THE CAPRICORNIAN'S

Conditions of Use

Incorporating…

- **Financial Services Guide**
- **Privacy Notification**
- **Account and Access Facility incorporating Customer Terms for Osko®**
- **Account Fees and Transaction Limits**
- **Schedule of Fees and Charges**
- **Schedule of Loan Fees and Charges**
- **Access Limits**
- **Eftpos Issuer Terms**

Date taking effect: 28 November 2025

The Capricornian's Account and Access Facility is issued by:
The Capricornian Ltd trading as The Capricornian Bank
ABN 54 087 650 940
AFSL / Australian Credit Licence 246780

TABLE OF CONTENTS

FINANCIAL SERVICES GUIDE

This Financial Services Guide was prepared on 4th April 2025

WHAT IS THE PURPOSE OF THIS FINANCIAL SERVICES GUIDE?

We have designed this Financial Services Guide (FSG) to assist you in deciding whether to use any of the financial services we offer. This FSG must provide you with information about:

- our name and contact details;
- the financial services we are authorised to provide;
- any remuneration that we, or any other relevant person, may be paid in relation to the financial services we offer; and
- how we deal with complaints against us.

However, this FSG does not provide information about our financial services in relation to basic deposit products and non-cash payment facilities, other than the information about:

- our name and contact details; and
- how we deal with complaints against us.

WHAT OTHER DOCUMENTS MIGHT I RECEIVE?

When we provide you with a financial service, we may also have to provide you with a Statement of Advice or a Product Disclosure Statement. These documents are described below.

Statement of Advice

A Statement of Advice is a document that sets out personal advice we give to you, the basis on which we give the advice, and any benefit or association that may influence the advice we provide to you. The Statement of Advice helps you to make an informed decision about whether to act upon that advice.

We must give you a Statement of Advice when we provide you with advice in relation to a financial product, after taking into consideration your objectives, financial situation or needs. We are not required to provide you with a Statement of Advice if our advice relates only to basic deposit products, non-cash payment facilities or general insurance products.

Product Disclosure Statement

A Product Disclosure Statement **(PDS)** is a document that provides you with information about a financial product and the entity that issues the financial product **(the Issuer).**

We must provide you with a PDS about a financial product for which a PDS is available when:

- we recommend that you acquire the financial product; or
- we issue, offer to issue, or arrange the issue of, the financial product to you.

The PDS must contain information about the financial product so that you can make an informed decision whether or not to acquire it. A PDS about a financial product must include, amongst other things:

- the Issuer's name and contact details;
- the significant features of the financial product and its terms and conditions,
- any significant benefits and risks associated with holding the financial product;
- the fees and costs associated with holding the financial product; and
- dispute resolution procedures, and how you can access them.

WHAT FINANCIAL SERVICES CAN WE PROVIDE?

Our Australian Financial Services Licence (**AFSL**) authorises us to deal in and provide advice about the following financial products:

- basic deposit products – our transaction, savings and term deposit accounts;**
- non-cash payment facilities – such as Visa card, mobile banking app and internet banking and travellers cheques';**
- term or investment deposit accounts that are not basic deposit products;
- general insurance; and
- consumer credit insurance.

** Please note that the only information we provide in this FSG about our basic deposit products and non-cash payment facilities is about our contact details and our dispute resolution system under "What should you do if you have a complaint?"

In addition to the financial services we provide under our (**AFSL**), we also deal in and advise on consumer and commercial lending products.

ON WHOSE BEHALF DO WE PROVIDE FINANCIAL SERVICES?

We generally provide financial services on our own behalf. However, when we arrange to issue insurance products, we do so on behalf of the insurers who are the product issuers. Details of who the relevant product issuer is will be included in the Product Disclosure Statement for that insurance product.

HOW DO YOU DO BUSINESS WITH US?

We generally prefer instructions for products and services be provided in person, and we usually require your signature to confirm these instructions. However, there are special arrangements in place for some products and services where we can receive your instructions electronically via email, by telephone or fax. Where this is possible, it will be specified in the terms and conditions for the relevant product.

Where available, we are also able to accept instructions by other matters- for example, Brille and various foreign languages. If you would prefer to instruct us in any of these ways, please make your request known to a member of our staff.

WHAT REMUNERATION OR OTHER BENEFITS DO WE RECEIVE FOR PROVIDING FINANCIAL SERVICES?

We do not receive fees or commissions for financial product advice we give or for issuing our non-basic term or investment products.

We may receive commissions from an insurer when we arrange an insurance product, as set out below:

- general insurance products – commissions range from 10% to 25% of premiums for new insurance and insurance renewals, depending on the type of insurance product;
- consumer credit insurance – the credit union receives 20% of premiums for new insurance.

If you receive personal advice from us in relation to insurance products, we will be required to provide you with more detailed information about the amount of commission that we may receive or the method in which commission is calculated.

WHAT REMUNERATION OR OTHER BENEFITS DO OUR EMPLOYEES RECEIVE FOR PROVIDING FINANCIAL SERVICES?

As a rule, our staff are remunerated principally by salary and do not receive any direct benefits for providing you with financial services in relation to our non-basic term or investment deposit accounts or insurance products.

From time to time, we may allow insurers to run promotion programs under which they may reward or provide benefits to our staff for their success in arranging the issue of insurance products during the promotion period. If you receive personal advice from us, we will be required to provide you with more detailed information about any relevant benefit in or with your Statement of Advice.

COMPENSATION ARRANGEMENTS

We have professional indemnity insurance arrangements in place to meet its obligations as the holder of an AFSL. Our insurance arrangements cover claims relating to the services and products we offer and the conduct of current and form our staff (where we are responsible for the conduct of the staff member at the time of relevant conduct).

Financial Hardship

You may experience financial hardship at some time. This may be related to illness, unemployment or reduced income, a pandemic, natural disaster or relationship breakdown. But getting support is important – and we're here to help.

If you are struggling to keep up or worried about managing your debt repayments in the future, get in touch with us. We can help with tailored support to suit your needs.

WHAT SHOULD YOU DO IF YOU HAVE A COMPLAINT?

We conduct a dispute resolution system to deal with any complaints you may have about any of our banking products or services, or about any financial service we provide in relation to insurance products. Our dispute resolution policy requires us to deal with any complaint efficiently, speedily and sympathetically. If you are not satisfied with the way in which we have tried to resolve your complaint, or if we do not respond speedily, you may refer the complaint to our external dispute resolution centre.

If you want to make a complaint, contact our staff at any branch and tell them that you want to make a complaint. Our staff has 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 have an easy to read guide to our dispute resolution system available to you on request.

CONTACT DETAILS

You can contact The Capricornian Bank:

- in person at one of our branches – visit our website at www.capricornian.com.au for our branch details
- by calling 1300 314 900
- by email at info@capricornian.com.au
- in writing to The Capricornian Bank
  PO Box 1135
  Rockhampton Qld 4700

Further Help

If you are not satisfied with the resolution offered by our staff members, you can have your complaint reviewed free of charge by the Australian Financial Complaints Authority (**AFCA**), an external dispute resolution scheme.

The AFCA is designed to offer fair, independent and accessible dispute resolution for consumers who are unable to resolve complaints directly with their financial services provider. In most cases you have two years to submit a complaint to AFCA after you have raised it with us and received a final outcome from us. Before AFCA investigates your complaint, they will generally give us an opportunity to resolve or respond to it.

Phone: 1800 931 678
Mail: Australian Financial Complaints Authority
GPO BOX 3, Melbourne VIC 3001
Email: info@afca.org.au
Website: www.afca.org.au

PRIVACY NOTIFICATION

OUTLINE

This Privacy Notification sets out:

- why we collect and use your information
- how we collect and use your information
- what happens if you do not wish to provide us with information
- whether we provide your information to other entities
- the availability of our Privacy Policy
- when we can disclose certain information to a credit reporting body
- how a credit reporting body may use your information
- whether we disclose your information overseas and if so, where
- how you can contact us.

COLLECTION & USE OF YOUR INFORMATION

We collect and use your information to:

- provide you with membership benefits, financial services and products or information about those benefits, services and products
- provide you with information about financial services and products from 3rd parties we have arrangements with
- conduct market and demographic research in relation to the products and services you and other members acquire from us
- protect the safety and security of our staff and visitors
- establish your eligibility for a loan
- establish your capacity to repay a loan.

The law also requires us to collect and hold your information:

- for our register of members under the Corporations Act
- to verify your identity and meet our obligations under the AML/CTF Act
- to assess your capacity to pay a loan under the National Consumer Credit Protection Act.

HOW WE COLLECT YOUR INFORMATION

We will collect information about you and your financial position from you directly.

When you apply for a loan, or for an increase to your credit limit, we will collect information about your credit history from a credit reporting body. We can do this without your consent.

The credit reporting body will record the fact that we have enquired about your credit history, and that record may be disclosed to other credit providers, and used and disclosed by the credit reporting body or a credit provider to assess your credit worthiness, including in the calculation of your credit score or credit rating.

When a credit enquiry is recorded on your credit report, it can affect your credit score in different ways. It might go up, down, or stay the same. This depends on factors like the type of credit you're applying for, how many other credit checks you've had recently, and other details in your report. An enquiry is more likely to lower your credit score if you make a lot of credit applications in a short time.

HOW YOU CAN ACCESS YOUR INFORMATION

You can request access to your information at any time.

WHAT IF YOU DO NOT WISH TO PROVIDE US WITH INFORMATION?

If you do not give us the information we require, we may not be able to admit you to membership or provide you with the financial service or product you have applied for.

PROVIDING YOUR INFORMATION TO CREDIT REPORTING BODIES

The credit reporting bodies we disclose information to is Equifax Pty Ltd and Experian Data Registries Pty Ltd.

If you do not make your repayments when they fall due or commit a serious credit infringement, we may disclose this to Equifax Pty Ltd and Experian Data Registries Pty Ltd. Any information we provide to Equifax Pty Ltd or Experian Data Registries Pty Ltd will be included in reports provided to credit providers to help them to assess your creditworthiness.

You can ask Equifax Pty Ltd and Experian Data Registries Pty Ltd not to use your information for pre-screening of direct marketing by a credit provider. You can also ask them not to use or disclose your information if you reasonably believe that you have been or are likely to be a victim of fraud.

Equifax Pty Ltd and Experian Data Registries Pty Ltd policy on the management of information is available at www.equifax.com.au/privacy, https://www.experian.com.au/content/dam/noindex/apac/australia/ExperianAustralia-PrivacyPolicy-FINAL.pdf

You can contact Equifax by: Telephone 13 83 32

You can contact Experian by: Telephone 1300 783 684

PROVIDING YOUR INFORMATION TO OTHER ENTITIES

We disclose your information to other entities. We can disclose your information to:

- entities that verify identity or help us comply with our obligations under the AML/CTF Act
- providers of payment and card services, when you make a transaction or receive a payment using a payment service or a card
- entities that help identify illegal activities and prevent fraud
- lawyers, conveyancers, accountants, brokers and agents who represent you
- contractors for statement printing and mail out, card and cheque production, market research or direct marketing
- affiliated product and service suppliers to provide information to you about their services and products
- credit reporting bodies and other financial institutions that have previously lent to you
- persons you use as referees
- for property loans – property valuers and insurers
- mortgage documentation service
- trustee and manager of securitised loan programs
- any guarantor or proposed guarantor of a loan
- debt collection agencies, lawyers, process servers
- our auditors.

We may disclose your personal information to a lenders mortgage insurer –*Helia Insurance Pty Limited or QBE* Lenders Mortgage Insurance Limited - if we decide to insure the loan. Individual lenders mortgage insurer's Privacy Policy can be viewed at https://helia.com.au/privacy-policy and www.qbe.com/lmi/about/governance/privacy-policy

We and the above third parties will also disclose your information to law enforcement and government agencies as required by law.

OUR PRIVACY POLICY

Our Privacy Policy is available at www.capricornian.com.au/privacy-policy/. The Policy contains information about:

- how you can access your information
- how you can seek correction of your information
- how you make a complaint and how we will deal with it
- in what overseas countries we are likely to disclose your information
- how we manage your credit-related personal information.

OVERSEAS DISCLOSURE

We do not currently disclose your credit information or credit eligibility information to entities that do not have an Australian link.

We do not currently disclose any of your other information to overseas recipients.

HOW TO CONTACT US

If you have any questions, wish to request a correction of the personal information we hold about you, or wish to make a complaint, you can contact us at:

- in person at one of our branches
- by calling us on 1300 314 900
- by email at info@capricornian.com.au
- in writing to The Capricornian Bank
  PO Box 1135
  Rockhampton Qld 4700

Australian Information Commissioner (**OAIC**)

You may also elect to contact the office of the Australian Information Commissioner (OAIC) if you have a complaint about the way we handle your personal information at:

- Post: GPO BOX 5288 Sydney NSW 2001
- Phone: 1300 363 992
- Fax: +61 2 6123 5145
- Email: foi@oaic.gov.au

ACCOUNT & ACCESS FACILITY

HOW TO CONTACT US

Visit us at any of our branches. Branch details and locations available at our website - https://www.capricornian.com.au/branch-locations/

Phone us on (07) 4931 4900

Write to us at
PO Box 1135 Rockhampton QLD 4700

Fax us on 07 4931 4970

To report the loss, theft or unauthorised use of your Visa card in Australia

- outside of business hours, call the VISA Card Hotline on 1800 139 241. Please also contact us to report the loss, theft or unauthorised use.
- **overseas – for Visa**
  Please contact us before you travel overseas for the current Visa hotline arrangements

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

CUSTOMER OWNED BANKING CODE OF PRACTICE

We warrant that we will comply with the Customer Owned Banking Code of Practice. Please see the section About the Customer Owned Banking Code of Practice at the end of these Conditions of Use for more detail.

EPAYMENTS CODE

We warrant that we will comply with the ePayments Code.

HOW OUR CONDITIONS OF USE BECOME BINDING ON YOU

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

ACCESSING COPIES OF THE CONDITIONS OF USE

Please keep these Conditions of Use in a safe place so you can refer to it when needed. Alternatively, you can view and download our current Conditions of Use from our website at https://www.capricornian.com.au/documents/conditions-of-use/

FINANCIAL CLAIMS SCHEME

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

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

WHAT IS THE CAPRICORNIAN'S ACCOUNT AND ACCESS FACILITY?

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

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

Please refer to the *Accounts & Availability of Access Facilities* brochure (Page 44) for available account types, the conditions applying to each account type and the access methods attaching to each account type.

HOW DO I OPEN AN ACCOUNT?

You will need to become a member of the Credit Union before we can issue The Capricornian Account and Access Facility to you. To become a member, you will need to:

- complete a membership application form; and
- subscribe for a member share in the Credit Union.

PROOF OF IDENTITY REQUIRED

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

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

- a Photo card (NSW only);
- a State or Territory drivers licence or proof of age card
- an Australian current passport or one that has expired within the last 2 years;
- a photo drivers licence issued by a foreign government;
- a passport issued by a foreign government, the United Nations or a UN agency; or
- a national ID card, with photo and signature, issued by a foreign government, the United Nations or a UN agency.
- Digital ID Verification Solution

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

The law does not allow you to open an account using an alias without you also giving us all the other names that you are commonly known by.

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

WHAT ACCOUNTS CAN I OPEN?

When we issue you with The Capricornian Account and Access Facility, you have access to the Personal Access Account. You can then activate other accounts as needed. Please first check the *Accounts & Availability of Access Facilities* brochure (Page 44) for the different account types available, any special conditions for opening, and the features and benefits of each account type.

JOINT ACCOUNTS

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

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

You can operate a joint account on an 'all to sign' or 'either/or to sign' basis:

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

All joint account holders must consent to the joint account being operated on an 'either/or to sign' basis. However, any one joint account holder can cancel this arrangement, making it 'all to sign'.

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

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

TRUST ACCOUNTS

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

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

WHAT FEES AND CHARGES ARE THERE?

Please refer to the *Account Fees and Transaction Limits and Schedule of Fees & Charges* brochures (Page 47) for current fees and charges. We may vary fees or charges from time to time.

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

WHAT INTEREST CAN I EARN ON MY ACCOUNT?

Our website has information about our current deposit and savings interest rates. We may vary deposit or savings interest rates from time to time on all deposit accounts except our term deposit accounts.

Our *Accounts & Availability of Access Facilities* brochure (Page 44) discloses how we calculate and credit interest to your account.

WHAT ARE THE TAXATION CONSEQUENCES?

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

DISCLOSING YOUR TAX FILE NUMBER (TFN)

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

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

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

Businesses need only quote their ABN instead of a TFN.

THIRD PARTY 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.

You can specify which of your accounts under The Capricornian Account & Access Facility you give the authorised person authority to operate on. You are responsible for all transactions your authorised person carries out on your account. **You should ensure that the person you authorise to operate on your account is a person you trust fully.**

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

MAKING DEPOSITS TO THE ACCOUNT

You can make deposits to the account:

- by direct credit e.g. from your employer for wages or salary – please note that we can reverse a direct credit if we do not receive full value for the direct credit
- by transfer from another account with us
- by transfer from another financial institution

DEPOSITS USING ELECTRONIC EQUIPMENT

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

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

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

WITHDRAWING OR TRANSFERRING FROM THE ACCOUNT

You can make or authorise withdrawals from the account:

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

unless otherwise indicated in the *Accounts & Availability of Access Facilities* brochure (Page 44).

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

DEBITING TRANSACTIONS GENERALLY

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

We have the right to decline to accept your authorisation for any transaction if we are uncertain for any reason of the authenticity or validity of the authorisation or your legal capacity to give the authorisation. We will not be liable to you or any other person for any loss or damage which you or such other person may suffer as a result of our action.

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

OVER THE COUNTER WITHDRAWALS

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

Please check:

- the *Accounts & Availability of Access Facilities* brochure (Page 44) for any restrictions on withdrawals applying to certain accounts; and
- the *Account Fees and Transactional Limits* and *Access Limits* brochures (Pages 49 & 50) for any applicable daily cash withdrawal limits or other transaction limits.

WITHDRAWAL TRANSACTION LIMITS

We limit the amount of daily withdrawals or payments you may make using electronic methods, either generally or in relation to a particular facility. These transaction limits are set out in the *Account Fees and Transaction Limits and Schedule of Fees & Charges* brochures (Page 47).

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

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

OVERDRAWING AN ACCOUNT

You must keep sufficient cleared funds in your account to cover your direct debit and electronic transactions (including PayTo payments). If you do not, we can dishonour the transaction and charge dishonour fees: see the *Account Fees and Transaction Limits and Schedule of Fees & Charges* brochures (Page 47).

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

- interest at our current overdraft rate, calculated on the daily closing balance; or
- a fee for each day (or part of a day) your account is overdrawn: see the *Account Fees and Transaction Limits and Schedule of Fees & Charges* brochures (Page 47).

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

SWEEP FACILITIES

You may nominate an account (the first account) which is 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 nominal balance or in credit. However, we are not obliged to transfer funds if there are insufficient funds in the second account to draw on.

ACCOUNT STATEMENTS

We will send you account statements at least every 6 months (including the three months period in which your account is closed). You can ask us for an account statement at any time. We may charge a fee for providing additional statements or copies: see the *Account Fees and Transaction Limits and Schedule of Fees & Charges* brochures (Page 47)

We can also provide your statements electronically. Please ask us about this facility.

Each statement will record all transactions on your account since the last statement. We recommend that you check your account statement as soon as you receive it. Immediately notify us of any unauthorised transactions or errors. Please refer to *How to Contact Us* on page 12 for our contact details.

WHAT HAPPENS IF I CHANGE MY NAME OR ADDRESS?

We recommend that if you change your name or address, you let us know immediately.

DORMANT ACCOUNTS

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

Once your account becomes dormant, we may:

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

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

ACCOUNT COMBINATION

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

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

We will not combine accounts if to do so would breach the Code of Operation for Centrelink Direct Credit Payments and any successor Code (both when enforcing indebtedness owed to us and, to the extent the law permits, when facilitating enforcement by a third-party judgement creditor).

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

CLOSING ACCOUNTS AND CANCELLING ACCESS FACILITIES

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

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

After giving you reasonable notice (Not less than 14 days).We can:

- close your account by notifying you and paying out the balance of your account;
- cancel any access facility for security reasons or if you breach these Conditions of Use; or classify your account as dormant (see section on “Dormant Accounts” above).

NOTIFYING CHANGES

We may change fees, charges, interest rates and other conditions at any time. The following table sets out how we will notify you of any change.

Type of change	Notice
Increasing any fee or charge	20 days
Adding a new fee or charge	20 days
Reducing the number of fee-free transactions permitted on your account	20 days
Changing the minimum balance to which an account keeping fee applies	20 days
Changing the method by which interest is calculated	20 days
Changing the circumstances when interest is credited to your account	20 days
Changing deposit interest rates	on the day of change
Increasing your liability for losses relating to ePayments (see the ePayments Conditions of Use Section 3 on page 23 for a list of ePayments)	20 days
Imposing, removing or changing any periodic transaction limit	20 days
Changing any other term or condition	when we next communicate with you

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

- notification by letter;
- notification on or with your next statement of account;
- notification on or with the next newsletter;
- advertisements in the local or national media; and
- notification on our website.

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

HOW WE SEND NOTICES & STATEMENTS

We may send you notices and statements:

- by post, to the address recorded in our records or to a mailing address you nominate;
- by fax;
- by email; and
- by advertisement in the media, for some notices only.

If you agree, we may, instead of sending you a notice or statement, post notices or statements to our website for you to retrieve. We will tell you when information is available for you to retrieve, either at the time or on setting up a facility that will have regular postings to the website.

You can change your email address, or revert to receiving paper notices or statements, at any time.

We have a dispute resolution system to deal with any complaints you may have in relation to The Capricornian Account and Access Facility or transactions on the account. Our dispute resolution policy requires us to deal with any complaint efficiently, speedily and sympathetically. If you are not satisfied with the way in which we resolve your complaint, or if we do not respond speedily, you may refer the complaint to our external dispute resolution centre.

If you want to make a complaint, contact our staff at any branch and tell them that you want to make a complaint. 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 dispute resolution system available to you on request.

Further Help

If you are not satisfied with the resolution offered by our staff members, you can have your complaint reviewed free of charge by the Australian Financial Complaints Authority (**AFCA**), an external dispute resolution scheme.

The AFCA is designed to offer fair, independent and accessible dispute resolution for consumers who are unable to resolve complaints directly with their financial services provider. In most cases you have two years to submit a complaint to AFCA after you have raised it with us and received a final outcome from us. Before AFCA investigates your complaint, they will generally give us an opportunity to resolve or respond to it.

Phone: 1800 931 678

Mail: Australian Financial Complaints Authority

GPO BOX 3, Melbourne VIC 3001

Email: info@afca.org.au

Website: www.afca.org.au

If you think we have breached the Customer Owned Banking Code of Practice, you can make a complaint to the Code Compliance Committee by:

Phone: 1800 931 678 (This is a telephone service provided by AFCA- please ask to speak to the Code team.

Fax: 03 9613 7481

Mail: PO Box 14240 Melbourne VIC 3001

Email: info@codecompliance.org.au

Media enquiries: media@codecompliance.org.au

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

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

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

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

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

This section does not apply to PayTo, which provides an alternative method to pre-authorise a biller to debit amounts from your eligible account. For PayTo see electronic access facilities and ePayments conditions of use 0 to 0.

PAYPAL

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

- you are responsible for all PayPal debits to your account
- if you dispute a PayPal debit, you can contact PayPal directly or ask us to do so
- we are not responsible for compensating you for any disputed PayPal debit, or for reversing any disputed PayPal debit to your account
- if you want to cancel your direct debit arrangement with PayPal, you can contact PayPal directly or ask us to do so; and
- when you ask us to pass on a disputed transaction to PayPal, or your request 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.

Payment Services Generally

Although we endeavour to effect payments, we do not accept responsibility to make them, and accordingly we won't incur any liability through any refusal or omission to make payments or by any reason of late payment or failure to follow instructions.

We may determine the priority of payments from your account at our absolute discretion.

A payment instruction will remain in force for our protection in respect of payments made in good faith after your death, bankruptcy or cancellation of the instructions or until we receive notice of any of those events.

We are not required to pay an amount which exceeds the available balance of your account.

INFORMATION ABOUT OUR EPAYMENT FACILITIES

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

Important Information You Need to Know Before Using a Device to Make Electronic Payments

- Sign the access card as soon as you receive it.
- Familiarise yourself with your obligations to keep your access card and pass codes secure.
- Familiarise yourself with the steps you have to take to report loss or theft of your access card or to report unauthorised use of your access card, BPAY®, PayTo or our mobile banking app or internet banking.
- Immediately report lost, theft or unauthorised use.
- If you change a pass code, do not select a pass code which represents your birth date or a recognisable part of your name.
- Never write the pass code on the access card.
- Never write the pass code PIN on anything which is kept with or near the access card.
- Never lend the access card to anybody.
- Never tell or show the pass code to another person.
- Use care to prevent anyone seeing the pass code being entered on a device.
- Keep a record of the VISA card number and the VISA Card Hotline telephone number for your area with your usual list of emergency telephone numbers.
- Check your statements regularly for any unauthorised use.
- Immediately notify us when you change your address.
- ALWAYS access our mobile banking app or internet banking service only using the OFFICIAL phone numbers and URL addresses.
- If accessing internet banking on someone else's PC, laptop, tablet or mobile phone, ALWAYS DELETE your browsing history.
- ALWAYS REJECT any request to provide or to confirm details of your pass code. We will NEVER ask you to provide us with these details.

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

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

Visa Card	Internet Banking
BPAY®	Mobile Banking App (the cap app)
Osko® Payments	PayTo

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

Visa Card

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

- check your account balances;
- withdraw cash from your account;
- make payments at retailers; and
- make online purchases.

We may choose not to give you a Visa Card if your banking history with the Credit Union is not satisfactory or if you are under 12 years of age.

Important Information about Chargebacks for VISA Card

If you believe a Visa Card transaction was:

- for goods or services and the merchant did not deliver them; or
- for goods and services which did not match the description provided by the merchant,

then you can ask us to 'chargeback' the transaction, by reversing the payment to the merchant's financial institution. You can do so by telling us within 30 days after the date of the statement that shows the transaction and providing us with any information we may require.

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

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

DEFINITIONS

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

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

ATM means automatic teller machine

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

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

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

ATM card;

debit card or credit card; and

token issued by a subscriber that generates a pass code;

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

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

facility means an arrangement through which you can perform transactions;

identifier means information that a user:

knows but is not required to keep secret; and

must provide to perform a transaction;

Examples include an account number or member number.

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

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

Migrated DDR Mandates has the meaning given in clause 1 of 0 "Migration of Direct Debit arrangements"

pass code means a password, code or pattern that the user must keep secret, that may be required to authenticate a transaction or user. A pass code may consist of patterns, numbers, letters, a combination of both, or a phrase.

Examples include:

personal identification number (PIN);

internet banking password;

mobile banking app password;

code generated by a security token; and

Osko® Payments smart address (PayID).

Cap App access pattern

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

Payment Agreement means an agreement established by you and an approved merchant or Payment Initiator, by which you authorise us to make payments from your account. Other than in 0 “Creating a PayTo Payment Agreement”, it includes a Migrated DDR Mandate

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

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

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

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

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

unauthorised transaction means a transaction that is not authorised by a user; and

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

a third party signatory to your account; and

a person you authorise us to issue an additional card to.

we, **us** or **our** means The Capricornian Ltd trading as The Capricornian Bank (The Capricornian Bank)

you means the person or persons in whose name this Account & Access Facility is held.

TRANSACTIONS

These ePayment 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.

Without limiting clause 3.1, these ePayment 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;

mobile banking app and bill payment transactions;

internet banking transactions, including ‘Pay Anyone’;

online transactions performed using a card number and expiry date;

online bill payments (including BPAY);

direct debits;

transactions using mobile devices;

Osko Payments; and

PayTo payments.

WHEN YOU ARE NOT LIABLE FOR LOSS

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

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

a device, identifier or pass code which is forged, faulty, expired or cancelled

a transaction requiring the use of a device and/or pass code that occurred before the user received the device and/or pass code (including a reissued device and/or pass code)

a transaction being incorrectly debited more than once to the same facility; and

an unauthorised transaction performed after we have been informed that a device has been misused, lost or stolen, or the security of a pass code has been breached.

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

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

In a dispute about whether a user received a device or pass code:

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 pass code 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 pass code.

WHEN YOU ARE LIABLE FOR LOSS

If 0 does not apply, you may only be made liable for losses arising from an unauthorised transaction in the circumstances specified in this Section 5.

Where we can prove on the balance of probability that a user contributed to a loss through fraud, or breaching the pass code security requirements in 0:

you are liable in full for the actual losses that occur before the loss, theft or misuse of a device or breach of pass code security is reported to us; and

you are not liable for the portion of losses:

incurred on any one day that exceeds any applicable daily transaction limit;

incurred in any period that exceeds any applicable periodic transaction limit;

that exceeds the balance on the facility, including any pre-arranged credit; and

incurred on any facility that we and you had not agreed could be accessed using the device or identifier and/or pass code used to perform the transaction.

Where:

more than one pass code is required to perform a transaction; and

we prove that a user breached the pass code security requirements in 0 for one or more of the required pass codes, but not all of the required pass codes

> you are liable under clause 0 only if we also prove on the balance of probability that the breach of the pass code security requirements under 0 was more than 50% responsible for the losses, when assessed together with all the contributing causes.

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

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

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

are liable for the actual losses that occur between:

when the user became aware of the security compromise, or should reasonably have become aware in the case of a lost or stolen device, and

when the security compromise was reported to us; and

are not liable for any portion of the losses:

incurred on any one day that exceeds any applicable daily transaction limit;

incurred in any period that exceeds any applicable periodic transaction limit;

that exceeds the balance on the facility, including any pre-arranged credit; and

incurred on any facility that we and you had not agreed could be accessed using the device and/or pass code used to perform the transaction.

Note: You may be liable under clause 0 if you were the user who contributed to the loss, or if a different user contributed to the loss.

Where a pass code was required to perform an unauthorised transaction, and clauses 0-0 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 pass code, including any prearranged credit; and

the actual loss at the time that the misuse, loss or theft of a device or breach of pass code security is reported to us, excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit.

In deciding whether on the balance of probabilities we have proved that a user has contributed to losses under clauses 0 and 0:

we must consider all reasonable evidence, including all reasonable explanations for the transaction occurring

the fact that a facility has been accessed with the correct device and/or pass code, 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 pass code security requirements in 0; 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.

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.

PASS CODE SECURITY REQUIREMENTS

0 applies where one or more pass codes are needed to perform a transaction.

A user must not:

voluntarily disclose one or more pass codes to anyone, including a family member or friend;

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

carried with a device;

liable to loss or theft simultaneously with a device;

unless the user makes a reasonable attempt to protect the security of the pass code; and

where a device is not needed to perform a transaction, keep a written record of all pass codes 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 pass code(s).

For the purpose of clauses 0–0, a reasonable attempt to protect the security of a pass code record includes making any reasonable attempt to disguise the pass code within the record, or prevent unauthorised access to the pass code record, including by:

hiding or disguising the pass code record among other records;

hiding or disguising the pass code record in a place where a pass code record would not be expected to be found;

keeping a record of the pass code record in a securely locked container; and

preventing unauthorised access to an electronically stored record of the pass code record.

This list is not exhaustive.

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

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

Note 2: For the obligations applying to the selection of a pass code by a user, see clause 0.

A user must not select a numeric pass code that represents their birth date, or an alphabetical pass code 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.

The onus is on us to prove, on the balance of probability, that we have complied with clause 0.

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 pass code security requirements in 0.

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 pass code that is required or recommended for the purpose of using the service does not breach the pass code security requirements in 0.

LIABILITY FOR LOSS CAUSED BY SYSTEM OR EQUIPMENT MALFUNCTION

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

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

correcting any errors; and

refunding any fees or charges imposed on the user.

NETWORK ARRANGEMENTS

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

we are a party to a shared electronic payments network; and

another party to the network caused the failure to meet the obligation.

We must not require you to:

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

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

AUDIT TRAILS

a) we must ensure that we can generate sufficient records to enable transactions to be traced and checked and to identify and correct errors.

DIGITAL WALLETS

9.1 This section applies to you, or an additional card holder, add an eligible Card to a Digital Wallet on a Supported Device. This Section applies in addition to the terms and conditions that apply to the Account and eligible Card.
Information about using Digital Wallets with our Eligible Cards, including how to add and remove Eligible Cards from Supported Devices, is available on The Capricornian website at https://www.capricornian.com.au/banking/access-your-money/digital-wallets/

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

9.3 Your Security Responsibilities

You, and each additional card holder, agree to protect and keep confidential your User ID, phone lock pass code, passwords and all other information required for you to make purchases with your eligible card using the Digital Wallet.

(a) At all times, you agree to protect your pass code by using a unique number that is secure and not easily guessed or deciphered. You agree, at all times, to take precautions when using the Digital Wallet. You must, at all times, protect your pass code.
(b) You, and each additional card holder, must:
    (i) not allow any other person's biometric identifier (for example, Face ID and fingerprint) to remain or be registered, on the supported device;
    (ii) not share any PIN or other pass code registered to the supported device with any person; or
    (iii) remove or unlink the eligible card from a supported device before disposing of that supported device.
(d) If you, or an additional card holder, allow another person's biometric identifier to remain or be registered on the supported device, or share any PIN or pass codes registered to the supported device with any person, then you are taken to have authorised that person to carry out transactions using the supported device and you will be responsible for their use of the eligible card. If your device has been lost or stolen, or you believe your security credentials have been compromised, you must immediately report it to The Capricornian Contact Centre Customer Service on 1300 314 900.
(e) You should immediately remove or unlink your eligible card from the Digital Wallet if your supported device is lost or stolen, or you believe your security credentials have been compromised.
(f) You should immediately contact us if your eligible card is lost or stolen, or you believe your security credentials have been compromised, including suspicions of any fraud activity.
(g) You may be liable for any unauthorised transactions should you delay notifying us and the delay is unreasonable.

9.4 Using Digital Wallets

a) Before allowing you or an additional cardholder to add an eligible card to the Digital Wallet, we will take steps to verify your and/or the additional card holder's identity. The addition of the eligible card to the Digital Wallet is at the discretion of us.
b) If your eligible card is a dual network debit card, depending on the network available to you, you may have the option to choose the network by which to process your payment – Visa or eftpos. eftpos may not be available for payments within apps, on the web or for use overseas.
c) As Apple Pay and Google Pay are provided by Apple and Google, we are not responsible or liable for their functionality or availability or any refusal by a merchant to process a transaction using Apple Pay or Google Pay except to the extent caused by the mistake, fraud, negligence or wilful misconduct of us, our agents or employees.
d) We are not responsible for any security breach affecting any information stored in the Digital Wallet or sent from the Digital Wallet. This is the responsibility of the Pay provider.

9.5 Your Information

a) We can provide Apple and Google and any card scheme networks with information required for the purpose of operating and generally improving Apple Pay or Google Pay. Each party's data collection and handling practices are in accordance with their respective privacy policies (Please refer to the providers' websites for their respective privacy policies).
b) By registering your eligible card within the Digital Wallet and agreeing to the T&Cs, you consent to us sharing your information with Apple, Google, Visa and eftpos. Do not register your eligible card with Apple Pay or Google Pay if you don't want us to collect or share this information with Apple Pay or Google Pay.
c) We are not responsible for any loss, injury or other harm you suffer in connection with Apple, Google, Visa or eftpos use of your information except to the extent caused by the mistake, fraud, negligence or wilful misconduct of us, our agents or employees.

9.6 You Agree to Allow Us to Contact You Electronically

a) You acknowledged that we may contact you electronically (via sms, email or app notifications) and that this is considered written notice for the purpose of these terms.

9.7 Changes to these Terms and Conditions (T&C's)

a) We may amend these Apple Pay and Google Pay T&Cs at any time and will notify you in accordance with the Conditions of Use.

b) By continuing to keep your eligible card in the Digital Wallet, you agree to the amendments.

9.8 Fees and Charges

a) The Apple Pay and Google Pay T&Cs and any relevant Product Schedules describe the fees and charges which apply to your eligible card. We do not charge you additional fees for adding or using Apple Pay or Google Pay.
b) You are responsible for any third-party charges associated with the use of Apple Pay or Google Pay (such as carrier or mobile data charges).

9.9 Privacy

a) To allow you to use the eligible card via the Digital Wallet, we may share and exchange with the Digital Wallet provider your personal information relevant to the setup and use of the Digital Wallet.

9.10 Removing your eligible card from a Digital Wallet

a) If you no longer wish to use your eligible card through a Digital Wallet, remove your eligible card from the Digital Wallet by following the card removal process (this process can be found on the Apple website and Google website).

9.11 Suspension or Removal of a card from a Digital Wallet by us

a) We may suspend or terminate the use of an eligible card in a Digital Wallet without notice and at any time, including if:
   (i) you, or an additional card holder, breach the Conditions of Use or these Digital Wallet T&Cs;
   (ii) we suspect a security issue/breach including if an unauthorised transaction has occurred; or
   (iii) we are required to do so under the instructions of a regulatory or governmental body.

9.12 Devices with the same Digital Wallet provider Account

a) If you add an eligible card to one of your devices and have other devices sharing the same account, this may permit the card to be added to the other devices and permit users of the other devices to see card information.

9.13 Definitions

Account means your account with us to which an **eligible card** is linked.

Account holder means the person who holds the account under the Conditions of Use.

eligible card means a debit or credit card issued by us that can be added to Apple Pay or Google Pay.

Apple is a trademark of and means Apple Inc. and includes its related bodies corporate and facilities including Apple Pty Limited ABN 46 002 510 054.

Apple Pay means the mobile digital wallet service provided by Apple.

Conditions of Use means The Capricornian's Conditions of Use (as supplemented, amended, updated or replaced from time to time) available on The Capricornian website.

Google is a trademark of and means Google Inc. and includes its related bodies corporate and facilities.
Google Pay means the mobile digital wallet service provided by Google. Google Pay (and Android) are trademarks of Google.

supported device means the device you use to access Apple Pay (such as an iPhone, Apple Watch or an iPad).

Visa means Visa Inc. or any Visa Inc. group company (including Visa Worldwide Pte. Limited).

Visa Debit Card has the meaning given to that term in the Conditions of Use.

we, **us**, **our**, **Capricornian** or **The Capricornian** means The Capricornian Limited ABN 54 087 650 940 and our successors and assigns.

you or **your** means the account holder and/or the additional cardholder.

MISTAKEN INTERNET PAYMENTS

In this Section 10:

direct entry means a direct debit or direct credit

mistaken internet payment means a payment by a user through a 'Pay Anyone' internet banking facility and processed by an ADI 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.

This does not include payments made using BPAY or PayTo.

receiving ADI means an ADI whose customer has received an internet payment; and

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

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

If we are satisfied that a mistaken internet payment has occurred, we must send the receiving ADI a request for the return of the funds

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

(i) acknowledge the request by the sending ADI for the return of funds, and

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

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

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

You may complain to us about how the report is dealt with, including that we 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 clauses 0-0, or as described in the box below.

When we receive a complaint under clause 0 we must:

deal with the complaint under our internal dispute resolution procedures

not require you to complain to the receiving ADI.

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

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

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

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

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

➢ **Process where funds are available & report is made within 10 business days**

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

➢ **Process where funds are available & report is made between 10 business days & 7 months**

- The receiving ADI must complete its investigation into the reported mistaken payment within 10 business days of receiving the request.
- If satisfied that a mistaken internet payment has occurred, the receiving ADI must:

a. prevent the unintended recipient from withdrawing the funds for 10 further business days, and

b. notify the unintended recipient that it will withdraw the funds from their account, if the unintended recipient does not establish that they are entitled to the funds within 10 business days commencing on the day the unintended recipient was prevented from withdrawing the funds.

- If the unintended recipient does not, within 10 business days, establish that they are entitled to the funds, the receiving ADI must return the funds to the sending ADI within 2 business days after the expiry of the 10 business day period, during which the unintended recipient is prevented from withdrawing the funds from their account.
- If the receiving ADI is not satisfied that a mistaken internet payment has occurred, it may seek the consent of the unintended recipient to return the funds to the holder.
- The sending ADI must return the funds to the holder as soon as practicable.

➢ **Process where funds are available and report is made after 7 months**

- If the receiving ADI is satisfied that a mistaken internet payment has occurred, it must seek the consent of the unintended recipient to return the funds to the user.
- If not satisfied that a mistaken internet payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder.
- If the unintended recipient consents to the return of the funds:

a. the receiving ADI must return the funds to the sending ADI, and

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

➢ **Process where funds are not available**

- Where the sending ADI and the receiving ADI are satisfied that a mistaken internet payment has occurred, but there are not sufficient credit funds available in the account of the unintended recipient to the full value of the mistaken internet payment, the receiving ADI must use reasonable endeavours to retrieve the funds from the unintended recipient for return to the holder (for example, by facilitating repayment of the funds by the unintended recipient by instalments).

USING OUR MOBILE BANKING APP (THE CAP APP) AND INTERNET BANKING

We do not warrant that:

the information available to you about your accounts through our home banking service is always up to date;

you will have 24 hours a day, 7 days per week, access to our mobile banking app or internet banking; and

data you transmit via the mobile banking app or internet banking is totally secure.

HOW TO REPORT LOSS, THEFT OR UNAUTHORISED USE OF YOUR ACCESS CARD OR PASS CODE

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

Please refer to How to Contact Us on page 12 for our contact details.

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

The access card HOTLINE is available when calling outside of business hours.

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

If the loss, theft or misuse, occurs OUTSIDE AUSTRALIA you must notify an organisation displaying the VISA sign and also then confirm the loss, theft or misuse of the card:

with us by telephone or priority paid mail as soon as possible; or

by telephoning the VISA Card Hotline number for the country you are in.

VISA CARD HOTLINE

AUSTRALIA WIDE TOLL FREE

1800 139 241

HOW TO REPORT UNAUTHORISED USE OF THE MOBILE BANKING APP OR INTERNET BANKING

If you believe that your pass codes for the mobile banking app or internet banking transactions have been

misused, lost or stolen, or, where relevant, your pass code has become known to someone else, you must contact us immediately.

Please refer to How to Contact Us on page 12 for our contact details. We will acknowledge your notification by giving you a reference number that verifies the date and time you contacted us. Please retain this reference number.

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

USING THE ACCESS CARD

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

We will advise you from time to time:

what transactions may be performed using access card;

what ATMs of other financial institutions may be used; and

what the daily cash withdrawal limits are.

Please refer to the *Account Fees and Transaction Limits and Schedule of Fees & Charges* brochure (Pages 47 & 50) *for details of current transaction limits*

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

The access card always remains our property.

USING VISA OUTSIDE AUSTRALIA

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

All transactions made in a foreign currency on the Visa Card are subject to a conversion fee. Please refer to the *Fees & Charges and Transaction Limits* brochure (Pages 47 & 48) for the current conversion fee.

Some overseas merchants and electronic terminals charge a surcharge for making a transaction using your Visa card. Once you have confirmed that transaction you will not be able to dispute the surcharge. The surcharge may appear on your statement as part of the purchase price.

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

ADDITIONAL ACCESS CARD

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

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

We will give each additional cardholder a separate pass code.

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

To cancel the additional access card you must notify us in writing. However, this cancellation may not be effective until the additional access card is returned to us or you have taken all reasonable steps to have the additional access card returned to us.

You will not be liable for the continued use of the additional access card from the date that you have:

notified us that you want it cancelled; and

taken all reasonable steps to have the additional access card returned to us.

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

USE AFTER CANCELLATION OR EXPIRY OF ACCESS CARD

You must not use your access card:

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

after the access card has been cancelled.

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

EXCLUSIONS OF ACCESS CARD WARRANTIES AND REPRESENTATIONS

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

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

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

CANCELLATION OF ACCESS CARD OR OF ACCESS TO HOME BANKING SERVICE, BPAY®, OSKO® OR PAYTO

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

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

for security reasons;

if you breach the Conditions of Use;

you, or someone acting on your behalf, is being fraudulent;

we suspect that you are using Osko® in a manner that is likely to affect our ability to continue providing Osko® to you or our other customers;

if we cease to be a participant in Osko® or PayTo, or

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

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

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

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

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

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

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

you cease to be our member; or

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

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

USING BPAY®

BPAY is a simple and convenient way to pay your bills 24 hours a day, 7 days a week. You can use BPAY® to pay bills bearing the BPAY® logo from those accounts that have the BPAY® facility.

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

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

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

PROCESSING BPAY® PAYMENTS

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

you become aware of any delays or mistakes in processing your BPAY payment;

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

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

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

A BPAY payment instruction is irrevocable.

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

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

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

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

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

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

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

Please note that the BPAY® payment may take longer to be credited to a biller if you tell us to make it on a Saturday, Sunday or a public holiday or if another participant in BPAY® does not process a BPAY® payment as soon as they receive its details.

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

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

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

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

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

advise you of this;

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

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

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

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

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

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

FUTURE-DATED BPAY® PAYMENTS

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

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

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

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

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

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

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

CONSEQUENTIAL DAMAGE FOR BPAY® PAYMENTS

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.

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.

USING OSKO®

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

make an Osko® payment

make scheduled and recurring Osko® payments

receive payment reminders

pay bills bearing the Osko® logo from those accounts that have the Osko® facility

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.

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

PROCESSING OSKO® PAYMENTS

We will attempt to make sure that your Osko® payments are processed promptly by participants in Osko®, and 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.

An Osko® payment instruction is irrevocable.

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.

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

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

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 Osko® payment; and

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

SCHEDULED AND RECURRING OSKO® PAYMENTS

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

You may schedule Osko® payments up to 60 days in advance of the time of payment and you can schedule Osko® 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 recurrent Osko® payment is made correctly;

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

you must contact us if you wish to cancel a scheduled or recurrent Osko® payment after you have given the direction by before the date of payment.

REGULAR PAYMENT ARRANGEMENTS

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

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

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

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

AUTHORITY TO RECOVER MISTAKEN OR MISDIRECTED PAYMENTS

Where we and the sending financial institution determine that an NPP Payment made to your Account is either a Mistaken Payment or a Misdirected Payment, we may, without your consent, and subject to

complying with any other applicable Terms and Conditions, deduct from your Account, an amount up to the original amount of the Mistaken Payment or Misdirected Payment. We will notify you by writing as soon as practicable if this occurs.

CREATING A PAYTO PAYMENT AGREEMENT

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

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

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

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

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

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

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

This 0 does not apply to Migrated DDR Mandates.

Amending a PAYMENT Agreement

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

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

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

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

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

Once a Payment Agreement has been established, you may instruct us to amend your name or transfer the Payment Agreement to another account you hold with us. If you wish to transfer the Payment Agreement to an account with another financial institution, you may, when available, give us a transfer instruction (see 0 “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

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

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

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

TRANSFERRING YOUR PAYMENT AGREEMENT

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

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

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

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

CANCELLING YOUR PAYMENT AGREEMENT

You may instruct us to cancel a Payment Agreement on your behalf. We will act on your instruction promptly by updating the record of the Payment Agreement in the Mandate Management Service. The Mandate Management Service will notify the merchant’s or Payment Initiator’s financial institution or payment processor of the cancellation. We are not liable for any loss that you or any other person may suffer as a result of cancelling a Payment Agreement.

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

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

MIGRATION OF DIRECT DEBIT ARRANGEMENTS

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

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

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

GENERAL PAYTO PROVISIONS

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. See “overdrawing an account” on page 16 for our rights if there are insufficient funds in your account.

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

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

We recommend that you allow notifications from The Capricornian via email, SMS or through the cap app or online banking] to ensure that you’re able to receive and respond to Payment Agreement creation requests, amendment requests and other notifications in a timely way.

You are responsible for ensuring that: (i) all data you provide to us or to any merchant or Payment Initiator that subscribes to PayTo is accurate and up to date; (ii) you do not use PayTo to send threatening, harassing or offensive messages to the merchant, Payment Initiator or any other person; and (iii) any passwords/PINs needed to access the facilities we provide are kept confidential and are not disclosed to any other person.

All intellectual property, including but not limited to the PayTo 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: (i) modifications to Our Intellectual Property by or on behalf of you in a manner that causes the infringement; (ii) use of any item in combination with any hardware, software or other products or services in a manner that causes the infringement and where such combination was not within the reasonable contemplation of the parties given the intended use of the item; (iii) your failure to use corrections or enhancements to Our Intellectual Property that are made available to you (except where the use of corrections or enhancements would have caused a defect in PayTo or would have had the

effect of removing functionality or adversely affecting the performance of PayTo); and (iv) your failure to use Our Intellectual Property in accordance with this agreement.

We may cancel or suspend your use of PayTo in accordance with our rights under 0 “Cancellation of access card or of access to home banking service, BPAY®, Osko® or PayTo”.

We may amend the terms and condition relating to PayTo in accordance with our rights under “notifying changes” on page 18. 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 under *Access Limits* (Page 50). 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:

transferring your PayID to another account (whether with us or another financial institution) will not automatically transfer the Payment Agreement to that account, and payments under the linked Payment Agreement will fail (subject to clause 0);

closing your PayID will cause payments under the linked Payment Agreement to fail (subject to clause 0).

To ensure payments under a linked Payment Agreement continue after transferring or closing the PayID you will also need to either link the Payment Agreement to an account with us (see 0 “Amending a Payment Agreement”) or, when available, transfer the Payment Agreement to another financial institution (see 0 “Transferring your Payment Agreement”).

PRIVACY AND PAYTO

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

AUTHORITY FOR PAYTO INSTRUCTIONS

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

CONFIRMATION OF PAYEE SERVICE

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

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

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

CONDUCTING A CONFIRMATION OF PAYEE LOOKUP

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

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

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

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

USE AND DISCLOSURE OF YOUR ACCOUNT DETAILS

You authorise, and provide consent to:

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

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

In special circumstances we may allow you to opt-out of the Confirmation of Payee service. Please contact us by calling 1300 314 900.

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.

In some circumstances you may provide alternative names to be recorded on your account for use in the Confirmation of Payee service. Please contact us by calling 1300 314 900.

SECTION 50. ACCOUNT CLOSURE REASONS

50.1. The Capricornian Bank reasonably suspects fraudulent or illegal use of the account or access facility

(a) if we reasonably suspect that a transaction may breach a law or sanction

(b) if we identify the purchase is for the purpose of gambling and you are under the age (of 18)

(c) to comply with our legal and regulatory obligations including our related policies and procedures

(d) or if you fail to provide us with information or documents was reasonably request

Prior Notice will be provided with fair timeframes to get alternatives sorted.

ABOUT THE CUSTOMER OWNED BANKING CODE OF PRACTICE

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

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

Our 7 Key Promises to you are:

1. We will be deliver banking services in the interests of our customers.
2. We will obey the law.
3. We will not mislead or deceive.
4. We will act honestly and fairly.
5. We will offer products and services that are fit for general purpose.
6. We will deliver services with reasonable care and skill.
7. We will contribute to our community.

You can download a copy of the Customer Owned Banking Code of Practice here

https://www.customerownedbanking.asn.au/storage/COBCOP/coba-55634-code-of-practice-a4-34pp-10-v15-16784273839WBsl.pdf

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

Code Compliance Committee Mutuals
PO Box 14240
Melbourne VIC 8001
Phone: 1800 367 287
Fax: 03 9613 7481
info@codecompliance.org.au
http://www.cobccc.org.au/for-consumers/resolving-complaints/

The Code Compliance Committee Mutuals (CCC) is an independent committee, established in accordance with the Code, to ensure that subscribers to the Code are meeting the standards of good practice that they promised to achieve when they signed up to the Code. The CCC investigates complaints that the Code has been breached and monitors compliance with the Code through as mystery shopping, surveys, compliance visits and complaint handling.

Please be aware that the CCC is not a dispute resolution body. To make a claim for financial compensation we recommend you contact us first. You can contact our external dispute resolution provider, the Australian Financial Complaints Authority (AFCA), directly. However, they will refer the complaint back to us to see if we can resolve it directly with you before involving them.

You can contact AFCA:

Online:	www.afca.org.au
Email:	info@afca.org.au
Phone:	1800 931 678 (free call)
Mail:	Australian Financial Complaints Authority GPO Box 3 Melbourne VIC 3001

ACCOUNT FEES AND TRANSACTION LIMITS

PERSONAL AND SAVINGS ACCOUNTS

	Personal Access	isaver	Everyday Saver	Club Account	Business Access
Electronic Transactions					
• Visa Debit[2]	free	na	na	na	free
• payWave	free	na	na	na	free
• Capricornian ATM Withdrawals, Balances & Declined	free	na	na	na	free
• EFTPOS incl declined transactions	$0.70	na	na	na	$0.70
• Visa Debit Cash Advance[3]	$0.70	na	na	na	$0.70
Internet & Mobile Banking app					
• Internal Funds Transfers	free	free	free	free	free
• External Funds Transfers	free	$1.00	free	free	free
• BPAY®	free	$1.00	free	free	free
• Direct Credits	free	free	free	free	free
• Direct Debits	free	$1.00	free	$0.30	free
Branch and Contact Centre					
• Cash Deposits	free	free	free	free	free
• Cash Withdrawals	free	na	free	free	free
• Internal Funds Transfer	free	na	free	free	free
• External Funds Transfer	free	na	$3.00	$3.00	$3.00
• BPAY®	free	na	$3.00	$3.00	$3.00
Account Service Fee	First account free for eligible members[1] $6.00 per month subsequent accounts	free	free	free	First account free for eligible members[4] $10.00 per month subsequent accounts

Footnote:

[1] Account Service Fee Exemptions on Personal Access Accounts:

- Members aged 25 years old & younger
- Members aged 65 years and older
- Minimum Deposit/Lending balance of $20,000 held within the membership

Personal Access Account transaction fees apply to Credit Line, Mortgage Line of Credit and Mortgage Plus Home Loan products.

[2] Where credit option is selected for purchases only

[3] Where credit option is selected for cash/cash and purchase transaction

[4] Account Service Fee Exemptions on Business Access Accounts:
Minimum Deposit/Lending balance of $20,000 held within the membership

ACCOUNTS & AVAILABILITY OF ACCESS FACILITIES

Current as at: 28 November 2025

This document must be read together with The Capricornian Account & Access Facility Conditions of Use and the Fees & Charges and Transaction Limits Brochure

Account	Access Account S1	Student Access Account S1	Packaged Access Account S2	Youth Access Account S7	Pension Access Account S50
	A simple and flexible everyday account, easy to transact with direct credit of your pay or other income and flexible withdrawal and transaction options to suit you.	Specifically designed exclusively for students, apprentices and trainees with 24/7 access to your hard earned money.	An everyday transaction account. specifically designed for our existing Packaged Home Loan Members (no longer available)	An access and savings account for your young people up to the age of 16 years offering a fully transactional account with a credit interest incentive.	An account exclusively aimed at our senior members who receive an aged pension into their Capricornian account or self-funded retirees aged 65 years and over, offering a solid return on their funds and a fair account fee structure.
Account Features					
Visa Debit Card	✓	✓	✓	✓	✓
ApplePay/GooglePay	✓	✓	✓	✓	✓
EFTPOS/ATM Access	✓	✓	✓	✓	✓
Internet & Mobile Banking app	✓	✓	✓	✓	✓
BPAY®	✓	✓	✓	✓	✓
Direct Credits/Debits	✓	✓	✓	✓	✓
Osko®	✓	✓	✓	✓	✓
PayTo®	✓	✓	✓	✓	✓
Interest					
Calculated daily	×	×	×	✓	✓
Paid	×	×	×	Monthly	Quarterly
Offset against home loan	×	×	×	×	×
Optional Overdraft	✓	✓	×	×	×
Over the Counter					
Withdraw Cash	✓	✓	✓	✓	✓
Deposit Cash/Foreign Cheques	✓	✓	✓	✓	✓
Transfer to another financial institution	✓	✓	✓	✓	✓
Transfer to another Capricornian account	✓	✓	✓	✓	✓

Current as at: 28 November 2025

This document must be read together with The Capricornian Account & Access Facility Conditions of Use and the Fees & Charges and Transaction Limits Brochure

	Savings Accounts	
Account	**iSaver** **S5**	**Everyday Saver** **S29**
	An on-line savings account with a high interest rate. Electronic access through internet banking service 24/7 with strong interest returns.	An alternative to the iSaver offering a competitive interest rate with access via the internet, phone or over the counter.
Account Features		
Visa Debit Card	×	×
ApplePay/GooglePay	×	×
EFTPOS/ATM Access	×	×
Internet & Mobile Banking app	✓	✓
BPAY®	✓	✓
Direct Credits/Debits	✓	✓
Osko®	✓	✓
PayTo®	✓	✓
Interest		
Calculated daily	✓	✓
Paid	Monthly	Monthly
Offset against home loan	✓	×
Optional Overdraft	×	×
Over the Counter		
Withdraw Cash	×	✓
Deposit Cash/Foreign Cheques	✓	✓
Transfer to another financial institution	×	✓
Transfer to another Capricornian account	×	✓

ACCOUNTS & AVAILABILITY OF ACCESS FACILITIES

Current as at: 28 November 2025

This document must be read together with The Capricornian Account & Access Facility Conditions of Use and the Fees & Charges and Transaction Limits Brochure

	Business Accounts	**Club Accounts**	**Investment Accounts**
Account	**Business Banking S19**	**Club Account S26**	**Term Deposit I3, I6, I12 & I24**
	Designed for our business members, the business banking account is a simple and flexible fully featured everyday transaction account.	Specifically designed for our non-profit clubs and associations offering a simple and flexible transaction accounts as well as a competitive credit interest rate.	Members seeking to 'grow a nest egg' with longer term deposits. Deposits available for 3, 6 12 & 24 month terms at attractive "better than at-call" rates.
Account Features			
Visa Debit Card	✓	✓	×
ApplePay/GooglePay	✓	✓	×
EFTPOS/ATM Access	✓	✓	×
Internet & Mobile Banking app	✓	✓	×
BPAY®	✓	✓	×
Direct Credits/Debits	✓	✓	×
Osko®	✓	✓	
PayTo®	✓	✓	
Minimum Deposit	×	×	$5,000
Interest			
Calculated daily	×	✓	✓
Paid	×	Monthly	Monthly, Annually or at Maturity
Offset against home loan	×	×	×
Optional Overdraft	✓	×	×
Over the Counter			
Withdraw Cash	✓	✓	On Maturity
Deposit Cash/Foreign Cheques	✓	✓	✓
Transfer to another financial institution	✓	✓	On Maturity
Transfer to another Capricornian account	✓	✓	On Maturity

SCHEDULE OF FEES AND CHARGES - Current as at 28 November 2025

Service Charges

Account and Statement Fees

Transaction Listing/Statement Copy	*$2.00 per page*
Document Search	*$40.00 per hour*
Monthly Paper Statement *(65 years or older - Nil)*	*$2.50*
Quarterly Paper Statement	*Nil*
Monthly E-Statement	*Nil*

Transfer Fees

RTGS/IPEX Outwards - same day transfer	*$20.00*
RTGS/IPEX Inwards	*$10.00*
Auto Transfer Dishonour	*Nil*

Cheque Fees

Foreign Cheque Deposit	*$15.00*
Foreign Cheque Deposit sent as Bill for Collection	*$75.00*
(plus third party costs from drawer institution)	

Deposit Book Issue Fee

Business Deposit Book - duplicate	*$5.00*

Direct Entry Fees

Direct Debit Dishonour	*$15.00*
Debit Exception	*Nil*
Direct Entry Trace Fee	*$25.00*
EFT Recall	*$50.00*
EFT Exception	*$5.00*
Stopped Payment Direct Entries	*$5.00*
Mistake Payment Fee	*$25.00*

Debit Card Fees

VISA Card Issue	*Nil*
ATM Enquiry/Dispute	*Nil*
VISA Card Replacement	*$25.00*
VISA Card Priority Express *(Domestic)*	*$60.00*
VISA Card Quarterly Fee	*$6.00*
Emergency VISA	*USD200.00*
VISA Card Recovery	*USD175.00*
VISA Card Voucher Enquiry	*$20.00*
Foreign Currency Conversion Fees	
(Foreign Currency will be converted to Australian currency at the wholesale market rate by VISA)	*3% of transaction value*

Other Fees

Coin Handling *(over $100)*	*5% of the total coin*
BPAY Enquiry	*$6.00*
BPAY Error Correction Fee	*$25.00*
Dormant Fee - account inactive for 12 months	*$5.00 /month*
Sweeping Dormant Funds to Unclaimed Money	*$20.00*
Recording Address as Unknown	*$2.50*
Audit/Certificate of Balance	*$40.00*
Sweep Fee	*Nil*

Honour Fee

An honour fee will apply if a Direct Debit payment overdraws your account or is paid against uncleared funds:

Honour Fee	*$20.00*

Credit Control Fees

All Third Party costs associated with the collection of loan arrears and overdrawn accounts will be passed on

1st Reminder Letter Fee	*$15.00*
2nd and subsequent Reminder Letter Fee	*$20.00*
Default Notice Fee	*$40.00*
Summons Fee	*$100.00*
Debt Agreement Fee	*$100.00*
Reminder Call Fee	*$5.00*
Account Combination Transfer/Journal	*$5.00*
Personal Default Visit	*$100.00*
Garnishee Processing Fee	*At Cost*

Fixed Term Deposits

The penalty applied to an early redemption of a Fixed Term Deposit is:

30 Days interest on the redeeming portion of the deposit

International Services

Convera

Telegraphic Transfer (TT) via Internet Banking	*$20.00*
Telegraphic Transfer (TT) Over the Counter	*$30.00*
Telegraphic Transfer in Australian Dollars	*$50.00*
Telegraphic Transfer Stop Payment	*$15.00*
Telegraphic Transfer Traces	*$25.00*

Foreign exchange margin of 5.95% applies for purchases with any merchant located outside of Australia

TT amendments and cancellations are subject to currency conversion changes

Cash Passport

Initial Load	*greater of 1.1% or $15.00*
Additional Card Fee	*$5.00*
BPAY reloads	*1%*
In-store reloads	*greater of 1.1% or $15.00*
Debit Card Load Fee	*$5.00*
EFTPOS	*Free*
International ATM withdrawal fee	*subject to Country and Currency*
Domestic ATM withdrawal fee	*2.95% of amount withdrawn*
Cash Out Fee	*$10.00*
Monthly inactivity fee (card inactive for 12 months)	*Free*
Negative balance fee	*Free*
Replacement Card Fee	*Free*

SCHEDULE OF LOAN FEES AND CHARGES - Current as at 28 November 2025

ESTABLISHMENT FEES

Mortgage Secured Loans & Lines of Credit

Establishment Fee - *Includes one valuation up to the cost of $300 - Excludes additional valuation costs and solicitor's costs to prepare mortgage documents and settlement fees.*

- Establishment Fee	*$600.00*
- Further Advance Establishment Fee	*$400.00*
- Bridging Loan Establishment Fee (No end debt)	*$1500.00*

Personal Loans & Overdrafts

Establishment Fee	*$250.00*

Commercial Loans & Overdrafts

Establishment Fee

Excludes solicitor's costs in mortgage & security preparation, valuation/s & settlement fees

- New Application Under $20,000	*$500.00*
- New Application $20,001-$100,000	*$600.00*
- New Application $100,001-$250,000	*$800.00*
- New Application greater than $250,000	*$1,000.00*
- Top up Application (Overdraft only)	*$400.00*

Temporary Overdrafts - Personal and Commercial

- $100 - $10,000	*$100.00*
- Greater than $10,000	*$250.00*

Performance (Credit Union) Guarantees

Excludes additional valuation costs and solicitor's costs to prepare mortgage documents and settlement fees.

Establishment Fee

($250 or 0.25% of the Bank Guarantee amount, whichever is greater)

Re-documentation fee (if you need to make changes to your documentation later)

($250 or 0.25% of the Bank Guarantee amount, whichever is greater)

Maintenance Fee (charged half yearly)	*3% p.a.*

State duties and taxes may apply. Fees incurred to search the records of a government agency and to register or vary the interest with a government agency are payable by the borrower.

SERVICE FEES

Service Fee

Home Loans	*$10.00 per month*
Payable on Mortgage Plus Home Loans	
Personal Overdrafts *(Overdraft Service Fee)*	*$5.00 per month*
Commercial Loans *(Loan Service Fee)* & Overdrafts *(Overdraft Service Fee)*	
· Under $5,000	*$5.00 per month*
· $5,001-$100,000	*$20.00 per month*
· $100,001-$250,000	*$30.00 per month*
· Greater than $250,000	*$50.00 per month*

Contract Variation & Consent Fee

A fee is charged when a member applies to vary their loan conditions including:

· Mortgage Secured Loans and Overdrafts	*$400.00*
· Personal Loans & Overdrafts (not mortgage secured)	*$150.00*

Fixed Rate Break Costs Payable during a fixed rate period when a member: repays the unpaid balance of their loan in full; makes unscheduled repayments totalling $10,000 or more; switches from one fixed rate to another; or switches from fixed rate to a variable rate loan	*Break costs can be obtained by contacting The Capricornian.*
Fixed Rate Lock Fee Allows you to secure a guaranteed fixed interest rate to protect you against potential interest rate increases that may occur during the settlement period of your loan. Fee is the greater of 0.15% of the amount of credit or $395 where funding is more than 60 days from the date of the Offer and Loan Contract.	
Mortgage Discharge Fee *This fee is payable in addition to solicitors fees, registration, searches and other third party fees that may apply*	*$300.00*
Arrears Fees	
1st Reminder Letter Fee	*$15.00*
Reminder call fee	*$5.00*
2nd and Subsequent Reminder Letter Fee	*$20.00*
Default Notice Fee	*$40.00*

ACCESS LIMITS

Cash Withdrawal Limitations for Access Cards & Accounts	Daily Limit
At any branch of The Capricornian cash withdrawal	$2,000.00 unless prior arrangements are made
ATM/EFTPOS within Australia	$1,000 combined limit
Visa Debit Card when credit option chosen	Balance of Account
payWave limits	$200 transaction account limit $1,000 daily transaction account limit

Please note that EFTPOS outlets may have other restrictions on the amount of cash that can be withdrawn. Merchants or other financial institutions my impose additional restrictions on the use of your Visa Debit card or other access method including but not limited to restrictions on cash withdrawals or services provided.

Withdrawal Limitations for Internet Banking	Daily Limit (per account)
Transfers by BPAY payment	$10,000.00 unless prior arrangements are made
Transfers to Internal accounts	$5,000.00 unless prior arrangements are made
Transfers to external third party account	$3,000.00 unless prior arrangements are made
International Transfers	$3,000.00 unless prior arrangements are made
New Payments Platform (NPP)	$3,000.00 unless prior arrangements are made

EFTPOS ISSUER TERMS

1. The timing of when the eftpos consumer's account will be debited for an eftpos Transaction

The timing of when the eftpos consumer's account will be debited for an eftpos transaction: This refers to the specific point in time when the funds are withdrawn from the consumer's bank account as a result of an eftpos transaction.

In more detail

a) **eftpos transaction**: When a consumer uses their card to make a purchase or other transaction at a point of sale (POS) terminal.

b) **Account debited**: The money is subtracted from the consumer's bank account.

The timing can vary depending on several factors

(a) **Immediate debit:** In many cases, the consumer's account is debited immediately or within a few minutes after the transaction is completed.

(b) **Batch processing**: Some transactions may be processed in batches at the end of the business day, meaning the debit could occur later that day or the next day.

(c) **Bank processing times**: Different banks may have different processing times which can affect when the debit actually occurs.

2. Disputed Transaction and Chargeback rights of the eftpos Consumer

Disputed transaction

a) This refers to a situation where a consumer challenges a transaction made through the eftpos system.

b) Common reasons for disputing a transaction include unauthorised transactions, incorrect transaction amounts, duplicate charges, or not receiving the goods or services paid for.

Chargeback rights

a) Chargeback rights are the consumer's rights to request a reversal of a disputed transaction.

b) If a consumer believes there has been an error or fraud, they can initiate a chargeback process through The Capricornian Bank.

c) The Capricornian will investigate the dispute, and if it is found to be valid, the transaction amount will be refunded to the consumer's account.

Process

a) **Initiation**: The consumer contacts The Capricornian to report the disputed transaction.

b) **Investigation**: The Capricornian will investigate the claim by reviewing transaction records, communicating with the merchant, and gathering relevant evidence.

c) **Resolution**: If the dispute is resolved in favour of the consumer, a chargeback is issued, and the funds are returned to the consumer's account. If the merchant's side is favoured, the charge remains.

Rights and protections*:*

a) eftpos consumers are typically protected by rules and regulations that govern electronic payment systems.

b) These protections ensure that consumers can dispute unauthorised or incorrect transactions and have a fair process for resolving disputes.

3. **Terms informing eftpos Consumers how Mobile Devices will be Provisioned for eftpos Mobile, including the process to be undertaken by the eftpos Consumer and the exchange of communications with the eftpos Consumer and other nominated parties that will take place, together with a statement of the nature of the information exchanged;**

Terms informing eftpos consumers how mobile devices will be provisioned for eftpos mobile. This refers to;

a) **Provisioning**: This refers to the steps the consumer needs to follow to enable their mobile device (e.g., smartphone or tablet) to perform eftpos transactions. This includes accessing the Wallet app, adding a Visa Debit Card, and verifying their identity.

b) **Activation**: Activation completes the provisioning process by verifying identification using=, SMS or using confirming details through a secure online portal, facilitated by The Capricornian.

c) **Notifications and Alerts**: Consumers will receive messages during the provisioning process, including SMS notifications and in-app alerts. These communications ensure that the consumer is informed about each step and any required actions.

d) **Customer Support**: Consumers can contact The Capricornian's Contact Centre for customer support if encountering issues during provisioning.

The Capricornian Contact Centre

Call: 1300 314 900

8.30am to 4.45pm **Monday** to **Thursday**
8.30am to 5pm **Friday**

Email: info@capricornian.com.au
Chat online: www.capricornian.com.au inside business hours

A statement of the nature of the information exchanged:

a) **Personal Information**: When provisioning a mobile device for eftpos mobile transactions (Digital Wallet), the consumer will need to provide name, Capricornian Visa Debit card details, and confirmation of identification.

b) **Transaction Information**: The common types of data communicated during transactions, include transaction amounts, merchant details, and timestamps.

c) **Security Information**: The Capricornian adheres to regulated Payment Card Industry (PCI) requirements, compliance and security protocols and data protection measures. The eftpos mobile services (Digital Wallet service) ensures sensitive card data is tokenised, with industry best practice protocols backed by eftpos' trusted infrastructure.

4. **Any limitations to the use of eftpos Mobile or eftpos In-App Payment, including the supported transactions for the eftpos Consumer, the availability constraints where there is diminished or no telephone reception and that there are a limited number of pre-loaded Payment Token keys that may be utilised if reception or connectivity to the eftpos Issuer host is lost, the limitations associated with the profile of the eftpos Card or eftpos Account Provisioned to the Mobile Device;**

4.1 This refers to:

a) Transaction Types: Details on which types of transactions are supported by the eftpos mobile and in-app payment system. For example, it may support contactless purchases, in-app purchase, online purchases.

Availability constraints where there is diminished or no telephone reception

Reception Issues: eftpos mobile and in-app payments may rely on a stable internet or mobile network connection. In areas with poor or no reception, the ability to complete transactions could be affected.

Connectivity: The consumer may experience delays or the inability to process transactions in real-time if the mobile device cannot connect to the network.

The limited number of pre-loaded payment token keys that may be utilised if reception or connectivity to the eftpos issuer host is lost

a) **Payment Tokens**: Payment tokens are secure, encrypted codes that represent a consumer's payment information. These can be pre-loaded onto the mobile device for offline use.

b) Token Limitation: There is a finite number of these tokens stored on the device. If the device loses connectivity to the eftpos issuer's host (e.g., The Capricornian), the consumer can only use the pre-loaded tokens until connectivity is restored.

Limitations associated with the profile of the eftpos card or eftpos account provisioned to the Mobile Device

a) **Card/Profile Restrictions**: Specific limitations tied to the type of eftpos card or account linked to the mobile device. For example, some cards may have transaction limits and geographic restrictions or may not support certain types of purchases.

b) **Account Features**: The features and capabilities available may vary depending on the account type (e.g., standard account vs. premium account) and the policies of the financial institution issuing the eftpos card.

5. Any rights of the eftpos Consumer, the eftpos Issuer, the Original Equipment Manufacturer (OEM),as relevant, and any other party to direct a change in the Payment Token due to a lifecycle event and the process to be used by the eftpos Consumer to give effect to those rights;

a) **eftpos Consumer**: The consumer has the right to request a change in their payment token under certain circumstances. This might include situations like replacing a lost or stolen card, updating their card information, or addressing security concerns.

b) **eftpos Issuer**: The issuer (e.g., The Capricornian) has the right to initiate changes to the payment token. This could be due to security updates, card replacements, expiration of the token, or other lifecycle events like fraud prevention measures.

c) **Original Equipment Manufacturer (OEM):** The manufacturer of the mobile device or the payment app provider may have the right to request a change in the payment token if there are updates or changes to the device's operating system, security features, or payment app.

d) **Other Parties**: This might include payment processors or third-party service providers involved in the payment ecosystem who may also have the right to request changes to ensure the security and functionality of the payment system.

Lifecycle Event

a) **Lifecycle Event**: An event that necessitates a change in the payment token. Examples include card expiration, card replacement, suspected fraud, security breaches, or updates to the payment app or mobile device.

Process to be Used by the eftpos Consumer to Give Effect to Those Rights

a) **Notification**: The consumer needs to be notified of the need to change the payment token. This notification could come from the issuer, OEM, or another relevant party.

b) **Authorisation**: The consumer may need to authorise the change. This could involve verifying their identity, confirming the reason for the change, and agreeing to the update.

c) **Update Procedure**: The consumer will follow a specified procedure to update the payment token. This might involve:

i. **Using an App**: Opening the payment or banking app on their mobile device and following prompts to update the token.

ii. **Customer Support**: Contacting The Capricornian Contact Centre support for assistance with the update.

iii. **Automatic Updates**: In some cases, the update may be performed automatically by the issuer or OEM, with the consumer only needing to confirm the change.

d) **Verification**: The updated payment token will need to be verified to ensure it works correctly. The consumer may need to perform a test transaction or follow other verification steps.

6. That the eftpos Consumer is authorised to:

a) use or receive the benefit of The Capricornian's Tokenisation service; and/or

Authorisation

a) **eftpos Consumer Rights**: The eftpos consumer (i.e., the cardholder or user of the eftpos service) is granted permission to use the The Capricornian's tokenisation service. This means they have the legal right to utilise this service as part of their eftpos payment solution.

Tokenisation Service

a) **Definition**: Tokenisation is a security process that replaces sensitive payment information (such as card numbers) with a unique identifier or "token." This token can be used to process payments without exposing the actual card details.

b) **Benefits**: The consumer benefits from enhanced security, as tokenisation reduces the risk of fraud and data breaches. It ensures that their actual payment information is not exposed during transactions.

Use or Receive the Benefit

a) **Utilisation**: The consumer can actively use the tokenisation service when making transactions, ensuring their payment information is securely processed.

b) **Receiving Benefits**: The consumer also passively benefits from the security measures implemented by the tokenisation service, which protect their payment information even if they are not directly interacting with the tokenisation process.

Use or receive the benefit of any eftpos applet embedded in an OEM Solution

Authorisation

a) **eftpos Consumer Rights**: The eftpos consumer is also authorised to use any eftpos applet that is embedded in an OEM solution. This means they have the legal right to access and utilise this applet as part of their eftpos service.

eftpos Applet

a) **Definition**: An applet is a small application or program designed to perform specific functions within a larger system. In this context, the eftpos applet is a software component embedded in the consumer's mobile device or other hardware provided by the OEM.

b) **Functionality**: The eftpos applet facilitates eftpos transactions, enabling the consumer to make payments using their mobile device or other OEM-provided hardware.

Embedded in an OEM Solution

a) **OEM Solution:** An OEM solution refers to hardware or software provided by the device manufacturer (e.g., a smartphone or tablet with pre-installed payment software).

b) **Integration**: The eftpos applet is integrated into the OEM solution, meaning it comes pre-installed or is embedded within the device or system provided by the manufacturer.

Use or Receive the Benefit

a) **Utilisation**: The consumer can use the eftpos applet to conduct transactions, leveraging the applet's functionality to make payments.

b) **Receiving Benefits:** The consumer also passively benefits from the convenience and integration of the applet within their device, which streamlines the payment process and enhances user experience.

7. **For the purposes of initiating and completing valid eftpos Transactions using enabled Mobile Devices, provided that the eftpos Consumer does not:**

a) grant any sublicenses to The Capricornian's Tokenisation service software and/or eftpos applet (as the case may be)

No Sublicensing

- **Prohibition**: The eftpos consumer is not permitted to sublicense The Capricornian's tokenisation service software or eftpos applet. Sublicensing refers to giving others the right to use this software. This restriction ensures that only authorised users have access to The Capricornian's proprietary technology, preventing unauthorised distribution or use.

a) copy, reverse engineer, decompile, disassemble, modify, adapt or make error corrections to The Capricornian's Tokenisation service software and/or eftpos applet (as the case may be), in whole or in part; or

Protection of Intellectual Property

- **Prohibited Actions**: The eftpos consumer is not allowed to:

Copy: Reproduce the software or applet.

b) **Reverse Engineer**: Analyse the software to understand its underlying structure, design, or functionality.

c) **Decompile**: Convert the software's binary code back into a human-readable format.

d) **Disassemble**: Break the software down into its component parts.

e) **Modify or Adapt**: Make changes or adaptations to the software.

f) **Make Error Corrections**: Attempt to fix any bugs or errors in the software.

- **In Whole or in Part:** These prohibitions apply to both the entire software and its individual components. These restrictions protect The Capricornian's intellectual property rights and ensure the integrity of its software.

a) attempt to gain unauthorised access to any infrastructure or software used by The Capricornian to provide the The Capricornian's Tokenisation service and/or eftpos applet (as the case may be) through any means.

Security and Access Control

a) **Unauthorised Access**: The eftpos consumer is prohibited from attempting to gain access to The Capricornian's infrastructure or software systems without proper authorisation. This includes backend systems, databases, servers, or any other components involved in providing the tokenisation service or eftpos applet.

b) **Through Any Means:** This prohibition covers all potential methods of gaining unauthorised access, such as hacking, exploiting security vulnerabilities, or using any other illicit means. This ensures that The Capricornian's systems remain secure, and that access is strictly controlled.