct the refunded amount from your account.

Visa Click to Pay

What is Visa Click to Pay?

Visa Click to Pay is Visa's online checkout service. It allows you to make payments to participating merchants using an eligible Visa debit card or Visa credit card without needing to manually enter your card details each time.
In these terms, Visa Card means an eligible Unity Bank Visa debit card or Unity Bank Visa credit card issued by us.

Enrolment in Visa Click to Pay

To use Visa Click to Pay, your Visa Card must be enrolled in the Visa Click to Pay service.

We may enrol eligible and active Unity Bank Visa Cards in Visa Click to Pay. As part of this process, we may share information with Visa to create a Visa Click to Pay profile for you, or to link your Visa Card to an existing Visa Click to Pay profile.

This information may include:

- the name on your Visa Card;
- your Visa Card number and expiry date; and
- personal details we hold about you, such as your name, mobile number, email address, and mailing or billing address.

Unity Bank Visa debit cards and Unity Bank Visa credit cards that are eligible and active as at the time of enrolment may be enrolled in Visa Click to Pay as part of a bulk enrolment process.

For enrolment to be successful, your Visa Card must be eligible and active at the time enrolment occurs.

Self-enrolment

You may be able to enrol an eligible Visa Card directly with Visa.

If we subsequently enrol your Visa Card in Visa Click to Pay, these terms and conditions will apply to your use of Visa Click to Pay with that Visa Card. Any separate arrangement between you and Visa for that card may cease to apply to the extent permitted by Visa's rules and applicable law.

Using Visa Click to Pay

When you use Visa Click to Pay, information linked to your Visa Click to Pay profile may be used to help complete checkout details with participating merchants.

By using Visa Click to Pay, you confirm that:

- the information we hold about you and provide to Visa is yours;
- you are authorised to use the Visa Card linked to the Visa Click to Pay profile; and
- the information you provide, or that is provided on your behalf, is accurate, complete and up to date.

Visa, participating merchants and other third parties may use and share information about your use of Visa Click to Pay, including information needed to complete or process a transaction.

Your obligations when using Visa Click to Pay

You must only use Visa Click to Pay in a lawful and proper manner.

You must not:

- use Visa Click to Pay for any unlawful purpose;
- interfere with, disrupt or misuse Visa Click to Pay;
- attempt to gain unauthorised access to Visa Click to Pay or any part of the service;
- use Visa Click to Pay in a way that may infringe another person's rights, including privacy or intellectual property rights;
- copy, reproduce, modify, decompile, reverse engineer, commercially exploit or distribute Visa Click to Pay or any part of the service; or
- use any device, software or process that interferes, or attempts to interfere, with the proper operation of Visa Click to Pay.

Authentication and device security

Visa Click to Pay may allow you to use authentication features on your device, such as fingerprint authentication, face authentication, a device passcode or other security features.

Your use of these authentication features is governed by the terms that apply between you and your device manufacturer or service provider.

You are responsible for keeping your device, passcodes, passwords, card details and other security credentials safe. You must tell us as soon as possible if you believe your Visa Card, device, passcode, password or other security credentials have been lost, stolen, misused or compromised.

Privacy

We will handle your personal information in accordance with our Privacy Policy.

Visa may also handle your personal information in connection with Visa Click to Pay. This may include processing your information overseas or in accordance with Visa's privacy notices.

By using Visa Click to Pay, you consent to information about you and your Visa Card being used and shared as reasonably required to enrol your Visa Card, operate Visa Click to Pay, authenticate transactions, process transactions, manage the service, and comply with applicable laws and scheme requirements.

Merchant transactions, disputes and liability

If you use Visa Click to Pay to make a transaction, the transaction is between you and the merchant.

Neither Unity Bank, Cuscal nor Visa is a party to that transaction or payment. We are not responsible for any goods or services you purchase using Visa Click to Pay, including if the goods or services are defective, not supplied, or not as described.

Transactions made using Visa Click to Pay are treated as card transactions. Your liability for transactions made using Visa Click to Pay, including any unauthorised or disputed transactions, will be dealt with under these Terms and Conditions, the ePayments Code where it applies, Visa scheme rules, and applicable law.

If you believe a transaction made using Visa Click to Pay is unauthorised, incorrect or otherwise needs to be disputed, you should contact us as soon as possible. We will handle the dispute in the same way as other disputed Visa card transactions, including considering any chargeback rights that may be available.

As far as the law permits, neither Unity Bank, Cuscal nor Visa will be liable for any damages, claims or losses, whether direct, indirect or otherwise, arising from or in connection with the Visa Click to Pay service.

Changes to Visa Click to Pay

Visa may change, suspend or stop Visa Click to Pay at any time.

We may update these terms and conditions to reflect changes to Visa Click to Pay, Visa scheme requirements, law, operational requirements or our card services.

If you continue to use Visa Click to Pay after a change takes effect, you will be taken to have accepted the change.

Opting out or removing a card

You do not have to use Visa Click to Pay.

You may remove a Visa Card from Visa Click to Pay or opt out of Visa Click to Pay by contacting us.

If you remove a Visa Card from Visa Click to Pay, you may no longer be able to use that Visa Card through Visa Click to Pay unless it is enrolled again.

Digital wallets

We may allow your Visa card to be used via a digital wallet such as Apple Pay, Google Pay, Samsung Pay or any other digital wallet that we may approve from time to time.

A digital wallet allows you to securely add your Visa card to your compatible phone or wearable device. It can be used in place of your physical Visa card to make purchases in-store, within apps or on participating websites.
We are not the digital wallet provider and we are not

liable for the use of the digital wallet. The digital wallet provider is responsible for the functioning of the digital wallet, not us. When you load the card into a digital wallet, there is a sharing of your personal information between us and the digital wallet provider and between you and the digital wallet provider.

You should read and understand all of the terms and conditions governing the use of the digital wallet issued by the digital wallet provider, your telecommunications provider, and us. You will be bound by those terms when you use the digital wallet. You can find the terms and conditions governing the digital wallet on our website.

WARNING: Your mobile device(s) may be linked to other devices by a common account. Under these circumstances, if you add your Visa card to a digital wallet using the mobile device, your Visa card may also be accessible to other users of those devices and they may be able to make transactions with your Visa card.

Important information you need to know when using your digital wallet on a mobile phone

You must protect and keep confidential your User ID, phone lock, passcode, passwords, and all other information required for you to make purchases with your card using the digital wallet.

Always protect your passcode by using a unique number or pattern that is not obvious or that can be easily guessed. Take precautions when using your digital wallet. Try to memorise your passcode or carefully disguise it. Never keep a record of your passcode with your device, on your device or computer, or tell anyone your passcode. Our Terms and Conditions require you to report these events to us immediately if:

- your device has been lost or stolen;
- you believe your security credentials have been compromised;
- you believe there are errors;
- you suspect fraud associated with your digital wallet

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

Section 2 – Definitions

In these ePayments Conditions of Use, the following terms have the following meanings:

Account	an account you hold with us
ADI	has the same meaning as authorised deposit-taking institution in the Banking Act 1959 or any successor term adopted by the Australian Prudential Regulation Authority
AFCA	the Australian Financial Complaints Authority
ATM	automatic teller machine
BECS procedures	the Bulk Electronic Clearing System Procedures as existing from time to time
Biller account	an internal account maintained by a business for the purpose of recording amounts owing and paid for goods or services provided by the business
Business day	a day that is not a Saturday, a Sunday or a public holiday or bank holiday in the place concerned
Complaint	an expression of dissatisfaction made to or about an organisation, related to its products, services or staff or the handling of a complaint, where a response or resolution is explicitly or implicitly expected or legally required.
Confirmation of Payee service	the service which enables you to confirm the account name of the BSB and account number you want to make a payment to
Cuscal	Cuscal Limited ABN 95 087 822 455, which provides payment processing and card scheme enablement services to us
Days	means calendar days, unless otherwise specified
Device	a device we give to a user that is used to perform a transaction. Examples include: ▪ debit card or credit card, whether physical or virtual; ▪ token issued by us that generates a passcode (if applicable); or ▪ contactless devices
Direct entry	direct entry means a direct debit or direct credit transaction as defined in the BECS procedures
Direct entry user	a person who issues debit or credit payment instructions using the BECS procedures
EFTPOS	Electronic funds transfer at the point of sale – a network for facilitating

	transactions at point of sale
Electronic banking	refers to our Online Banking, Mobile App, Osko and PayTo services
Electronic Funds Transfer (EFT)	being a transfer of money from one financial institution account to another, either within a single financial institution or across multiple institutions, via computer based systems and made without using a physical currency
Electronic transaction	a payment, funds transfer or cash withdrawal transaction initiated using electronic equipment that is not intended to be authenticated by comparing a manual signature with a specimen signature
Electronic equipment	includes, but is not limited to, an electronic terminal, computer, television and telephone
ePayments Code	means the ePayments Code issued by the Australian Securities and Investments Commission (ASIC)
Expiry date	a restriction on a facility that means the facility cannot be used after a certain date
Facility	an arrangement through which you can perform transactions
Gambling transaction	making a purchase with a casino, lottery operator, betting agency or an entity conducting any form of gambling business
Holder	an individual in whose name a facility has been established, or to whom a facility has been issued
Identifier	information that a user: ▪ knows but is not required to keep secret, such as an account number, serial number, PayID or token generated information ▪ must provide to perform a transaction
Mandate management service	the central, secure database operated by NPP Australia Limited of payment agreements
Merchant	a business which accepts the Visa card as payment for goods and services with which you have established, or would like to

	establish, a payment agreement
Migrated DDR	means a Payment agreement created by a merchant or Payment Initiator to process payments under an existing direct debit arrangement as PayTo Payments instead of through the direct debit system
Mistaken internet payment	has the meaning provided in Section 9 (Mistaken Internet Payments)
NPP	the New Payments Platform operated by or on behalf of NPP Australia Ltd
NPP payment	means a payment settled and cleared through the NPP and includes Osko payments and PayTo payments
OTP password	a unique one time password that is issued to you for the purposes of completing a transaction and which can only be used for that single transaction
Osko®	the fast payment service operated by BPAY Pty Ltd
Osko payment	payment made using Osko allowing members to receive real time payments
Passcode	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) ▪ Online Banking or Mobile App password ▪ code generated by a physical token (if applicable) ▪ a One Time Password (OTP) provided by us via SMS or email to you; ▪ fingerprint access; or ▪ any other access mechanisms, including other biometrics such as facial recognition. A passcode does not include a number printed on a device (e.g. a security number printed on a Visa card).
PayID	is the NPP addressing service which allows you to use a mobile number, email address or ABN as a way to

	send and receive fast payments
PayID name	the name that identifies a User of the PayID Service. People sending money using NPP Payments will see the recipient's PayID Name before confirming the transaction.
PayTo agreement	an agreement created by an approved merchant or Payment Initiator in the Mandate Management Service by which you authorise us to make payments from your account or a Migrated DDR.
Payment initiator	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	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.
PayTo payment	NPP payment we make pursuant to a payment agreement.
Periodical payment	Payments scheduled from account to account or account to loan, both within the bank or externally to another institution.
PIN	Personal Identification Number
Purchase	any transaction (other than a cash advance) with a merchant, the payment for which is authorised by a cardholder to be made on the Visa card account and includes an order made for goods or services that are not taken
Receiving ADI	an ADI whose customer has received an internet payment
Regular payment arrangement	means either a recurring or an instalment payment agreement between you (the cardholder) and a merchant in which you have preauthorised the merchant to bill your account at predetermined intervals (e.g. monthly or quarterly) or at intervals agreed by you. The amount may differ or be the same for each transaction.
Scheme	A payment scheme through which transactions can be made from your account including:
	▪ BPAY; ▪ Bank@Post; ▪ Visa; ▪ eftpos; ▪ BECS operated by Australia Payments Network Ltd (trading as AusPayNet) ▪ APCS (The Australian Paper Clearing System for Cheques operated by Australia Payments Network Ltd trading as AusPayNet); and ▪ the NPP (Osko and PayTo)
Sending ADI	an ADI whose customer has made an internet payment
Transaction	a transaction to which these ePayment Conditions of Use apply, as set out in Section 3
Transfer ID	a unique identification number generated by the mandate management service in connection with a request to transfer payment agreements
Unintended recipient	the recipient of funds as a result of a mistaken internet payment
Unauthorised transaction	a transaction that is not authorised by a user. It does not include any transaction that is performed by a user themselves or anyone who performs a transaction with the knowledge and consent of a user
User	you or an individual you have authorised to perform transactions on your account, including: ▪ an authorised signatory to your account; or ▪ a person you authorise us to issue a Visa card to
Visa	refers to Visa Inc. or any Visa Inc. group company
Visa card	means a debit or credit card issued to you or an additional cardholder by us including a card accessed via a Mobile App and/or digital wallet
Visa Click to Pay	Visa's online checkout service that allows you to make payments to participating merchants using an eligible Visa card without manually entering the details

Visa Secure (formerly Verified by Visa)	The online transaction authentication service provided by Visa that we give to you in conjunction with your Visa Card
We, Us, Our or the Bank	Unity Bank Limited. ABN 72 087 650 637 AFSL & Australian Credit Licence 238311.
You	the person or persons in whose name a Visa card or Account and Access Facility is held

Section 3 – Account and Transactions

3.1 If you enable a biometric identifier such as fingerprint or face identifier login in the mobile banking app settings, we may permit you to login to the Mobile Banking app using the registered biometric identifier on that device. You can still login to the Mobile Banking app using the pass code that is registered to your account.

3.2 When you log into the Mobile Banking app using your biometric identifier, you instruct us to perform any transactions requested during the mobile banking app session.

WARNING: If you enable the biometric identifier login option, then any of the biometric identifiers stored on your device can be used to log into our Mobile Banking App. You must ensure that only your biometric identifier (and not any other persons) is stored on the mobile device to access our Mobile Banking App.

We strongly recommend that at all times you should use your passcode to access our Mobile App.

3.3 If you authorise a user to perform transactions on an account of yours to which these ePayments Conditions of Use apply, then, in order to perform transactions on that account, the user must login using their own identifier and login details.

3.4 These ePayments Conditions of Use apply 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.

3.5 These ePayments Conditions of Use apply to the following transactions:

- 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;
- electronic banking transactions including Osko and bill payment transactions;
- online transactions performed using a card number and expiry date;
- online bill payments (including BPAY);
- transactions using facilities with contactless features and prepaid cards, not intended to be authenticated by comparing a manual signature with a specimen signature;
- direct debits;
- transactions using mobile devices;
- any other transaction to which the ePayments Code applies.

Section 4 – When you are not liable for loss

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

- 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 cardholder 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.

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

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

4.4 In a dispute about whether a user received a device or passcode:

- 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; and
- we may not rely on proof of delivery to a user's correct mailing or electronic address as proof that the user received the device or passcode.

Section 5 – When you are liable for loss

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

5.2 Where we can prove on the balance of probability that a user contributed to a loss through fraud, or breaching the passcode security requirements set out in Section 6:

- 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:
  a) incurred on any one day that exceeds any applicable daily transaction limit;
  b) incurred in any period that exceeds any applicable periodic transaction limit;
  c) that exceeds the balance on the facility, including any pre-arranged credit; or
  d) 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.

Note: A breach of the passcode security requirements in itself is not sufficient to make a consumer liable for loss from an unauthorised transaction. We must prove on the balance of probability that the user's breach contributed to the loss.

5.3 Where:

- more than one passcode is required to perform a transaction; and
- we prove that a user breached the passcode security requirements in Section 6 for one or more of the required passcodes, but not all of the required passcodes;

you are liable under clause 5.2 only if we also prove on the balance of probability that the breach of the passcode security requirements was more than 50% responsible for the losses, when assessed together with all the contributing causes.

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

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

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

- are liable for the actual losses that occur between:
  a) 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
  b) when the security compromise was reported to us
- are not liable for any portion of the losses:
  a) incurred on any one day that exceeds any applicable daily transaction limit;
  b) incurred in any period that exceeds any applicable periodic transaction limit;
  c) that exceeds the balance on the facility, including any pre-arranged credit; or
  d) incurred on any facility that we and you had not agreed could be accessed using the device and/or passcode used to perform the transaction.

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

5.6 Where a passcode was required to perform an unauthorised transaction, and these preceding clauses 5.2-5.5 do not apply, you are liable for the least of:

- $150, or a lower figure determined by us;
- the balance of the facility or facilities which we and you have agreed can be accessed using the device and/or passcode, including any prearranged credit; or
- the actual loss at the time that the misuse, loss or theft of a device or breach of passcode security is

reported to us, excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit.

5.7 In deciding whether on the balance of probabilities we have proved that a user has contributed to losses under the preceding clauses 5.2 and 5.5:

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

5.8 If a user reports an unauthorised transaction on a credit card account, debit card account or charge card account we will not hold you liable for losses under Section 5 for an amount greater than your liability if we exercised any rights we had under the rules of the card scheme at the time the report was made, against other parties to the scheme (for example, charge-back rights).

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

Section 6 – Passcode security requirements

6.1 This section applies where one or more passcodes are needed to perform a transaction. Any liability for losses resulting from unauthorised transactions will be determined by the ePayments Code, rather than these passcode security requirements.

6.2 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:
  a) carried with a card/device; or
  b) liable to loss or theft simultaneously with a card/device

  unless the user makes a reasonable attempt to protect the security of the passcode(s).
- where a card/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).
- allow anyone else's fingerprint or face to be registered to the card/device which is used to access Online Banking or digital wallet.

Note: If a user discloses a passcode under the first bullet point in clause 6.2, without having the benefit of an exception in clause 6.7 or 6.8, and we can prove on the balance of probability that the consumer contributed to a loss by breaching the passcode security requirements, we are not required to indemnify the user for that loss.

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

- 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; or
- preventing unauthorised access to an electronically stored record of the passcode record.

This list is not exhaustive.

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

Note 1: An example of extreme carelessness is storing a member number, username and passcode for Online Banking in a diary, smartphone, computer or other personal electronic device that is not password protected under the heading 'Online banking codes'.

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

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

- specifically instructed the user not to do so; and

- warned the user of the consequences of doing so.

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

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

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

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

Note 1: For example, when we permit users to give their passcode(s) to an account aggregator service, a user who discloses their passcode(s) to the service does not breach the passcode security requirements in clause 6.

Note 2: For example, if we permit the storage of passcodes in an electronic folder in the user's computer, a user who stores their passcode(s) in this way does not breach the passcode security requirements in clause 6.

Section 7 – Liability for loss caused by system or equipment malfunction

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

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

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

Section 8 – Network arrangements

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

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

8.2 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; or
- have a complaint or dispute investigated by any other party to a shared electronic payments network.

Section 9 – Mistaken internet payments

9.1 In this Section 9:

a) direct entry means a direct debit or direct credit but does not include NPP Payments.

b) mistaken internet payment means a payment by a 'user' (as defined by the ePayments Code):

- through a 'Pay Anyone' internet banking facility and processed by an ADI which has subscribed to the ePayments Code through direct entry 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; or
- that is an NPP Payment which, as a result of the user's error, is directed to the wrong account.

This does not include payments made using BPAY or PayTo payments.

Note: The 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.

c) receiving ADI means an ADI whose customer has received an internet payment

d) unintended recipient means the recipient of funds as a result of a mistaken internet payment

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

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

Note: 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.

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

9.5 The other obligations of the sending ADI and the receiving ADI, under the ePayments Code, depend on how long it is between when the mistaken internet payment was made and when it was reported, whether the receiving ADI is satisfied that a mistaken internet payment has occurred, and whether there are sufficient funds in the account of the recipient to cover payment. Those obligations are summarised in the table below.

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

You made a payment	You received a payment
Sufficient funds are available in the recipient's account and the report is made within ten business days:	
▪ If both we and the receiving ADI are satisfied that a mistaken internet payment has occurred, the receiving ADI must return the funds to us, within five business days of receiving the request from us, if practicable, or such longer period as is reasonably necessary, up to a maximum of ten business days. ▪ 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 us. ▪ If we receive the funds back from the receiving ADI, we will return the funds to you as soon as practicable.	▪ If we receive a request from a sending ADI and we are satisfied that a mistaken internet payment has occurred, we will return the funds to the sending ADI. This may take up to ten business days. ▪ If we are not satisfied that a mistaken internet payment has occurred, we may ask for your consent to return the funds.
Sufficient funds are available in the recipient's account and the report is made between ten business days and seven months:	
▪ The receiving ADI has ten business days to investigate. ▪ If it is satisfied that a mistaken internet payment has occurred, the receiving ADI must place a hold on the funds and give the recipient ten business days to establish that they are entitled to the funds. ▪ If the recipient does not establish that they are entitled to the funds the receiving ADI must return the funds. ▪ If the receiving ADI is not satisfied that a mistaken internet payment has occurred, it may seek the consent from the recipient to return the funds to us. ▪ If we receive the funds back from the receiving ADI, we will return the funds to you as soon as practicable.	▪ If we receive a request from a sending ADI we have ten business days to investigate. ▪ If we are satisfied that a mistaken internet payment has occurred, we will place a hold on the funds and give you ten business days to establish that you are entitled to those funds. ▪ If you do not establish that you are entitled to the funds, we will return the funds to the sending ADI. ▪ If we are not satisfied that a mistaken internet payment has occurred, we may seek your consent to return the funds to the sender.
Sufficient funds are available in the recipient's account and the report is made after seven 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 us.	▪ If we receive a request from a sending ADI and we are satisfied that a mistaken internet payment has occurred, we will ask for your consent to return the funds.

▪ 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 us. ▪ If the unintended recipient consents to the return of the funds, the receiving ADI must return the funds to us. ▪ If we receive the funds back from the receiving ADI, we will return the funds to you as soon as practicable.	▪ If we are not satisfied that a mistaken internet payment has occurred, we may ask for your consent to return the funds.
Sufficient funds are not available in the recipient's account	
▪ If there are some funds in the account, but not sufficient to cover the payment, the obligations set out above (in this column) will apply in relation to those funds. ▪ As to the balance of the payment, if the receiving ADI is satisfied that a mistaken internet payment has occurred it has a discretion, to be exercised taking into account factors set out in the ePayments Code, as to whether it should pursue part, all or none of the balance from the unintended recipient. ▪ If the receiving ADI determines that it will pursue part or all of the balance, it must use reasonable endeavours to do so (for example, by facilitating repayment by the unintended recipient by instalments). In determining what are reasonable endeavours it must take into account factors set out in the ePayments Code.	▪ If there are some funds in the account, but not sufficient to cover the payment, the obligations set out above will apply in relation to those funds. ▪ As to the balance of the payment, if we are satisfied that a mistaken internet payment has occurred we have a discretion, to be exercised taking into account factors set out in the ePayments Code, as to whether we should pursue part, all or none of the balance from you. ▪ If we determine that we will pursue part or all of the balance, we must use reasonable endeavours to do so (for example, by facilitating repayment by you by instalments). In determining what are reasonable endeavours we must take into account factors set out in the ePayments Code.

9.6 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, including details of your right to complain.

9.7 You may complain to us about how the report is dealt with, including that we and/or the receiving ADI:

- are not satisfied that a mistaken internet payment has occurred
- have not complied with the processes and timeframes set out in accordance with the ePayments Code.

9.8 When we receive a complaint under clause 9.7 we must:

- deal with the complaint under our internal dispute resolution procedures; and
- not require you to complain to another ADI instead.

9.9 If you are not satisfied with the outcome of a complaint, you are able to complain to our external dispute resolution scheme provider.

Section 10 – Using Online Banking or Mobile App

10.1 We do not warrant that:

- the information available to you about your accounts through our electronic or phone services is always up to date;
- you will have 24 hours a day, 7 days per week, access to Online Banking or Mobile App; or
- data you transmit via Online Banking or Mobile App is totally secure.

External Transfers

10.2 When you tell us to transfer funds to another person using electronic banking, you must provide us with the information we request including the details for the account to which the funds are being transferred which can be:

- the BSB number and the account number for the account; or
- a PayID which has been created for the account

10.3 You must ensure that the BSB and account number or PayID you tell us are correct. We will not be liable for any loss you suffer as a result of you telling us the wrong information.

10.4 If you instruct us to transfer funds using a PayID, and we display the PayID Name registered to that PayID to you, you must ensure that the name reasonably represents the intended recipient of the funds before you confirm your instruction. You must cancel the instruction if the PayID Name that we display to you as being registered to the PayID is not the intended recipient.

10.5 Where we allow you to include a transfer reference or description with a transfer, you must ensure it does not contain, reference or link to:

- any swearing, profanity, offensive, discriminatory, threatening or abusive content;
- any information that is confidential or must be kept secret;

- sensitive personal information of any person (including information or an opinion about a person's racial or ethnic origin, political opinions or membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record, health information);
- anything which infringes the intellectual property rights of any person; or
- anything which is illegal or seeks to promote illegal activity.

Where we consider it appropriate to do so, we may disclose the information you include in a transfer reference or description to appropriate law enforcement authorities or, in the case of personal information about another person, to the person the personal information relates to.

You should keep in mind that any transfer reference or description you include with a transfer will be able to be seen by all account holders for the recipient account.

10.6 We are not required to process a transfer if you do not give us all the required information or if any of the information you give us is inaccurate or incomplete.

10.7 Subject to the events described in Clause 10.18, we will immediately debit the amount of a transfer and any applicable fees to your nominated account when we accept your transfer instruction.

10.8 A transfer instruction you give us using electronic banking is irrevocable and you cannot stop or cancel a transfer instruction once we have accepted it.

Processing of External Transfers

10.9 Where it is possible to effect a transfer through different payment channels or systems, we may choose, at our discretion, which payment channel or system to use.

10.10 If the financial institution at which the recipient account is held is an Osko subscriber and advises us that the recipient account is able to receive Osko Payments, we may process the transfer as an Osko Payment. We will tell you if your transfer is being sent as an Osko Payment at the time we accept your instruction.

10.11 Subject to the events described in Clause 10.18, where we process a transfer as an Osko Payment, we will process the transfer immediately and the funds will usually be available to the payee immediately.

10.12 You can see within your Online Banking records details of Osko Payments we have processed on your behalf including whether an Osko Payment has been successfully processed or has failed for any reason.

10.13 We will tell you if, for any reason, we cease to be able to offer you Osko Payments.

10.14 Where we process a transfer as an Osko Payment, we may need to disclose your personal information to BPAY Pty Ltd, the operator of Osko. By requesting a transfer, you consent to us disclosing your personal information to Osko and such other Osko participants as necessary to effect the transfer as an Osko Payment.

Other transfers

10.15 Where we do not send a transfer as an Osko Payment we will send it as a standard transfer.

10.16 Where we process a transfer as a standard transfer:

- If you instructed us on a business day (in New South Wales), before the cut off time, we will generally process it on that day; and
- If you instruct us after the cut off time, or on a day that is not a business day (in New South Wales), we will process it on the next business day.

10.17 Funds sent by standard transfer will generally not be available to the recipient until 1-2 business days after the day we process the transfer.

Delays

10.18 Delays may occur in processing transfers where:

- we experience a services disruption or systems outage which prevents us or our service providers from processing transfers;
- we are required to delay processing a transfer to comply with any applicable laws (including any laws in relation to anti-money laundering and sanctions);
- you fail to comply with any of your obligations under any relevant terms and conditions;
- the financial institution at which the recipient account is held or the recipient fails to comply with their obligations or is experiencing a services disruption which prevents them from processing transfers;
- the financial institution at which the recipient account is held decides to delay processing;
- we delay processing to investigate and review the transfer instruction to ensure it is not fraudulent, illegal or improper or to confirm that it has been properly authorised by you; or

- an account is operated on a two or more to sign basis and a transaction has been initiated by one of the signatories using Online Banking, but we have not received authorisation from the other signatory or signatories.

10.19 We will not be liable to you for any delay in a transfer being processed or the funds being received by the recipient for any reason.

Suspension of the transfers

10.20 We may suspend your right to make transfers using electronic banking at any time without prior notice to you if you are suspected of acting in an illegal, fraudulent or improper manner or if we believe doing so is necessary to protect the security or integrity of our systems or to prevent you or us suffering any loss or damage.

Transaction limits

10.21 We may decline any transfer request or instruction from you where accepting it would cause you to exceed any applicable transaction or period limit we have imposed. You may view and vary your transaction limits at any time through Online Banking. Please refer to the Summary of Accounts and Access Facilities for details of current transaction limits.

Failed transfers

10.22 If we are advised that a transfer cannot be processed or it fails and cannot be completed for any reason we will advise you of this where practicable and credit your account with the amount debited in relation to the transfer. Where we have transferred funds to another financial institution as part of processing the transfer, we will not credit your account with the amount until the funds have been returned to us from the other financial institution.

Mistakes and issues with transfers

10.23 If you make a transfer and later discover that:

- the amount you transferred was greater than the amount you needed to pay, you must contact the recipient to obtain a refund of the excess. If we processed the transfer as an Osko payment, we may be able to request that the funds, or just the overpaid amount, be returned on your behalf if you ask us to do so. However, the amount may not be returned to you unless the recipient consents to their financial institution returning the funds; or
- the amount you transferred was less than the amount you needed to pay, you will need to make another transfer for the difference between the amount you actually transferred and the amount you needed to pay.

10.24 You should notify us immediately if you think that:

- you have made a mistake when transferring funds;
- you did not authorise a transfer that has been debited to your account or you think a transfer has not been processed in accordance with your instructions;
- you become aware that a transfer made using a PayID from your account was directed to an incorrect recipient; or
- you were fraudulently induced to make a transfer.

The timing of your report may impact on our ability to assist you to recover funds (where possible).

10.25 See Section 9 for information about how Mistaken Internet Payments will be dealt with.

10.26 Where we consider it appropriate and we are reasonably able to do so, we may request that the financial institution to whom the funds were transferred returns the funds to us, on your behalf. However, depending on the circumstances, the financial Institution may not return the funds to us unless the recipient consents.

10.27 Where the transferred funds are returned to us, we will credit them to your account and make them available to you as soon as practicable.

10.28 You indemnify us against, and will be liable to us for, any direct or indirect loss, damage, charge, expense, fee or claim we may suffer or incur as a result of the return of funds to us where we have requested that transferred funds be returned on your behalf. We may debit any such loss, damage or cost to any account you hold with us.

Refunds and chargebacks

10.29 Except as provided in Section 9 (Mistaken Internet Payments) and clause 10.26 above, refunds cannot be processed in respect of funds transferred by electronic banking.

10.30 Where a transfer has been correctly completed but you have a dispute with the recipient, you will need to resolve the dispute directly with that person.

10.31 No “chargeback” rights are available in relation to funds transferred by electronic banking, even if the transfer has been made from a credit card account.

Section 11 – How to report a loss, theft or unauthorised use of your Visa card or passcode

11.1 If you believe your Visa card has been misused, lost or stolen, or the passcode has become known to someone else, you must immediately contact us during business hours or the Visa Card Hotline at any time. Please refer to the 'How to contact us' section for our contact details.

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

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

11.4 If the loss, theft or misuse occurs outside Australia you must notify a financial institution displaying the Visa sign and then confirm the loss, theft or misuse of the card:

- with us by telephone or priority paid mail as soon as possible; or
- by telephoning the Visa Card Hotline for the country you are located in.

A fee may apply for the replacement of a lost, stolen or damaged Visa card.

Section 12 – How to report unauthorised use of Online Banking or Mobile App

12.1 If you believe that your passcodes for Online Banking or Mobile App transactions have been misused, lost or stolen, or, where relevant, your passcode has become known to someone else, you must contact us immediately. Please refer to the 'How to contact us' for our contact details.

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

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

Section 13 – Using your Visa card for foreign currency transactions

13.1 You agree to reimburse us for any costs, fees or charges of any nature arising out of a failure to comply with any exchange control requirements or tax laws.

13.2 All transactions made in foreign currency (irrespective of where the transactions occurs) 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).

13.3 All transactions made in a foreign currency on the Visa card are subject to a conversion fee payable to Cuscal Limited, the principal member of Visa Worldwide under which we can provide you with the Visa card. Please refer to the Fees and Charges Schedule for the current conversion fee.

13.4 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.

13.5 Some merchants and terminals allow the cardholder the option at the point of sale to convert the transaction into Australian dollars at point of sale. This is known as "Dynamic Currency Conversion". Please note that if you choose this option, then once you have confirmed the transaction you will not be able to dispute the exchange rate applied.

Section 14 – Additional cardholder

14.1 You may authorise us, if we agree, to issue an additional Visa card to an additional cardholder provided this person is aged 18 or over (unless we agree to a younger age). Additional cardholders will receive a separate PIN and have the same rights as signatories to the account, refer to the 'Authorised Signatory' section for more information.

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

14.3 You must ensure that any additional cardholders protect their card and PIN in the same way as we require you to protect your card and PIN.

14.4 To remove an additional cardholder, you must notify us in writing. However, this cancellation may not be effective until the additional card is returned to us or

you have taken all reasonable steps to have the additional card returned to us. You can also contact us to request that we place a hold or freeze on any cards issued to your account to prevent transactions from occurring.

14.5 You'll not be liable for the continued use of the additional card from the date that you have:

- notified us that you want it cancelled;
- and taken all reasonable steps to have the additional card returned to us.

Please note that if you are unable to return the additional card to us, we may require you to make a written statement describing the steps you have taken to return the card.

Section 15 – Use after cancellation or expiry of Visa card

15.1 You must not use your Visa card:

- after the expiration date shown on the card; or
- after the card has been cancelled.

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

Section 16 – Exclusions of Visa card warranties and representations

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

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

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

Section 17 – Cancellation of Visa card or access to electronic banking or BPAY

17.1 You may cancel your Visa card, your access to electronic banking or BPAY at any time by notifying us by phone or in writing using secure messages in Online Banking or by email.

17.2 We may immediately cancel or suspend your Visa card or access to electronic banking or BPAY at any time for security reasons or if you breach these ePayment Conditions. In the case of a Visa card, we may cancel the card by capture at any ATM.

17.3 We may cancel your access to electronic banking or BPAY at any time by giving you 30 days' notice. The notice does not have to specify the reasons for cancellation.

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

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

17.6 Your Visa card or your access to electronic banking or BPAY will be terminated when:

- we notify you that we have cancelled your access method to the account with us;
- you close the last of your accounts with us to which the Visa card applies or which has electronic banking or BPAY access;
- you cease to be our member; or
- you alter the authorities governing the use of your account or accounts which the Visa card applies or which has electronic banking or BPAY access (unless we agree otherwise).

17.7 In the case of a Visa card, we may demand the return or destruction of any cancelled card.

Section 18 - Using BPAY payments facility ("BPAY")

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

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

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

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

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

Section 19 – Processing BPAY payments

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

- 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.

19.2 A BPAY payment instruction is irrevocable. BPAY payments for goods or services using your Visa card will also be governed by the operating rules applicable to BPAY as published by BPAY from time to time.

If you use your Visa card to make a BPAY payment you do not have the right to reverse the payment or chargeback the transaction, notwithstanding that the merchant failed to deliver the goods and/or services to you.
If there is any inconsistency between the BPAY conditions of use and these Conditions of Use, the BPAY conditions of use will apply to the extent of that inconsistency.

The ePayments Code does not apply in relation to BPAY payments.

BPAY payments made from a Visa Credit Card are treated as cash advances.

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

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

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

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

19.6 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 New South Wales 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.

19.7 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 or you use Online Banking or our Mobile App to 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.

19.8 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

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

- 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.

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

Section 20 – Future-dated BPAY payments

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

Section 21 – Consequential damage for BPAY payments

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

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

Section 22 – Using Osko

22.1 You can use Osko to make payments from those accounts that have the Osko facility, including:

- make an Osko payment;
- make scheduled and recurring Osko payments;
- receive payment reminders; and
- pay bills bearing the Osko logo from those accounts that have the Osko facility.

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

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

22.5 We may monitor Osko payment activity to identify high-frequency or unusual Osko payment behaviour. This includes the frequency, value, pattern or funds recipient of Osko payments which may indicate fraud, misuse or inconsistency with the purpose declared at account opening. If we deem your Osko usage contradicts the behavioural expectations of a standard personal transaction account, or purpose declared at account opening, we may:

- contact you to obtain further information;
- provide you with a Notice to Cease;
- pause or cancel your Osko payment service;
- issue a formal written warning outlining required behavioural changes;
- advise that continued misuse will result in restrictions and potential account closure.

22.6 If we cancel or suspend your access to the Osko payment service, we may refuse any directions you provide us to make an Osko payment without giving any reason or advance notice to you.

Section 23 – Processing Osko payments

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

- you become aware of any delays or 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.

23.2 An Osko payment instruction is irrevocable.

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

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

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

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

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

Section 24 – Scheduled and recurring Osko payments

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

- you are responsible for maintaining, in the account to be drawn on, sufficient cleared funds to cover all scheduled and recurring Osko payments (and any other drawings) on the day(s) you have nominated for payment or, if the account is a credit facility, there must be sufficient available credit for that purpose.
- 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 that the scheduled or recurring Osko payment is made correctly;
- you should contact us if there are any problems with your scheduled or recurring Osko payments; and
- you must contact us if you wish to cancel a scheduled or recurring Osko payment after you have given the direction but before the date for payment.

Section 25 – Regular payment arrangements

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

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

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

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

Section 26 – PayTo

26.1 This section applies in relation to your use or attempted use of PayTo and any Payment Agreement that is created for an account, and related PayTo payments, if PayTo is available for your account. See the Summary of Accounts and Access Facilities to determine whether PayTo is available for your account.

Creating a PayTo payment agreement

26.2 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.

26.3 Payment agreements must be recorded in the mandate management service before NPP payments can be processed in accordance with them. The

merchant or payment initiator is responsible for creating and submitting a record of each payment agreement to their financial institution or payments processor for inclusion in the mandate management service. The mandate management service will notify us of the creation of any payment agreement established using your account or PayID details.

26.4 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.

26.5 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.

26.6 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.

26.7 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.

Amending a PayTo payment agreement

26.8 Your payment agreement may be amended by the merchant or payment initiator from time to time, or by us on your instruction.

26.9 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.

26.10 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.

26.11 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.

26.12 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 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.

Pausing your payment agreement

26.13 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.

26.14 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.

26.15 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.

Transferring your payment agreement

26.16 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.

26.17 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.

26.18 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.

26.19 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.

Cancelling your payment agreement

26.20 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.

26.21 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.

Migration of direct debit arrangements

26.22 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.

26.23 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.

26.24 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.

General PayTo provisions

26.25 The following general PayTo provisions apply:

- a payment agreement can only be linked to an account that has the PayTo facility.
- 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.
- 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.
- you are responsible for ensuring that:
    a) all data you provide to us or to any merchant or payment initiator that subscribes to PayTo is accurate and up to date;
    b) you do not use PayTo to send threatening, harassing or offensive messages to the merchant, payment initiator or any other person; and
    c) any passwords/pins needed to access the facilities we provide are kept confidential and are not disclosed to any other person.
- all intellectual property, including but not limited to the PayTo trademarks and all documentation, remains our property, or that of our licensors (our intellectual property). We grant to you a royalty free, non-exclusive license (or where applicable, sub-license) for the term to use our intellectual property for the sole purpose of using PayTo in a way that is consistent with 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:
    a) modifications to our intellectual property by or on behalf of you in a manner that causes the infringement;
    b) use of any item in combination with any hardware, software or other products or services in a manner that causes the infringement and where such combination was not within the reasonable contemplation of the parties given the intended use of the item;
    c) your failure to use corrections or enhancements to our intellectual property that are made available to you (except where the use of corrections or enhancements would have caused a defect in PayTo or would have had the effect of removing functionality or adversely affecting the performance of PayTo); and
    d) your failure to use our intellectual property in accordance with this agreement.
- we may cancel or suspend your use of PayTo in accordance with our rights under section cancelling your card or access service.
- we may amend the terms and condition relating to PayTo in accordance with our rights under the terms and conditions for savings accounts and payment services. 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, 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 Summary of Accounts and Access Facilities for savings accounts and payment services. 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.

- If your payment agreement is linked to a PayID:
  a) transferring your PayID to another account (whether with us or another financial institution) will not automatically transfer the payment agreement to that account, and payments under the linked payment agreement will fail;
  b) closing your PayID will cause payments under the linked payment agreement to fail.
- to ensure payments under a linked payment agreement continue after transferring or closing the PayID you will also need to either link the payment agreement to an account with us or, when available, transfer the payment agreement to another financial institution.

Privacy and PayTo

26.26 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.

Authority for PayTo instructions

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

Section 27 – Confirmation of Payee

27.1 The Confirmation of Payee service allows you to confirm the account name of the BSB, and account number you want to make a payment to.

Conducting a Confirmation of Payee Lookup

27.2 For a payment using a BSB and account number, it is your responsibility to ensure the BSB and account number you want to pay to is correct. The Confirmation of Payee service may provide you with a view on the likelihood that the account name you enter matches the account. If the Confirmation of Payee service response indicates that the details do not look right, you should check the account details with the intended recipient before proceeding with the payment.

27.3 You must not misuse the Confirmation of Payee service in breach of these terms and conditions. We may limit or suspend your use if we believe it is reasonably necessary to protect you or us from possible fraudulent activity, scams or other activities that might cause you or us to lose money.

Privacy and Confirmation of Payee

27.4 We will ensure that your Account details are accurately recorded by us for the use of the Confirmation of Payee service.

27.5 You acknowledge and authorise:
a) us to use and disclose your Account details in the Confirmation of Payee service; and;
b) payer's financial institutions to use your Account details for the purpose of the Confirmation of Payee service and prior to making payments to you.

27.6 In special circumstance we may allow you to opt-out of the Confirmation of Payee service. Please contact us on 1300 364 400.

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

27.8 In some circumstances you may provide alternative names to be recorded on your account for use in the Confirmation of Payee service.

Other things you need to know

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.

The above does not apply to documents we are no longer legally required to retain.

If we are giving you a copy of a document then we will do so within 14 days if the original came into existence 1 year or less before you make the request or within 30 days if the original came into existence more than 1 year but less than 7 years before you make the request. If for some reason we are unable to provide a document within these timeframes, we will advise you in writing, together with the expected timeframe for providing the document.

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.

Third party payment services

We provide Outward and Inward Telegraphic Transfer services to our customers through our business partner Convera Australia Pty Ltd ACN 150 129 749; AFSL 404092, (trading as Convera). All telegraphic transfers you initiate will be sent to the beneficiary's account via Convera. Fees and charges and terms and conditions apply.

Inward Telegraphic Transfers

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

Each institution involved in the transfer process may deduct a processing fee from the amount being remitted before on-forwarding the funds. We do not charge any fees but will pass on any fee charged by other financial institutions involved in the transfer. We will credit telegraphic transfer funds to your account within 1 to 2 business days once the payment has been received by us.
Provided all information supplied on the request is complete and correct, funds transferred in major overseas currencies generally take three to five business days to be received, however this is an estimate only and cannot be guaranteed. Funds transferred in minor overseas currencies generally take seven to ten 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 by us for processing.

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

Outward Telegraphic Transfers

Requests to transfer funds via telegraphic transfer will be processed within one to two 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 in major overseas currencies generally take three to five business days to be received, however this is an estimate only and cannot be guaranteed. Funds transferred in minor overseas currencies generally take seven to ten 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.

We cannot lodge a trace on international telegraphic transfers until five 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 (however caused).

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 ten 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 to advise you of that by email. You will be liable for our fees and charges notwithstanding that the telegraphic transfer has been rejected.

If you complete a telegraphic transfer through Online 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 Fees & Charges Schedule) 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.

Account switching

Account switching makes it easier for you to switch your account from one financial institution to another. Both your old and new financial institution will help with re-establishing your direct debit and credit arrangements to your new account.

For more information on account switching and how we can help, please contact us.

Account verbal password

We understand that sometimes you can't come into a Service Centre but you would still like to talk to a real person. To make it easier to give us instructions over the phone, you can arrange a verbal password to be added to your account. This also provides additional security to our usual personal identification processes.
The first time you call us we will ask you some questions to help us confirm your identity, then we will ask you to choose a verbal password to use when you call us from then on.

Money laundering and illegal activity

To ensure we can meet our legal and regulatory obligations, we must exercise a level of control and monitoring over accounts and access facilities opened with us. This means that we may delay, freeze, block or refuse to make or receive any payment using the services detailed in these Terms and Conditions 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 us with the following undertakings and indemnify us 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.

Comprehensive Credit Reporting

Under comprehensive credit reporting we can share

additional credit information about you with credit reporting bodies which includes:

- up to 24 months repayment history on your accounts, such as credit cards and loans;
- the types of credit accounts opened with us;
- the dates you've applied for, opened, and closed credit accounts; and
- the current limits on our credit products.

This is referred to as Comprehensive Credit Reporting (CCR) data.

Collection and disclosure of information

Before, during or after the provision of our products and services to you, we may collect your personal information (including credit-related information) for the purposes of providing products and services to you and managing our business. When providing credit to you, this may include assessing your application for consumer or commercial credit or to be a guarantor, assessing your credit worthiness, managing your loan or the arrangements under which your loan is funded or collecting overdue payments.

Some laws require us to obtain personal information about you before we provide you with particular products or services or process particular transactions in which you are involved – e.g. laws relating to anti-money laundering and counter- terrorism financing, consumer credit, taxation and real property transactions.

If you do not provide us with the personal information that we request, we may not be able to consider your application for credit or provide other products and services.

With respect to providing credit to you, the credit reporting bodies that we disclose information to are Equifax and Experian.

Contact details:

Equifax

Phone:	13 83 32
Mail:	PO Box 964, North Sydney, NSW 2059
Website:	www.equifax.com.au

Experian

Phone:	1300 783 684
Mail:	PO BOX 7405 St Kilda Road, Melbourne, VIC 3004
Website:	www.experian.com.au

If you do not make your repayments when they fall due or commit a serious credit infringement, we may disclose this to Equifax or Experian. This may include information about whether you make repayments on time and whether your obligation to make those payments has been affected by a financial hardship arrangement. Any information that we provide to these bodies may be included in reports provided to credit providers to help them assess your creditworthiness.

You can also ask a credit reporting body, through contact details on their website, not to use or disclose your personal information if you believe on reasonable grounds that you have been or are likely to be a victim of fraud, including identity fraud.

Access to personal information

You may request access to the personal information (including credit-related information) that we hold about you at any time.

We will respond to your request for access within a reasonable time. If we refuse to give you access to any of your personal information, we will provide you with reasons for the refusal and the relevant provisions of the Privacy Act that we rely on to refuse access. You can contact our Privacy Officer if you would like to challenge our decision to refuse access.

We may recover the reasonable costs of our response to a request for access to personal information.

Accuracy and Correction

We take reasonable steps to make sure that the personal information (including credit-related information) that we collect, hold, use or disclose is accurate, complete and up-to-date. However, if you believe your information is incorrect, incomplete or not current, you can request that we update the information. We will take all reasonable steps to action your request. This includes assessing your request and informing you whether we agree that a correction should be made.

If you believe there is an error on your credit report, you can contact the credit reporting body where you obtained your report, or contact the financial institution that provided the incorrect information and ask them to investigate.

Instructions to us

Subject to the provisions of this clause, you are responsible for all instructions given in relation to your accounts which are authorised by a user's 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 Online Banking or provided access to secure passcodes which a person has used to provide instructions. Such instructions are valid, irrevocable authorities to us to follow the instructions.