Hiver

Hiver Bank Conditions of Use

Accounts and Access

Important information

Who we are

Hiver Bank is a division of
Teachers Mutual Bank Limited
ABN 30 087 650 459
AFSL/Australian Credit Licence 238981.

Other divisions of Teachers Mutual Bank Limited are:

- Teachers Mutual Bank
- Firefighters Mutual Bank
- UniBank
- Health Professionals Bank

In this document, "the Bank", "we", "us" and "our" means Teachers Mutual Bank Limited; and "you" means a person with one or more of our products or services.

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 details.

ePayments Code

We warrant that we will comply with the ePayments Code.

Privacy

We have a Privacy and Credit Reporting Policy that sets out:

- our obligations regarding the confidentiality of your personal information and
- how we collect, hold, use and disclose your personal information.

You can access our Privacy & Credit Reporting Policy on our website.

How our Conditions of Use become binding on you

By opening an account or using an access facility you become bound by these Conditions of Use.

Accessing copies of this document

You can view and download this document from our website. Please keep a copy so you can refer to it when needed.

The Financial Claims Scheme

In the unlikely event that a bank, credit union or building society fails, the Australian Government may activate its guarantee scheme known as the Financial Claims Scheme (FCS). This enables account holders to have quick access to their deposits which are protected under the FCS. Depositors are protected up to $250,000 for each account holder at each licensed ADI.

Please note that, as stated, the FCS guarantee is per account holder per institution. We operate under more than one brand name but have only one banking licence. The limit of $250,000 consequently applies to the total funds any account holder has in deposit products issued by us, not withstanding that a particular product or service may carry any one of our brand names.

For further information about the Financial Claims Scheme visit

www.apra.gov.au/financial-claims-scheme

Contents

Division 2: Electronic Access Facilities and ePayments Conditions of Use

Division 1: Opening and operating your accounts

Joining us

Before you can open an account with us, you will need to become a member of the Bank. To do this download the Hiver app and complete the membership application process and open an Everyday and Saver Account.

If we accept your application, you need to pay $10 for a share and then you become a shareholding member and you are bound by our Constitution. You can find our Constitution on our website.

To become a member you must be:

- 18 years of age or over; and
- An Australian citizen; and

you must meet the eligibility criteria under our Constitution, which includes:

- Either:
  - (a) Currently employed in Health Care, Education, Emergency Services;or
  - (b) Studying at or have graduated from an Australian university; or
- A family member of an existing member.

Membership and accounts can only be opened for individuals solely or personal purposes and not for business purposes.

Accounts and access facilities

These Conditions of Use Accounts and Access govern the use of the following range of accounts, which includes transaction accounts and savings accounts and these access facilities:

- Visa Card (including mobile wallets and contactless transactions)
- Fast Payments via Osko Payment;
- BPAY
- Electronic banking via the Hiver App or internet banking)
- EFTPOS and ATM access
- Direct debit
- Direct credit
- Periodical payment
- PayTo

We may refuse to provide any banking product or service at our discretion.

Please refer to the table on page 6 for account types, conditions and access facilities

Proof of identity

Under the Anti-Money Laundering and *Counter-Terrorism Financing Act, 2006* we are required to verify your identity when you open an account, when you become a signatory to an account.

Account details

Refer to the details below and the table on page 12 for the account types available and their access options.

Introductory, bonus and promotional interest

From time to time we may offer a higher rate or additional interest to certain account holders of these accounts with respect to certain funds held within these accounts, which will be subject to specified criteria and for limited or specific periods of time. Where we offer higher or additional interest, it may be calculated and paid in a different manner to the standard interest paid on these accounts.

If you make withdrawals from these accounts during a specified period or you close your account before the end of a specified promotional or introductory period, you may lose your eligibility for the higher rate or additional interest.

Details of any offer, including eligibility and how interest will be calculated and paid, will be publicised in promotional material and on our website during the relevant period.

Transaction accounts

Everyday Account

This is a daily electronic transaction account with a range of access methods including Visa Debit card and electronic banking

Saver Account

For the convenience of keeping money separate from your Everyday account, saving online and to earn a higher interest rate than our transaction accounts, this account can be accessed through electronic banking.

This account pays bonus interest each month, if during the month, you make one deposit per month and no more than one withdrawal in that same month and your account has a credit balance at all times. This last requirement means that your account must not be overdrawn at any time during the month, including, e.g. during a day, or when the balance is carried forward from the previous month. If all criteria are not met, the standard interest rate will apply.

Summary of accounts and access facilities

Account		
	Everyday account	**Saver account**
Minimum opening deposit	$0	$0
Interest calculated	N/A	Daily
Interest paid	N/A	Monthly
ATM	✓	×
EFTPOS	✓	×
Electronic banking	✓	✓
Direct debit	✓	✓
BPAY	✓	✓
Internal periodical payment	✓	✓
Electronic funds transfer	✓	✓
Direct credit	✓	✓
PayTo	✓	✓
Link PayID	✓	✓
Can receive NPP payment	✓	✓
Can send NPP payment	✓	✓

Fees and charges

Refer to the Fees and charges brochure available on the Hiver app or our website for current details. We may vary fees or charges from time to time. We will debit fees and charges from your transaction account.

Fees and charges brochure

The Fees and charges brochure is referenced throughout these Conditions of Use – Accounts and access. You can get a copy of this brochure on our website.

Information about non-standard fees and charges

Your account may have specific account related fees and charges, for example, a monthly account fee. Non-standard fees apply in particular situations, for example, fees if you overdraw an account. We have prepared some general information on how to avoid or minimise non-standard fees and charges. You can find this information by visiting our website.

Interest earned

If a variable interest rate applies to your account, this rate may vary from time to time. Our website and the Hiver app provide information about our current interest rates.

We may at any time, subject to giving you the appropriate prior notice:

- vary interest rates on all accounts;
- set balance amounts above which we will not pay any interest.

We will calculate interest daily by applying the daily interest rate to the cleared closing balance of your account at the end of the day. The daily interest rate is the relevant annual interest rate divided by 365 and the end of the day is the time we treat as being the end of the day for our end of day transaction processing on your account. Interest will be credited to your account on or about the last day of each month.

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

Tax File Numbers

We will ask you whether you want to disclose your Tax File Number (TFN) or exemption. If you disclose it, we will note your TFN against any account you open. 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 plus the Medicare Levy.

Deposits and withdrawals

How to deposit

You can make deposits to the account:

- by cheque at all offices;
- electronic credit e.g. from a third party such as your employer, for wages or salary – please note that we can reverse a direct credit if we do not receive full value for the electronic credit;
- transfer from another account with us; or
- by electronic funds transfer from another financial institution.

Note: Electronic deposits may not be processed on the same day.

Cheque deposits

You may deposit a cheque at any of the Bank's branches. All cheques for deposit can only be accepted if it is issued in the name of the account holder whether it has been endorsed or not. Cheques payable to a company or business cannot be paid into a personal account in circumstances.

If a cheque deposited to your account is dishonoured, putting your account into debit or exceeding any credit limit you may have, you are responsible for bringing the account back into credit or under the credit limit.

The proceeds of the cheque may not be available until it has cleared which may take up to 7 business days.

In certain circumstances we may allow you to draw on the proceeds a cheque drawn on Australian Banks, building societies and mutual entities before it is cleared.

If we allow you to draw on the proceeds of the cheque immediately, we are not representing that the cheque will be honoured.

You understand that:

- it is at your own risk if you draw down on the proceeds of a cheque before it is cleared;
- you can minimise your risk by asking us to arrange for a special clearance.

If the cheque is subsequently dishonoured:

- we will debit the account for the amount of the cheque
- if this overdraws the account, you are personally liable to pay back the amount overdrawn.

How to withdraw and transfer

You can make withdrawals and transfer from the account:

- by direct debit;
- via electronic banking including Osko Payments through internet banking, NPP Payments, electronic payment to a third-party supplier via direct debit;
- via BPAY to make a payment to a biller;
- by PayTo
- at selected ATMs, if your account is linked to a Visa Card; or
- via selected EFTPOS terminals, when you purchase goods using payWave or passcode (if you have a compatible digital wallet) and if your account is linked to a Visa Card (note that merchants may impose restrictions on withdrawing cash); or
- in any other manner we permit (if we do, we can set further terms and conditions for those withdrawals).

We will require acceptable proof of your authorisation for any withdrawal transactions.

Debiting transactions

We will debit transactions received on any one day in the order we determine in our absolute discretion.

Overdrawing an account

We do not provide you with any credit on your account. You must keep sufficient available funds in your accounts to cover all debit transactions. You must not make a withdrawal for an amount more than what you have in your account balance. Sometimes a withdrawal or a fee may cause your account balance to go into negative balance. When that happens, your account is "overdrawn". You must immediately put extra funds into your account to bring your account balance back into positive. We will charge you interest on the overdrawn amount. We calculate interest daily by applying the daily interest rate to the balance of cleared funds in your account at the end of the day. The daily interest rate is the relevant annual interest rate divided by 365. Interest will be debited to your account on or about the last day of each month.

You can find out our current interest rate using the Hiver app. We may, subject to giving you the appropriate prior notice, vary the interest rate at any time.

Available funds are the proceeds of:

- cheque deposits to your account (once the cheque is cleared)
- cash deposits and direct credits

Any outstanding card transactions are subtracted from the available balance.

Electronic credits

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

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

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

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

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

Where there are sufficient funds to cover the recalled amount, we will debit the account credited for the amount of the incorrect credit.

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

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

Direct debits

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

To cancel the DDR Service Agreement, you can contact either the remitter or us. You may contact us using the secure messages in Hiver app or internet banking, or by contacting us on 13 12 21.

If you contact us we will promptly take action to cancel the facility.

If you believe a direct debit initiated by a merchant or service provider is wrong you should contact us and we will promptly investigate. You may also try to contact the merchant or service provider to try to resolve the issue. If you give us the information we require we will forward your claim to the merchant or service provider. However, we are not liable to compensate you for the merchant or service provider's error.

If you set up the payment on your Visa 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, remitters will not be able to initiate a direct debit from your account under their DDR Service Agreement. Under the terms of their DDR Service Agreement, the remitter may charge you a fee for each dishonour of their direct debit request.

If you have authorised a remitter to debit your account as a direct debit and the remitter migrates the direct debit arrangement to PayTo, the direct debit arrangement will cease to be a direct debit arrangement and will instead be treated as a PayTo Payment Agreement (see section 23 of Division 2: Electronic Access Facilities and ePayments Conditions of Use for more information about PayTo and Migrated DDRs).

Other information

Transaction limits

Refer to our Fees and charges brochure on the Hiver app and our website for details.

Statements of Account

We will generally give you a statement of account at least every six months setting out all transactions relating to your account with us. However, we will not give you a statement of account or may give you statements of account less frequently where permitted under applicable law, the ePayments Code and for accounts that are dormant under the Customer Owned Banking Code of Practice.

For the purposes of the Customer Owned Banking Code of Practice, we treat your account as dormant if there have been no transactions on your account and the balance of your account is zero, over a six month statement period.

A statement of account includes all your deposit accounts and credit contracts, except credit card contracts.

We will notify you electronically (for example by email, SMS text message, message or notification in the Hiver app or internet banking) when we make a new statement of account available for you to access, view and download in internet banking.

You should check each statement of account using internet banking as soon as you receive it and immediately tell us of any entry in the statement which you dispute.

There is additional costs for print copy of statement of accounts. Please refer to our Fees and charges brochure for current details.

How we give you notices and other communications and documents

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

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

- by the Hiver app;
- by publishing it on our website and notifying you that it is available by email, SMS text message, secure messages or notification in the Hiver app or internet banking;
- by including it in or with a statement of account provided to you in the Hiver app or internet banking; or
- by national media advertisement.

Changing fees, charges, interest rates and these Conditions of Use

We may change fees and charges, interest rates and Conditions of Use. The table on page 12 below sets out how we will notify you of any change.

Change of name or address

If you change your name, phone, email, address or contact details you must let us know immediately. You may at any time update or change your email address or contact details in the Hiver app. Your details will be updated immediately on our system.

If you change your name, you will need to provide us with evidence of your name change in the form of a marriage or deed poll certificate. You will need to send us certified copy of the evidence. Your details will be updated on our system once we have processed the evidence you have provided to us.

Dormant accounts

If no transactions are carried out on your account for at least 12 months (other than transactions initiated by us, such as crediting interest or debiting fees and charges) you will receive a message or notification in the Hiver app or internet banking informing you that there has been no activity for the past 12 months on your account and setting out the steps you will need to take to withdraw or deposit funds to your account.

If you do not reply we will treat your account as dormant.

Once your account becomes dormant, we may 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 government as unclaimed money.

Blocking transactions and access to your account

We may suspend your right to perform transactions at any time without prior notice if we reasonably suspect that your account is being used or operated on in a fraudulent or improper manner or if we reasonably believe that suspension is necessary to protect the security or integrity of our systems or to prevent you or us suffering any loss or damage.

If any of these circumstances apply, we may also block access to your account.

We will not be liable to you or any other party on any basis for any decision we make in good faith under this provision

Account combination

If you have more than one account with us, we may apply the credit balance of any of your accounts to any other account of yours, the balance of which is:

- in debit and there is no approved credit limit; or
- in debit and is in excess of the approved credit limit; or
- a loan account or credit facility where default has occurred and the full amount owing under the loan or facility has become due and payable.

We may also combine your accounts (whether deposit or loan accounts) on termination of your membership.

We may do this so long as where combining accounts would not breach the Code of Operation for Centrelink Direct Credit Payments.

We may close all or any of your accounts after combination. We will give you written notice promptly after exercising any rights.

Closing an account and cancelling access facilities

By you:

You can close your account at any time, subject to the following conditions:

- If your account is in credit, we will pay the balance to you. You must return all physical access cards to us. We may withhold sufficient funds to cover payment of any pending or outstanding transactions, fees and charges;
- If your account is in debit, you must pay to us the outstanding balance, plus the amount of any pending or outstanding transactions, accrued interest and fees and charges before we will close your account;
- We may delay closure if there are any uncleared funds. Closure will be effected once we are satisfied that all funds are cleared;
- Please note that if any electronic transactions (an example is direct debits) are presented after the closure of your account, such items will be dishonoured.

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

You must always keep at least one Everyday account and one Saver Account open if you want to be a member of the Bank.

By us:

In addition to our rights of account combination, we may close your account and cancel your access facilities:

- in our absolute discretion by giving you 14 days' notice in writing;
- at any time without prior notice if we reasonably suspect your account is being used or operated on in illegal, fraudulent or improper manner or if we believe that closure is necessary to protect the security or integrity of our systems or to prevent you or us suffering any loss or damage.

After closure, we will pay you the credit balance of your account after deducting any outstanding fees and charges together with any other amounts to which we are entitled and being satisfied that there are no uncleared funds. We will not be liable to you or any person on any basis for a decision made by us in good faith to close an account and cancel access facilities.

Complaints

We have a dispute resolution system to deal with any complaints you may have win relation to your account and access facilities. 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.

Our external dispute resolution provider is the Australian Financial Complaints Authority (AFCA). AFCA provides fair and independent financial services complaint resolution that is free to consumers.

- Website: www.afca.org.au
- Email: info@afca.org.au
- Online complaints form: https://ocf.afca.org.au/
- Telephone: 1800 931 678 (free call)
- In writing: GPO Box 3 Melbourne, VIC 3001.

If you want to make a complaint, contact us using secure messages in Hiver app. 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 a dispute resolution guide available to you on request.

Summary of accounts and access facilities

Type of change	Minimum number of days notice	Method
Increasing any fee or charge	30 days	Electronically or by national media advertisement
Adding a new fee or charge	30 days	Electronically
Changing interest rates	Day of change	Electronically or by national media advertisement
Changing the method by which interest is calculated	20 days	Electronically
Changing the frequency with which interest is credited or debited	20 days	Electronically
Changing the minimum balance to which an account keeping fee applies or reducing the number of fee-free transactions permitted on the account	20 days	Electronically
Changing the balance ranges within which interest rates apply	20 days	Electronically
Increasing your liability for losses in relation to EFT transactions	20 days	Electronically
Imposing, removing or adjusting daily or periodic limits in relation to EFT transactions Note: If you do not want your daily limit on transactions via BPAY, Visa Card to be increased, you must notify us before the effective date of the change.	20 days	Electronically
Changing any other condition of use	Day of change	Electronically or by national media advertisement

Division 2: Electronic Access Facilities and ePayments Conditions of Use

Section 1

Information about our ePayment facilities

You should follow the guidelines in the box below to protect against unauthorised use of the Hiver app, internet banking; your access card and passcode. These guidelines provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised 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 or internet banking.
- If you change a passcode, do not select a passcode which represents your birth date or a recognisable part of your name.
- Never write the passcode on the access card.
- Never write the passcode on anything which is kept with or near the access card.
- Never lend the access card to anybody.
- Never tell or show the passcode to another person.
- Use care to prevent anyone seeing the passcode being entered on a device.
- Keep a record of the Visa Card number and the Visa Card Hotline telephone number for your area with your usual list of emergency phone numbers.
- Check your statements regularly for any unauthorised use.
- Immediately notify us when you change your address.
- ALWAYS access the electronic banking service only using the OFFICIAL Hiver apps, phone numbers and URL addresses.
- If accessing electronic banking on someone else's PC, laptop, tablet or mobile phone, ALWAYS DELETE your browsing history
- ALWAYS REJECT any request to provide or to confirm details of your passcode. We will NEVER ask you to provide us with these details.

If you fail to ensure the security of the Hiver app, your access card access facility and passcodes or you fail to promptly tell us about a security breach on your account you may increase your liability for unauthorised transactions.

These ePayment Conditions of Use govern all electronic transactions made using any one of our access cards

or facilities, listed below:

- Visa Card
- BPAY
- Electronic banking (Hiver app and Internet banking)

You can use any of these electronic access facilities to access an account, as listed in the *Summary of accounts and of access facilities*

We may impose limits on the amount that you can take out of your account, either by transaction or by time period.

Visa Card

Your 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 physical Visa Card. Your digital Visa Card is embedded into the Hiver app and is instantly available 24/7 with the Hiver app. You can use your digital Visa Card just like your physical Visa Card to shop online, pay bills, make in-app purchases and set up your recurring card payments or add it to your mobile wallet.

Visa Card also allows you to use an ATM to:

- check your account balances
- withdraw cash from your account
- transfer money between accounts

We may choose not to give you a Visa Card if your banking history with us is not satisfactory.

Contactless transactions using payWave

If your physical Visa Card has the payWave logo displayed on the card that means that your Visa Card is enabled to make contactless transactions at EFTPOS terminals. You do not need to swipe and enter your PIN or sign your name to perform transactions. You can simply tap your Visa Card on the EFTPOS terminal. You can still use your PIN if you do not wish to use payWave to transact. Before tapping your Visa Card on the EFTPOS terminal, you should check that the transaction details are correct, in particular the transaction amount on the EFTPOS terminal. You should never hand over your Visa Card to the merchant.

Mobile wallets

We may allow your Visa Card to be used via a mobile wallet such as Apple Pay, Google Pay, Samsung Pay or any other mobile wallets that we may approve from time to time. A mobile wallet is a mobile application on a smartphone or wearable device that allows details of your Visa Card to be embedded within it such that it can be used in place of your physical Visa Card at EFTPOS terminals.

You should read and understand the terms and conditions governing the use of the mobile wallet issued by the mobile wallet provider and your telecommunications provider. You will be bound by those terms when you use the mobile wallet. We are not the mobile wallet provider and we are not liable for the use of the mobile wallet.

You can find the terms and conditions governing the mobile wallet on our website.

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

Important information about disputed transactions for Visa Cards

If you believe a Visa Card transaction was:

- **unauthorised;**
- **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 dispute and seek a reversal of the transaction (sometimes referred to as a "chargeback"), by reversing the payment to the merchant's financial institution. However, we can only do so if you inform us of the disputed transaction within the timeframe determined by Visa.

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

It is important to inform us as soon as possible if you become aware of circumstances which might entitle you to a reversal of a transaction and provide us with sufficient information we reasonably ask for.

Section 2

Definitions

a) **access card** means an ATM card, debit card or credit card and includes our Visa Card in digital or physical form.

b) **ATM** means automatic teller machine

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

d) **Cut Off Time** means 5pm in New South Wales

e) **device** means a device, including and access card, we give to a user that is used to perform a transaction. Examples include:

   i) ATM card

   ii) debit card or credit card

   iii) token issued by us that generates a passcode

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

g) **electronic banking** includes internet banking, mobile banking app, the Hiver app and PayTo.

h) **facility** means an arrangement through which you can perform transactions

i) **Fast Payment** means an NPP Payment that is not an Osko Payment

j) **identifier** means information that a user:

   i) knows but is not required to keep secret, and

   ii) must provide to perform a transaction

   Examples include an account number or member number.

k) **Mandate Management Service (MMS)** means the Mandate Management Service being a central, secure database of Payment Agreements operated by NPP Australia Limited.

l) **manual signature** means a handwritten signature, including a signature written

on paper and a signature written on an electronic tablet

m) **Migrated DDR** means a Payment Agreement created by a Merchant or Payment Initiator to process payments under an existing direct debit arrangement as PayTo Payments instead of through the direct debit system – see the 'Migration of direct debits' clause below

n) **Mistaken Payment** has the meaning provided in section 9 (Mistaken Payments)

o) **Merchant** means a merchant with which you have established, or would like to establish, a Payment Agreement.

p) **NPP** means the New Payments Platform operated by or on behalf of NPP Australia Ltd

q) **NPP Payment** means a payment settled and cleared through the NPP and includes Fast Payments, Osko Payments and PayTo Payments

r) **Osko** means the 'Osko' payment service operated by BPAY Pty Ltd

s) **Osko Payment** means a payment made using Osko

t) **passcode** means a password or code that the user must keep secret, that may be required to authenticate a transaction or user. A passcode may consist of numbers, letters, a combination of both, or a phrase. Examples include:

i) personal identification number (PIN)

ii) electronic banking password

iii) code generated by a security token.

iv) pattern

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

u) **PayID** means a PayID which has been created in the PayID service component of the NPP.

v) **PayID Name** means the PayID Name that is recorded in the PayID service component of the NPP for a PayID.

w) **PayTo Agreement** or **Payment Agreement** means an agreement created by an approved Merchant or Payment Initiator in the Mandate Management Service by which you authorise us to make payments from your account or a Migrated DDR.

x) **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.

y) **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.

z) **PayTo Payment** means an NPP Payment we make pursuant to a Payment Agreement.

aa) **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 Visa Card at predetermined intervals (e.g. monthly or quarterly) or at intervals agreed by you. The amount may differ or be the same for each transaction.

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

cc) **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.

dd) **unauthorised** transaction means a transaction that is not authorised by a user

ee) **user** means you or an individual you have authorised to perform transactions on your account including a person you authorise us to issue an to issue an additional card to

ff) **we, us**, or **our** means Teachers Mutual Bank Limited

gg) **you** means the person or persons in whose name an Account and access facility is held and, where the context permits, a user.

Section 3

Biometric identifier

If you enable a biometric identifier such as fingerprint or face identifier login in the Hiver app settings, we may permit you to login into Hiver app using the registered biometric identifier on that device. You can still login to the Hiver app using the passcode that is registered to your account.

When you log into the Hiver app using your biometric identifier, you instruct us to perform any transactions requested during the Hiver app session.

WARNING: If you enable the biometric identifier login option, then any of the biometric identifiers stored on your device can be used to log into the Hiver app. You must ensure that only your biometric identifier (and not any other persons) is stored on the mobile device To access the Hiver app. We strongly recommend that all times you should use your passcode to access the Hiver app.

Accounts and transactions

3.1 These ePayment Conditions of Use apply to payment, funds transfer and cash withdrawal transactions that are:

a) initiated using electronic equipment, and

b) not intended to be authenticated by comparing a manual signature with a specimen signature.

3.2 These ePayment Conditions of Use apply to the following transactions:

a) all transactions using the Hiver app or internet banking;

b) access card transactions, including ATM, EFTPOS, credit card and debit card transactions performed by digital or physical card that are not intended to be authenticated by comparing a manual signature with a specimen signature;

c) electronic banking transactions and bill payment transactions

d) online transactions performed using a card number and expiry date

e) online bill payments (including BPAY)

f) direct debits.

Section 4

When you are not liable for loss

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

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

b) a device, identifier or passcode which is forged, faulty, expired or cancelled

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

d) a transaction being incorrectly debited more than once to the same facility

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

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

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

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

a) there is a presumption that the user did not receive it, unless we can prove that the user did receive it

b) we can prove that a user received a device or passcode by obtaining an acknowledgment of receipt from the user

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

Section 5

When you are liable for loss

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

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

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

b) you are not liable for the portion of losses:

i) incurred on any one day that exceeds any applicable daily transaction limit

ii) incurred in any period that exceeds any applicable periodic transaction limit

iii) that exceeds the balance on the facility, including any pre-arranged credit

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

5.3 Where:

a) more than one passcode is required to perform a transaction; and

b) we prove that a user breached the passcode security requirements in Section 6 for one or more of the required passcodes, but not all of the required passcodes you are liable under clause 5.2 only if we also prove on the balance of probability that the breach of the passcode security requirements under Section 6 was more than 50% responsible for the losses, when assessed together with all the contributing causes.

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

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

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

a) are liable for the actual losses that occur between:

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

ii) when the security compromise was reported to us

b) are not liable for any portion of the losses:

i) incurred on any one day that exceeds any applicable daily transaction limit

ii) incurred in any period that exceeds any applicable periodic transaction limit

iii) that exceeds the balance on the facility, including any pre-arranged credit

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

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

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

a) $150, or a lower figure determined by us

b) the balance of the facility or facilities which we and you have agreed can be accessed using the device and/or passcode, including any prearranged credit

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

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

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

b) the fact that a facility has been accessed with the correct device and/or passcode, while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the passcode security requirements in Section 6

c) the use or security of any information required to perform a transaction that is not required to be kept secret by users (for example, the number and expiry date of a device) is not relevant to a user's liability.

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

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

Section 6

Passcode security requirements

6.1 Section 6 applies where one or more passcodes are needed to perform a transaction.

6.2 A user must not:

a) voluntarily disclose one or more passcodes to anyone, including a family member or friend

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

i) carried with a device

ii) liable to loss or theft simultaneously with a device unless the user makes a reasonable attempt to protect the security of the passcode

c) where a device is not needed to perform a transaction, keep a written record of all passcodes required to perform transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the passcode(s).

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

a) hiding or disguising the passcode record among other records

b) hiding or disguising the passcode record in a place where a passcode

record would not be expected to be found

c) keeping a record of the passcode record in a securely locked container

d) preventing unauthorised access to an electronically stored record of the passcode record.

This list is not exhaustive.

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

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

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

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

a) specifically instructed the user not to do so

b) warned the user of the consequences of doing so.

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

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

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

Section 7

Liability for loss caused by system or equipment malfunction

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

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

a) correcting any errors

b) refunding any fees or charges imposed on the user.

Section 8

Network arrangements

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

a) we are a party to a shared electronic payments network

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

8.2 We must not require you to:

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

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

Section 9

Mistaken internet payments

9.1 In this Section 9:

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

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

- through a 'PayAnyone' internet banking facility and processed by an ADI which has subscribed to the ePayments Code through direct entry where funds are paid into the account of an unintended recipient because the user enters or selects a Bank/ State/ Branch (BSB) number and/ or identifier that does not belong to the named and/or intended recipient as a result of the user's error or the user being advised of the wrong BSB number and/or identifier; or
- that is an NPP Payment which, as a result of the user's error, is directed to the wrong account.

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

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

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

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

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, after receipt 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.
- After receipt 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.

- After receipt 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 after receipt to the sending ADI, and
  b) after receipt, 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).

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

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

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

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

a) are not satisfied that a mistaken internet payment has occurred
b) have not complied with the processes and timeframes set out in clauses 9.2-9.5, or as described in the box below.

9.7 When we receive a complaint under clause 9.6 we must:

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

9.8. If you are not satisfied with the outcome of a complaint, you are able to complain to 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.

Section 10

Using electronic banking

10.1 We do not warrant that:

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

b) you will have 24 hours a day, 7 days per week, access to electronic banking.

c) data you transmit via electronic banking is totally secure.

External transfers

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

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

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

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

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

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

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

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

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

10.7 Subject to the events described in Clause 10.21, we will immediately debit the amount of a transfer and any applicable fees to your nominated account when we accept your transfer instruction.

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

Processing of External Transfers

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

Osko Payments

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

10.11 Subject to the events described in Clause 10.21, where we process a transfer as an Osko Payment, we will process the transfer immediately and the funds will usually be available to the payee immediately.

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

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

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

Fast Payments

10.15 Where we cannot process a transfer as an Osko Payment, we may still be able to process as a Fast Payment, if the financial institution at which the recipient account is held is able to receive NPP Payments.

10.16 Subject to the events described in Clause 10.21, where we process a transfer as a Fast Payment, we will process the transfer immediately and the funds will be available to the recipient as soon as the recipient's financial institution makes them available.

10.17 Where possible, we may show you in internet banking if a transfer we have processed as a Fast Payment is successful or fails.

Other transfers

10.18 Where we do not send a transfer as an Osko Payment or a Fast Payment we will send it as a standard transfer.

10.19 Where we process a transfer as a standard transfer:

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

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

Delays

10.21 Delays may occur in processing transfers where:

- we experience a services disruption or systems outage which prevents us or our service providers from processing transfers;
- we are required to delay processing a transfer to comply with any applicable laws (including any laws in relation to anti-money laundering and sanctions);
- you fail to comply with any of your obligations under any relevant terms and conditions;
- the financial institution at which the recipient account is held or the recipient fails to comply with their obligations or is experiencing a services disruption which prevents them from processing transfers;
- the financial institution at which the recipient account is held decides to delay processing; or
- we delay processing to investigate and review the transfer instruction

to ensure it is not fraudulent, illegal or improper or to confirm that it has been properly authorised by you.

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

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

Suspension of the transfers

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

Transaction limits

10.24 We may decline any transfer request or instruction from you where accepting it would cause you to exceed any applicable transaction or period limit we have imposed. Please refer to the Fees and charges brochure for details of current transaction limits.

Failed transfers

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

Mistakes and Issues with transfers

10.26 If you make a transfer and later discover that:

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

10.27 You should notify us immediately if you think that:

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

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

10.28 See section 9 for information about how Mistaken Internet Payments will be dealt with.

10.29 Where we consider it appropriate and we are reasonably able to do so, we may request that the financial institution to whom the funds were transferred returns the funds to us,

on your behalf. However, depending on the circumstances, the financial institution may not return the funds to us unless the recipient consents.

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

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

Refunds and chargebacks

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

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

10.34 No "chargeback" rights are available in relation to funds transferred by electronic banking, even if the transfer has been made from a credit card account or another account with an access card linked to it.

Section 11

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

11.1 If you believe your access card has been misused, lost or stolen or the passcode has become known to someone else, you must immediately contact us using secure messages in Hiver app during business hours or the access card Hotline at any time.

Please refer to How to contact us on the back page of these Conditions of use.

11.2 We will acknowledge your notification by using secure messages in Hiver app to give you a reference number that verifies the date and time you contacted us, Please retain this reference number.

11.3 The access card Hotline is available 24 hours a day, 7 days a week.

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

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

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

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

Visa Card Hotline

Within Australia
13 12 21

Outside Australia
+1303 967 1090

Section 12

How to report unauthorised use of electronic banking

12.1 If you believe that your passcodes for electronic banking transactions have been misused, lost or stolen, or, where relevant, your passcode has become known to someone else, you must use secure messages in Hiver app to inform us immediately.

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

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

Section 13

Using the access card

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

13.2 We will use secure messages in Hiver app to advise you from time to time:

a) what transactions may be performed using the access card;

b) what ATMs of other financial institutions may be used; and

c) what the daily cash withdrawal limits are.

Please refer to the Fees and charges brochure for details of current transaction limits.

13.3 You may only use your access card to perform transactions on those accounts we permit. We will use secure messages in Hiver app to advise you of the accounts which you may use your access card to access.

13.4 The access card always remains our property.

Section 14

Using VISA for foreign currency transactions

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

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

14.3 All transactions made in a foreign currency (irrespective of where the transaction occurs) on the Visa Card are subject to a currency conversion fee payable to Cuscal Limited as the principal member of Visa Worldwide under which we provide you with the Visa Card. Please refer to the Fees and charges brochure for the current currency conversion fee.

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

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

Please also note: "transaction" includes any transaction in a foreign currency whether in Australia or overseas, such as purchasing goods or services at VISA outlets, making ATM withdrawals and payments via electronic banking.

Section 15

Use after cancellation or expiry of access card

15.1 You must not use your access card:

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

b) after the access card has been cancelled.

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

Section 16

Exclusions of access card warranties and representations

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

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

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

Section 17

Cancellation of access card or of access to electronic banking service or BPAY

17.1 You may cancel your access card, your access to electronic banking or BPAY at any time by using secure messages in Hiver app to give us written notice.

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

17.3 We may cancel your access card or your access to electronic banking or BPAY for any reason by using the Hiver app to give you 30 days' notice. The notice does not have to specify the reasons for cancellation.

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

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

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

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

b) you close the last of your accounts with us to which the access card applies or which has electronic banking or BPAY access;

c) you cease to be our member; or

d) you alter the authorities governing the use of your account or accounts to which the access card applies or which has electronic banking or BPAY access (unless we agree otherwise).

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

Section 18

Using BPAY Payments facility ("BPAY")

18.1 With electronic banking you can use BPAY to pay bills bearing the BPAY logo from those accounts that have the BPAY facility.

18.2 When you tell us to make a BPAY payment you must tell us the biller's code number (found on your bill), your Customer Reference Number (e.g.

your account number with the biller), the amount to be paid and the account from which the amount is to be paid.

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

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

Section 19

Processing BPAY payments

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

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

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

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

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

19.2 A BPAY payment instruction is irrevocable.

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

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

19.5 You should use the Hiver app to 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 use the Hiver app to provide us with written consent addressed to the biller who received that BPAY *payment. If you do not give us that consent, the biller may not be permitted under law to disclose to us the information we need to investigate or rectify that* BPAY *payment.*

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

a) on the date you direct us to make it, if we receive your direction by the Cut Off Time on a banking business day;

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

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

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

a) there is a public or bank holiday on the day after you use secure messages in Hiver app to instruct us to make the BPAY payment;

b) you use secure messages in Hiver app to tell us to make a BPAY payment on a day which is not a banking business day or after the Cut Off Time on a banking business day; or

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

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

a) use secure messages in Hiver app to advise you of this;

b) credit your account with the amount of the BPAY payment; and

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

19.9 You must be careful to ensure you use the Hiver app to tell us the correct amount you wish to pay. If you make a

BPAY payment and later discover that:

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

b) the amount you paid was less than the amount you needed to pay you BPAY payment for the difference between the amount you actually paid and the amount you needed to pay.

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

Section 20

Future-dated BPAY payments

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

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

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

b) If there are insufficient cleared funds or, as relevant, insufficient available credit, the BPAY payment will not be made.

c) You are responsible for checking your account transaction details or account statement to ensure the future-dated payment is made correctly.

d) You should use secure messages in Hiver app to contact us if there are any problems with your future-dated payment.

e) You must use secure messages in Hiver app to contact us if you wish to cancel a future-dated payment after you have given the direction but before the date for payment. You cannot stop the BPAY payment on or after that date.

Section 21

Consequential damage for BPAY payments

21.1 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.

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

Section 22

Regular payment arrangements

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

22.2 To change or cancel any regular payment arrangement you should contact the merchant or use secure messages in Hiver app to contact us at least 15 days prior to the next scheduled payment. If possible you should retain a copy of this change/ cancellation request.

22.3 Should your card details be changed (for example if your Visa Card was lost, stolen or expired and has been replaced) then you must request the merchant to change the details of your existing regular payment arrangement to ensure payments under that arrangement continue. If you fail to do so your regular payment

arrangement may not be honoured, or the merchant may stop providing the goods and/or services.

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

Section 23

PayTo

23.1 This section 23 applies in relation to your use or attempted use of PayTo and any Payment Agreement that is created for an account, and related PayTo Payments, if PayTo is available for your account, when we begin to offer PayTo. See the Summary of accounts and access facilities to determine whether PayTo is available for your account.

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

23.3 We will send certain PayTo notifications by email and/or SMS text message so you should ensure you have given us your current email address and mobile phone number and promptly tell us if they change. If we do not have a current email address or mobile phone number you will not receive some PayTo notifications from us.

Creating a Payment Agreement

23.4 You can set up a Payment Agreement with a Merchant or Payment Initiator that offers PayTo as a payment option by providing the Merchant or Payment Initiator with a PayID you have created for your account or the account's BSB and account number (being either the unique account number or your member number together with your account code e.g. S1). You are responsible for ensuring that the PayID or BSB and account number you provide for the purpose of establishing a Payment Agreement are correct. Any personal information or data you provide to a Merchant or Payment Initiator will be subject to the privacy policy and terms and conditions of the relevant Merchant or Payment Initiator.

23.5 You should not set up a Payment Agreement with a Merchant or Payment Initiator using only your BSB and member number without the unique account code (e.g. S1). If you do, we will reject the Payment Agreement.

23.6 If you agree to setup a Payment Agreement with a Merchant or Payment Initiator, they will create the Payment Agreement in the Mandate Management Service through their financial institution or payments processor and we will be notified.

23.7 After we receive notification that a new Payment Agreement has been created for your account, we will notify you with the details of the Payment Agreement by SMS text message and/or email and ask you to confirm your approval of the Payment Agreement through internet banking. If you do not have internet banking, you can contact us by telephone to approve or decline the Payment Agreement. You may approve or decline any Payment Agreement at your discretion and we will record whether you approved or declined the Payment Agreement in the Mandate Management Service.

23.8 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 or it may expire.

23.9 If you tell us that you approve a Payment Agreement it will be active once we record your approval in the Mandate Management Service. Payment requests may be made by a Merchant or Payment Initiator immediately after you have approved a Payment Agreement so do not approve a Payment Agreement unless you are sure all the details are correct.

23.10 If you think the payment amount, frequency or any other detail presented in a Payment Agreement is incorrect, you should decline the Payment Agreement and contact the relevant Merchant or Payment Initiator to have them resubmit a new Payment Agreement with the correct details.

23.11 By approving a Payment Agreement, you:

a) authorise us to collect, use and store your name and account details and other details about you and the Payment Agreement from and in the Mandate Management Service; and

b) acknowledge that these details may be disclosed to NPP Australia Limited (who operates the Mandate Management Service) and the financial institution or payment processor for the Merchant or Payment Initiator for the purposes of creating payment instructions and constructing NPP Payment messages, enabling us to make PayTo Payments from your account and for related purposes; and

c) consent to us, other financial institutions and payment processors, NPP Australia Limited, Merchants and Payment Initiators using and disclosing such of your personal information as is contained in a Payment Agreement record in the Mandate Management Service as contemplated by the NPP regulations and procedures.

PayTo Payments

23.12 We will process payment instructions we receive from a Merchant or Payment Initiator in connection with a Payment Agreement only if you have approved the associated Payment Agreement.

23.13 By authorising a Payment Agreement you instruct us to make PayTo Payments from your relevant account in accordance with the Payment Agreement each time a PayTo Payment is requested by the Merchant or Payment Initiator who is a party to the Payment Agreement or their financial institution or payment processor.

23.14 It is your responsibility to ensure you have sufficient funds in your account to process each PayTo Payment. We are not required to make a PayTo Payment if there are insufficient cleared funds in your account at the time the PayTo Payment is requested (see the 'Overdrawing an account' section for more information).

Amending a Payment Agreement

23.15 A Payment Agreement may be amended by the Merchant or Payment Initiator from time to time.

23.16 If we are notified that a Merchant or Payment Initiator seeks to amend a Payment Agreement and that amendment requires your approval we will notify you of the amendment request by SMS text message and/or email and request that you approve or decline the amendment. You may approve or decline an amendment request presented for your approval through internet banking. If you do not have internet banking, you can contact us by telephone to confirm or decline the amendment request.

23.17 We will promptly record whether you approved or declined the Payment Agreement amendment request in the Mandate Management Service. If you tell us that you approve an amendment request the amendment will be active once we record your approval in the Mandate Management Service. If you decline a Payment Agreement amendment request, the Payment Agreement will not be affected by the amendment request and will continue as if the amendment request had not been submitted.

23.18 If you think the payment amount, frequency or any other detail presented in a Payment Agreement amendment request we provide to you for approval is incorrect, you should decline the amendment request and contact the relevant Merchant or Payment Initiator to have them resubmit a new amendment

request with the correct details. We cannot change the details in an amendment request.

23.19 If a Payment Agreement amendment request requires your approval within a timeframe stipulated by the Merchant or Payment Initiator, or NPP, and you do not provide approval within that timeframe, the Payment Agreement amendment may expire and it will be treated as being declined by you.

23.20 You may instruct us to amend your name, PayID or BSB and account details in a Payment Agreement. You can also amend your PayID or BSB and account details in a Payment Agreement through internet banking. Account details may only be replaced with a PayID or BSB and account number of an eligible account you hold with us. If you wish to amend the account details to refer to an account with another financial institution, you must cancel the Payment Agreement and contact the Merchant or Payment Initiator to create a new Payment Agreement with the new account details. 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 detail of the Merchant or Payment Initiator, or another party.

Pausing or resuming a Payment Agreement

23.21 You can pause and resume a Payment Agreement, or resume a paused Payment Agreement, through internet banking or by contacting us by telephone. We will promptly act on your instruction to pause or resume a Payment Agreement by updating the Mandate Management Service. The Merchant or Payment Initiator who is a party to the Payment Agreement will be notified each time you pause or resume a Payment Agreement.

23.22 A Payment Agreement may also be paused or resumed by the relevant Merchant or Payment Initiator. We will notify you each time we are notified that a Payment Agreement is paused or resumed by the Merchant or Payment Initiator.

23.23 We may also pause any Payment Agreement that has been setup using a PayID if the PayID is locked or closed. If we do, we will resume the Payment Agreement once the PayID is unlocked or we obtain instructions from you that otherwise enable the Payment Agreement to be resumed (unless the Payment Agreement has since been cancelled). We will notify you if we pause or resume a Payment Agreement and the Merchant or Payment Initiator associated with the Payment Agreement will also be notified each time we pause or resume a Payment Agreement.

23.24 While a Payment Agreement is paused, we will not process any PayTo Payment requests we receive pursuant to the Payment Agreement. PayTo Payments will resume once a paused Payment Agreement is resumed.

23.25 Although pausing a Payment Agreement will stop related PayTo Payments being made from your account, doing so may breach the terms of your agreement with the relevant Merchant or Payment Initiator or you may be required to make payment in some other way. We suggest that you ensure you understand the consequences of pausing a Payment Agreement before you do so and, if necessary, contact the relevant Merchant or Payment Initiator.

Transferring a Payment Agreement

23.26 It is not currently possible to transfer a Payment Agreement between accounts with us and accounts with another financial institution. If you want to change a Payment Agreement to an account with another financial institution, you must contact the Merchant or Payment Initiator to create a new Payment Agreement with the new account details.

Cancelling a Payment Agreement

23.27 You can cancel a Payment Agreement at any time through internet banking or by contacting us by telephone. We will promptly act on your instruction to cancel a Payment Agreement by updating the Mandate Management Service. The Merchant or Payment Initiator associated with your Payment Agreement will then be notified that you have cancelled the Payment Agreement.

23.28 A Payment Agreement may also be cancelled by the relevant Merchant or Payment Initiator. We will notify you through internet banking if we are notified that a Payment Agreement is cancelled by the Merchant or Payment Initiator.

23.29 We will not process any PayTo Payment requests we receive from the Merchant or Payment Initiator pursuant to a Payment Agreement after it has been cancelled.

23.30 Although cancelling a Payment Agreement will stop related PayTo Payments being made from your account, doing so may breach the terms of your agreement with the relevant Merchant or Payment Initiator or you may be required to make payment in some other way. We suggest that you ensure you understand the consequences of cancelling a Payment Agreement before you do so and, if necessary, contact the relevant Merchant or Payment Initiator.

Migration of direct debits

23.31 If you have an existing direct debit arrangement with a Merchant or a Payment Initiator, the Merchant or Payment Initiator may choose to create a Payment Agreement for the direct debit arrangement to process payments as PayTo Payments instead of as direct debit payments.

23.32 If a Merchant or a Payment Initiator does this, you will be notified by them that your future payments will be processed from your account through PayTo and you will then have the option of telling the Merchant or Payment Initiator that you do not consent.

23.33 If you do not advise the Merchant or Payment Initiator that you do not consent to your direct debit arrangement being migrated to PayTo, the Merchant or Payment Initiator may create a Migrated DDR Payment Agreement in the Mandate Management Service that reflects the terms of your direct debit service agreement and the Payment Agreement will be deemed to have been approved by you. We will not seek your approval of a Payment Agreement that relates to a Migrated DDR.

23.34 Once the Migrated DDR Payment Agreement has been created by the Merchant or Payment Initiator, you and the Merchant or Payment Initiator will be able to amend, pause and resume and cancel the Payment Agreement in the same way as any other Payment Agreement as set out above.

23.35 If a direct debit arrangement you have set up using only your member number (instead of either your unique account number or your member number together with your account code e.g. S1) is migrated to PayTo as a Migrated DDR, we will allocate it to any of your accounts that allow PayTo in our discretion and the account the Migrated DDR is set up for may be different than the account the direct debit arrangement was previously set up for. Where this is the case we may change the account we have allocated the Migrated DDR to in our discretion from time to time unless you have instructed us to change it to a specific account number (see 'Amending a Payment Agreement' above for information about how you can amend the account details in Payment Agreements).

23.36 By permitting the creation of a Payment Agreement for a direct

debit arrangement (by not contacting the Merchant or Payment Initiator and telling them that you do not consent), you:

a) authorise us to collect, use and store your name and account details and other details about you and the Payment Agreement from and in the PayTo Service;

b) acknowledge that these details may be disclosed to NPP Australia (who operates the PayTo Service) and the financial institution or payment processor for the Merchant or Payment Initiator for the purposes of creating payment instructions and constructing NPP Payment messages, enabling us to make PayTo Payments from your account and for related purposes; and

c) consent to us, other financial institutions and payment processors, NPP Australia Limited, Merchants and Payment Initiators using and disclosing such of your personal information as is contained in a Payment Agreement record in the PayTo Service as contemplated by the NPP regulations and procedures.

General PayTo obligations

23.37 We will accurately reflect all information you provide to us in connection with a Payment Agreement in the Mandate Management Service.

23.38 You must:

a) ensure that you carefully consider any Payment Agreement creation request or amendment request made in respect of your Payment Agreement and promptly respond to such requests;

b) ensure that all information and data you provide to us or to any Merchant or Payment Initiator that is authorised to use PayTo is accurate and up-to-date;

c) not use PayTo to send threatening, harassing or offensive messages to a Merchant, Payment Initiator or any other person;

d) where we allow you to provide a payment description or reference in connection with a Payment Agreement you must ensure that it does not contain, refer to or link to:

i) any swearing, profanity or offensive, discriminatory, threatening or abusive content;

ii) any information that is confidential or must be kept secret;

iii) sensitive personal information of any person (including information or an opinion about a person's racial or ethnic origin, political opinions or membership of a political association, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practices, criminal record and health information);

iv) anything which infringes the intellectual property rights of any person; or

iv) anything which is illegal or seeks to promote illegal activity;

e) comply with all applicable laws in connection with your use of PayTo;

f) promptly consider, action and respond to any Payment Agreement creation request, amendment request or other notification we send you;

g) immediately notify us if you no longer hold or have authority to operate the account from which payments under a Payment Agreement you have approved or permitted to be created are being or are to be made;

h) promptly notify us if you receive a Payment Agreement creation request or amendment request or become aware of PayTo Payments being processed from your account that you are not expecting, or experience any other activities that appear suspicious, fraudulent or erroneous;

i) promptly notify us if you become aware of a PayTo Payment being made from your account that is not permitted under the terms of your Payment Agreement or that was not approved by you; and

j) comply with any direction we give you where doing so is necessary for us to comply with our obligations relating to PayTo including under the NPP regulations and procedures.

23.39 You are responsible for complying with the terms of any agreement that you have with the Merchant or Payment Initiator who is a party to a Payment Agreement (including any payment and notice giving obligations or termination requirements) and for dealing with the Merchant or Payment Initiator in relation to any concerns or complaints you have in relation to any goods or services relating to the Payment Agreement.

23.40 From time to time, we may request that you confirm that one or more of your Payment Agreements are accurate and up-to-date. You must promptly action and respond to any such request. If you fail to do so, we may pause the relevant Payment Agreement(s).

23.41 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 if we pause or cancel a Payment Agreement for these purposes but only if we are legally permitted to do so. 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.

23.42 If you notify us of a PayTo Payment being made from your account that is not permitted under the terms of your Payment Agreement or that was not approved by you and submit a claim, we will acknowledge your claim within 1 business day and provide a formal response to your claim within 30 business days. If the claim is founded, we will refund the PayTo Payment to your account.

Liability for PayTo

23.43 To the maximum extent permitted by law, we will not be liable to you or any other person for any loss suffered as a result of:

a) processing PayTo Payments under a Payment Agreement which you have approved or are deemed to have approved;

b) you failing to properly consider or promptly respond to any Payment Agreement creation request or amendment request we send you;

c) you failing to properly consider and action any notification we send you in relation to any Payment Agreement;

d) you or a Merchant or Payment Initiator pausing, resuming or cancelling a Payment Agreement; or

e) any delay or failure in respect of a Payment Agreement or a PayTo Payment being processed due to the unavailability or failure of the PayTo Service,

except to the extent such loss is caused by us failing to comply with our obligations relating to PayTo under these terms and conditions.

About The Customer Owned Banking Code of Practice

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

Our promises to you are:

1. We will 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 from our website.

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

Customer Owned Banking Code Compliance Committee

PO Box 14240

Melbourne VIC 8001

Phone: 1800 367 287

Fax: 03 9613 7481

Email: info@codecompliance.org.au **Web:** www.cobccc.org.au

The Code Compliance Committee (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 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. If you are not satisfied with our response, you can contact our external dispute resolution provider, the Australian Financial Complaints Authority (AFCA), directly. AFCA provides fair and independent financial services complaint resolution that is free to consumers.

For the current contact details for AFCA please refer to our Complaints and dispute resolution brochure.

Website: www.afca.org.au **Email:** info@afca.org.au

Telephone: 1800 931 678 (free call) In writing: GPO Box 3 Melbourne, VIC 3001.

Hiver

Need more information we're here to help

You can contact us via:

- **the Hiver app (on a compatible iOS or Android device)**
- **telephone on 1800 044 837**
- **or overseas on +61 1800 044 837**
- **email on support@hiver.bank**

Card lost or stolen?

Head to the Hiver app to immediately update your card status to lost or stolen or block your card if you're seeing unauthorised charges on your account.

If for some reason you are unable to complete this in the Hiver app and for your protection give us a call on 1800 044 837 as soon as possible to let us report the loss, theft or unauthorised use of your card.

If you are outside Australia – please make sure you notify us before traveling overseas and for Visa Cards call +1303 967 1090 report your card as lost or stolen or if you're seeing unauthorised charges on your account.

Hiver Bank is a division of Teachers Mutual Bank Limited ABN 30 087 650 459
AFSL/Australian Credit Licence 238981

Effective 31 October 2022 I OP02172-OPS-HIVE-1022