



INFORMATION DOCUMENT

Conditions of Use

MoveBank Limited MoveBank
AFSL / Australian credit licence 234536
ABN: 91 087 651 090

Effective Date
30 January 2026

How to Contact Us



Website: movebank.com.au



Telephone: 1300 362 216



Postal Address: GPO Box 648, Brisbane QLD 4000



Email: info@movebank.com.au



In person: Visit us at our branch, see our web site for branch details including opening hours.

This document should be read in conjunction with our:

- Interest Rate Schedule
- Summary of Accounts and Access Facilities brochure
- Fees and Charges Schedule

Together these brochures form the conditions of use for the MoveBank Account and Access Facility.



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

▪ In Australia

Call the Visa card hotline on 1800 621 199. This service is available 24 hours a day, every day. Please also contact us to report the loss, theft or unauthorised use during business hours.

▪ Overseas

Please contact us before you travel overseas for the current Visa hotline arrangements.

To report a loss resulting from any other unauthorised use of an access facility, contact us directly.

Customer Owned Banking Code of Practice

We warrant that we will comply with the Customer Owned Banking Code of Practice. You can download a copy of the Customer Owned Banking Code of Practice at www.customerownedbanking.asn.au

ePayments Code

We warrant that we will comply with the ePayments Code.

How our Conditions Become Binding on You and How to Access Copies

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

Please keep these Conditions of Use in a safe place so you can refer to it when needed.

Alternatively, you can obtain information set out in this document and download this document by visiting our website at movebank.com.au.

Financial Claims Scheme

Under the Financial Claims Scheme (FCS) administered by APRA, the Australian Government has provided a guarantee of deposits held in regulated authorised deposit-taking institutions (ADIs) incorporated in Australia, subject to a limit for each account holder.

Depositors with MoveBank may be entitled to receive a payment from the FCS, subject to a limit per depositor. For further information about the FCS visit the website fcs.gov.au.

Table of Contents

How to Contact Us	1
Account Operations.....	5
What is the Account and Access Facility?	5
How do I open an account?	5
Proof of identity required	5
Opening an account	5
What fees and charges are there?.....	6
What interest can I earn on my account?.....	6
What are the taxation consequences?.....	6
Disclosing your tax file number (TFN).....	6
Foreign tax residency status.....	6
Joint accounts	7
Trust accounts.....	8
Third party access	8
Making deposits to the account	8
Deposits using electronic equipment.....	8
Depositing cheques.....	9
Withdrawing or transferring from the account	9
Debiting transactions generally	10
Conducting a Confirmation of Payee Lookup.....	10
Withdrawals using our corporate cheques	10
Transaction limits	11
Overdrawing an account.....	11
Sweep facility	11
Account statements.....	11
What happens if my details change?.....	12
Dormant accounts	12
Account combination	12
Closing accounts, cancelling access facilities & delaying, blocking, freezing or refusing transactions.....	12
Notifying changes	14
How We Send Notices & Statements	14
Direct Debits & Periodical Payments.....	15
Term Deposits	16
Electronic Access Facilities and ePayments Conditions of Use.....	17
Section 1. Information about ePayment Facilities	17
Section 2. Definitions	19

Section 3. Transactions	20
Section 4. When you are not liable for loss	20
Section 5. When you are liable for a loss	21
Section 6. Passcode security requirements	22
Section 7. Liability for Loss Caused by System or Equipment Malfunction	23
Section 8. Network Arrangements	23
Section 9. Mistaken Internet Payments.....	24
Section 10. Using Internet or Mobile Banking	26
Section 11. How to report loss, theft or unauthorised use of your access card or passcode ...	26
Complaints	40
Customer Owned Banking Code of Practice Compliance.....	40

Account Operations

What is the Account and Access Facility?

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

- Visa card
- BPAY®(registered to BPAY Pty Ltd ABN 69 079 137 518)
- Osko ® payments
- Internet and mobile banking
- ATM access
- Direct debit requests
- PayTo
- Periodical payments

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

How do I open an account?

You will need to become a member of MoveBank before we can issue an Account and Access Facility to you. To become a member you must be an Australian resident and meet other eligibility requirements.

To apply, you need to provide your:

- Full name
- Australian residential address
- Australian mobile phone number
- date of birth
- email address
- information that we require in order to determine your tax residency status, and
- any other details requested by us, including documents and information to verify your identity.

We may use a third-party provider to verify some or all of this information.

If you don't provide information we require within an acceptable time frame, we may place a stop on your account. We also reserve the right to refuse admission at our absolute discretion.

Proof of identity required

The law requires us to verify your identity when you open an account or when you become a signatory to an account.

In most cases we may verify your identity electronically using information provided. If electronic verification isn't available, you can prove your identity by supplying a government issued photo identify document such as a driver's licence or passport. If you do not have photo ID, please contact us to discuss what other forms of identification may be acceptable.

If you change your name, for example, upon marriage, you will need to give us a change of name statement. We will give you guidance on how to go about this.

Opening an account

Prior to opening an account, you should first check the Interest Rate Schedule and Summary of Accounts, Access Facilities and Transaction Limits brochure for the different account types available, any conditions that apply, and the features and benefits of each account type to ensure that it meets your needs.

When you open an account via internet banking, you may be able to deposit funds into the account immediately. You will not be able to transfer out of the account until we have contacted you to verify information provided to us including your account opening instructions. This is to help protect your accounts.

We reserve the right not to provide an account or related access facility at our absolute discretion.

What fees and charges are there?

We may debit your account with fees and charges as set out in our Fees and Charges Schedule along with any applicable government fees and charges.

We calculate and credit interest to your account as set out in the Interest Rate Schedule. We may vary fees or charges from time to time as set out under *Notifying Changes* on page 13.

For some accounts fees, charges and the interest rate received on accounts may vary based on activities within the account within the prior month. For these accounts, a “month” is taken to be from the first day of the calendar month until 5pm on the final day of the calendar month.

What interest can I earn on my account?

Full information on our current savings and term deposit interest rates is provided in our Interest Rates Schedule and it is also available on our website.

We calculate and credit interest to your account as set out in the Interest Rate Schedule. We may vary savings or term deposit interest rates from time to time. Interest rates on term deposits remain fixed for the agreed term of the deposit.

What are the taxation consequences?

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

Disclosing your tax file number (TFN)

When you apply for the Account and Access Facility, we will ask you for your tax file number or exemption.

We apply your tax file number to all accounts held with MoveBank when supplied, unless you instruct us not to do so.

You are not obliged to disclose your tax file number to us however, if you do not, we are obliged to deduct withholding tax from interest paid on the account at the highest marginal rate.

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

Children under 16 are exempt from tax earned on interest, provided they do not exceed the amount allowed by the Australian Tax Office (ATO). If the interest earned by a child exceeds the allowed limit, the child may need to supply a tax file number. Further details can be obtained from the ATO website.

For business accounts, you need only quote your ABN instead of a tax file number.

Foreign tax residency status

We are required by law to collect certain information about you in order to determine your Foreign Tax Residency Status, and where required, report that information, as well as information about any account you hold, to the ATO. The ATO is required to exchange that information with equivalent foreign country tax authorities.

If you believe that there has been a change to your Foreign Tax Residency Status, you need to let us know within 30 days.

We may require you to provide additional information including documentation and certifications. If you don't provide the information we reasonably require by the time we require it, we may seek information from a third party or place a stop on your account(s).

Joint accounts

A joint account is an account in the name of more than one person. The important legal consequences of holding a joint account are:

- the right of survivorship – when one joint holder dies, the surviving joint holders automatically take the deceased joint holder's interest in the account;
- joint and several liability – each joint holder is individually liable for the full amount owing on the joint account.

You can operate a joint account on a 'joint operation' or 'individual operation' basis:

- '**joint operation**' means all joint holders must authorise any withdrawal, payment, or transfer from the account;
- '**individual operation**' means any one joint holder can authorise any withdrawal, payment or transfer from the account.

By default, new joint accounts will be opened on an individual operation basis unless the joint holders instruct otherwise in the account opening process. The joint holders can jointly change account operating instructions in writing at any time.

However, irrespective of the joint account operating instructions, any one joint holder can instruct us to:

- change the account operation to joint operation by all joint holders only; or
- suspend the account to allow the joint holders time to reach agreement about dispersal of the account funds,

in which case these instructions will remain in effect until all joint holders agree otherwise.

We may also change the account operation to joint operation by all joint holders only, if we become aware of a dispute between the joint holders, or of the bankruptcy of any joint holder.

Please note that some access facilities (such as access cards) may not be available if the joint account operates on a joint operation basis.

Irrespective of the joint account operating instructions, all joint account holders will need to provide instructions to

- appoint a third-party signatory to the account
- request a transaction limit increase at MoveBank's discretion for large amount transfers

The above applies to joint personal accounts. For joint business accounts, such as partnership accounts, we may accept and rely on different account operating instructions. Please contact us for information about joint business accounts.

Should there be a dispute between joint account holders, MoveBank may restrict access to the account so that all parties must authorise transactions.

Trust accounts

You can open an account as a trust account, however:

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

Third party access

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

You are responsible for all transactions the signatory carries out on your account. You should ensure that the person you authorise to operate on your account is a person you trust fully.

For personal accounts, a signatory's authority is limited to:

- carrying out withdrawals, payments or transfers from the account;
- making enquiries about account balances and transactions on the account, including any debit balance or available credit on a transactional account.

For business accounts please contact us about applicable signatory options.

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

Making deposits to the account

You can make deposits to the account by:

- direct credit from your employer or external bank account. To arrange this you need to provide the MoveBank BSB (724-100) and your account number
- transfer from another financial institution
- transfer from another account with us
- via Bank@Post if you have a Visa card

unless otherwise indicated in the Summary of Accounts, Access Facilities and Transaction Limits brochure. Credits that are not the result of new money transferred to the account e.g. reversal of a transaction, are not considered deposits to the account.

Please note that we can reverse a direct credit if we do not receive full value for the direct credit.

Electronic deposits may not be processed on the same day. Please refer to ePayments Conditions of Use.

Deposits using electronic equipment

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

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

Depositing cheques

Cheque deposits are available exclusively via Bank@Post.

You can only access the proceeds of a cheque when it has cleared. All cheques are subject to clearance times regardless of the origin of the cheque however, you can ask us for a special clearance for which we may charge a fee.

Some cheques (such as overseas cheques) will take longer to clear. For full details of clearance times, please refer to our Summary of Accounts, Access Facilities and Transaction Limits brochure.

Cheques deposited to your account will be credited conditionally. If a cheque deposited is refused payment by the paying bank, your account will be debited, a fee may apply and accruing interest adjusted.

Bank@Post will only accept cheques for deposit to your account, in the following circumstances:

- Cheque payable to account holder

Bank@Post may accept a cheque into a joint account which is made payable to one of the account holders, however cheques payable to a joint account will not be accepted. Bank@Post do not accept cheques payable to a third party which have been endorsed to the account holder.

Stale cheques

A cheque may be deemed stale and refused by the paying bank where the date of the cheque is more than:

- 15 months old when drawn on an Australian bank
- 3 months old when drawn on an overseas bank

Withdrawing or transferring from the account

You can make withdrawals (including transfers) from the account:

- over the counter at our branch (cash facilities not available)
- by direct debit, PayTo or periodical payment
- via internet or mobile banking (including by Osko payment where available)
- via BPAY to make a payment to a biller
- at selected ATMs, if your account is linked to a Visa card
- via selected terminals, if your account is linked to a Visa card
- by mail to our office (transfer only – no cash withdrawals)
- via Bank@Post if your account is linked to a Visa card

unless otherwise indicated in the Summary of Accounts, Access Facilities and Transaction Limits brochure.

In the case of VISA transactions, merchants may impose restrictions on withdrawing cash.

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

Debiting transactions generally

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

We have the right to decline to accept your authorisation for any transaction if we are uncertain for any reason of the authenticity or validity of the authorisation or your legal capacity to give the authorisation. We may also delay or not process a transaction for any of the reasons set out in *Closing Accounts, Cancelling Access Facilities & Delaying, Blocking, Freezing or Refusing Transactions* on page 11. We will not be liable to you or any other person for any loss or damage which you or such other person may suffer as a result us reasonably exercising these rights.

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

Conducting a Confirmation of Payee Lookup

For a payment made to a BSB and account number, it is your responsibility to ensure the BSB and account number you want to pay to is correct. The Confirmation of Payee service may provide you with a view on the likelihood that the account name you enter matches the account. If the Confirmation of Payee service suggests details do not look right, you should only proceed if you have checked the account details with the intended recipient and you are confident that the account is legitimate.

If the Confirmation of Payee lookup service becomes unavailable due to outages, scheduled maintenance or other reasons we recommend you delay payments to BSB and account until the service is restored.

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

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

By using our accounts and access facilities, you acknowledge and authorise:

- (i) MoveBank to use and disclose your account details including Account Name in the Confirmation of Payee service; and
- (ii) Payers' financial institutions to use your account details for the purposes of the Confirmation of Payee service and prior to making payments to you.

To the extent your account details and the use of your account details constitutes disclosure, storage and use of your personal information within the meaning of the Privacy Law, you acknowledge and agree that you consent to that disclosure, storage and use.

In limited circumstances, you may elect to opt-out of the Confirmation of Payee or provide an alternative name for your account by contacting us through the MoveBank App or by emailing info@movebank.com.au

Notwithstanding the ability to opt-out of the service, you acknowledge and authorise us to confirm, disclose, store and use your Account details through the Confirmation of Payee service to government agencies for the purposes of making a payment to you by government agencies.

Withdrawals using our corporate cheques

Withdrawals via cheque are not available to our members.

Where MoveBank has rejected or terminated a member's membership in line with 'Closing accounts, cancelling access facilities & delaying, blocking, freezing or refusing transactions' and we are unable to confirm account details to transfer funds to, we may issue a cheque to the last known address of the member.

Transaction limits

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

These transaction limits are set out in the Summary of Accounts, Access Facilities and Transaction Limits brochure.

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

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

Overdrawing an account

You must keep sufficient cleared funds in your account to cover your direct debit, periodical payment, PayTo and EFT transactions. If you do not, we can dishonour the transaction and charge dishonour fees: see the Fees and Charges Schedule.

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

We may charge you:

- interest at our current overdraft rate, calculated on the daily closing balance
- an honour fee: see the Fees & Charges Schedule
- an ongoing fee if the account remains overdrawn for an extended period

If we honour a transaction by overdrawing your account, it does not mean that we have any obligation to do so in the future.

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

Sweep facility

A sweep is an automatic transfer of funds service available if you open more than one savings account. The sweep will transfer funds from a nominated account into another account to cover transactions which might otherwise overdraw your account.

We are not obliged to transfer funds if there are insufficient funds in the nominated account.

We will endeavour to effect sweep transfers in accordance with your instructions, however MoveBank will accept no responsibility from a failure to do so.

Account statements

We will send you account statements at least every 6 months. You can ask us for an account statement at any time. We may charge a fee for providing additional statements or copies.

In the case of joint account holders, a statement will be sent to the first named account holder only.

We may offer 'digital only' accounts, with statements provided electronically via internet or mobile banking only: see the Summary of Accounts & Access Facilities brochure. For all other accounts, statements will normally be provided electronically via internet or mobile banking unless:

- you request that statements be sent in paper form;
- you have not registered for internet banking access; or

- you have not provided us with an email address or mobile phone number we can use to notify you when the statements are available,

in which case we will provide paper statements and may charge you a fee: see the Fees and Charges brochure. We may provide paper statements in other circumstances.

We recommend that you check your account statement as soon as you receive it and immediately notify us of any unauthorised transactions or errors: see How to Contact Us on page 2.

What happens if my details change?

You must let us know immediately if you change any of your personal or contact details including your name, address, email address or mobile phone number. You can update your contact details via internet banking or by contacting us (see How to Contact Us on page 2).

Dormant accounts

If no deposits or withdrawals are carried out on your account for at least 12 months (other than transactions initiated by MoveBank, such as crediting interest or debiting fees and charges) we may write to you asking if you want to keep the account open. If you do not reply, or transact on the account, within 10 business days of the date of our notice to you, we may treat your account as dormant.

Once your account becomes dormant, we may:

- charge a dormancy fee
- stop paying interest or reduce the amount of interest
- cancel any attached access facilities
- close the account

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

Account combination

If you have more than one account with us, we may apply a deposit balance in any account to any other account in the same name, including joint accounts. This may happen if one of the accounts is overdrawn or to satisfy any other debt owing to MoveBank.

Where a duplicate membership is held with MoveBank, we may transfer all accounts and attached access facilities of the duplicate membership to one membership number. Unless you notify us of a preferred membership number, we can determine which membership number is to be retained.

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

If we combine accounts, we'll comply with the Code of Operation: Recovery of Debts from Customer Nominated Bank Accounts in receipt of Services Australia income support payments or Department of Veterans Affairs' payments and any successor Code (both when enforcing indebtedness owed to us and, to the extent the law permits, when facilitating enforcement by a third party judgment creditor).

We will give you written notice promptly after exercising any right to combine your accounts, this may include advice on your next statement.

Closing accounts, cancelling access facilities & delaying, blocking, freezing or refusing transactions

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

You will be responsible for any transactions that have been authorised by you prior to the account closure, such as regular Visa debits.

We can close the Account and Access Facility in our absolute discretion by giving you at least 14 days' notice.

However, without prior notice, we can close, or suspend your access to, any account, cancel any access facility, or delay, block, freeze or refuse any transaction:

- if we reasonably believe doing so will protect you or us from harm or loss;
- if we reasonably suspect fraudulent or illegal use of the account or access facility;
- if we reasonably suspect that a transaction may breach a law or sanction;
- to comply with our legal and regulatory obligations, including with our related policies and procedures; or
- if you fail to provide us with information or documents we reasonably request

Fraudulent or illegal use of the account

Where we reasonably believe account transactions relate to fraudulent or illegal use of the account or otherwise may breach a law or sanction and receive a request from another financial institution to return funds received into your account, we may return those funds or otherwise remove your access to them at our discretion and without notice.

Use of the account related to financial or domestic abuse and related inappropriate behaviour

We also may take action to close, or suspend your access to, any account, cancel any access facility, or delay, block, freeze or refuse any transaction or return funds where we reasonably believe that those accounts or transactions are being used to perpetrate financial, domestic or other forms of abuse.

We will act fairly and reasonably towards you when taking action against your accounts and transactions without prior notice.

If we close your account, we will pay you the net credit balance in the account unless we reasonably believe that our legal or regulatory obligations prevent us from doing so and subject to our right to combine accounts (see *Account Combination* on page 12).

Notifying changes

We may change fees, charges, interest rates and other conditions applicable to the Account & Access Facility at any time. We will act reasonably in making these changes and only do so for legitimate business purposes. If you do not like the change, you can ask us to close your Account and Access Facility, or close any account or cancel any access facility in it, in accordance with these Conditions of Use: see *Closing Accounts, Cancelling Access Facilities & Delaying, Blocking, Freezing or Refusing Transactions* on page 12.

The following table sets out when we will notify you of any change:

Type of change	Minimum Notice
Increasing any fee or charge	20 days
Adding a new fee or charge	20 days
Reducing the number of fee-free transactions permitted on your account	20 days
Changing the minimum balance to which an account keeping fee applies	20 days
Changing the method by which interest is calculated	20 days
Changing the circumstances when interest is credited or debited to your account	20 days
Increasing your liability for losses relating to ePayments: see <i>ePayments Section</i>	20 days
Imposing, removing or changing any periodic transaction limit relating to ePayments	20 days
Changing an interest rate	the day of change

For all other changes, we will provide reasonable notice (which, depending on the nature of the change, may be before or after the change is made). If we reasonably consider that such a change is unfavourable to you, we will provide at least 20 days' notice. However, we may give shorter, or no, advance notice of a change unfavourable to you if it is reasonable for us to manage a material and immediate risk.

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

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

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

We will always provide notice in accordance with any applicable law or industry code (such as the Customer Owned Banking Code of Practice).

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

How We Send Notices & Statements

To the extent permitted by law, we may send you notices and statements by:

- post, to the address recorded in our records or to a mailing address you nominate;

- electronic means, including by email to an email address you have given us, SMS to a mobile phone number you have given us, or other electronic message eg. via internet banking
- advertisement in the media or our website, for some notices only;
- other means we agree with you.

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

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

You must ensure your address and other contact details, including email address and mobile phone number, are correct and up to date at all times.

If you change address and don't tell us, we can still give notice to you to the address last recorded with us. If we receive returned mail because you haven't advised us of your change of contact details, we may place a stop on your account(s).

Direct Debits & Periodical Payments

Direct Debits

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

To cancel the DDR Service Agreement, you can contact either the biller or us. If you contact us, we will take action within 1 business day to cancel the facility. We suggest that you also contact the biller.

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

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

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

Periodical Payments

A periodical payment is an automatic transfer of funds from your account to a specified recipient account with MoveBank, another financial institution or biller, on a regular basis.

Periodical payments can be established through internet banking, or by contacting us or completing a periodical payment form.

If your periodical payment falls on a non-business day, we may process your authority on the business day immediately preceding or succeeding the due date.

If there are insufficient funds held in your account to cover a periodical payment on 5 occasions, MoveBank may cancel the authority.

We do not have to advise you if a periodical payment is not made, or an authority is cancelled by us. A periodical payment authority can be cancelled by the same means by which it was established, that is, through internet banking or by contacting MoveBank. Please ensure that at least 3 business days' prior notice is given for cancellation requests.

Term Deposits

A term deposit can be established online through internet banking, by calling our contact centre or visiting our branch.

Deposit Restrictions

You may only increase the value of your term deposits on maturity.

We have the right to refuse to accept any deposit and may set maximum and minimum amounts for deposits and terms.

Interest

The interest rate on your term deposit is fixed for the term of your investment. If we quote you a rate for a term deposit the rate may differ if the deposit is not made on the same day.

Interest will be calculated on closing daily balances. The daily interest rate is the relevant annual rate divided by the number of whole days in the year. We will not change the method of interest calculation during the term of the deposit.

Interest is paid annually, monthly or at maturity depending on the term. For terms longer than 12 months, interest is paid every 12 months and then at maturity. Please see the Interest Rate Schedule for specific information regarding the payment of interest.

Withdrawal Restrictions

The term deposit is issued on terms that the funds will be available on maturity.

If you wish to withdraw the whole or part of the balance of a Term Deposit prior to maturity, you must give us 7 days' notice.

Subject to the preceding paragraph, if you wish to withdraw the whole or part of the balance early, the interest earned on the withdrawn amount from the beginning of the term will be reduced as follows:

Proportion of term completed at time of redemption	Interest reduction as a %age of the interest earned to the time of redemption
0% < 25%	80%
25% < 50%	60%
50% < 75%	40%
75% < 100%	20%

If we have already paid you interest during the term that exceeds the total interest you are entitled to under the reduced rate, then the difference is due and payable by you, and we may deduct it from the funds withdrawn early.

In special circumstances, such as hardship, we may allow you to withdraw the whole or part of the balance of a Term Deposit prior to maturity without the 7 days' notice period, however the reduced interest rate may still apply.

In the case of partial redemptions, the amount remaining will continue to earn the interest rate originally agreed until the date of maturity. If the amount remaining is less than the minimum allowed for that type of term deposit, the whole balance must be redeemed, and reduced interest will apply.

No interest rate reduction shall apply where the term deposit is released early due to the death of a depositor.

Maturity

We will write to you at least 30 days prior to the maturity of your term deposit detailing your re-investment options.

Where you respond, on the maturity date, the principal and interest will be disbursed in accordance with your instructions.

If you do not contact us, we will automatically reinvest your funds for the same term as the previous term deposit at the current rate of interest applicable. If the same term is not available, we will reinvest your deposit for the closest term. We will accept your instructions up to 7 days after the maturity date without incurring a reduction in interest.

Electronic Access Facilities and ePayments Conditions of Use

Section 1. Information about ePayment Facilities

You should follow the guidelines in the box below to protect against unauthorised use of your access cards, devices and passcodes.

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 ABOUT PROTECTING YOUR ACCESS CARDS, DEVICES AND PASSCODES

- Sign the access card as soon as you receive it
- Familiarise yourself with your obligations to keep your access card and passcodes secure
- Familiarise yourself with the steps you have to take to report loss or theft of your access card or device, or to report unauthorised use of your access card, BPAY or internet or mobile banking
- Immediately report loss, theft or unauthorised use or access (see *How to Contact Us* on page 2)
- If you change a passcode, do not select a passcode which represents your birth date or a recognisable part of your name
- Never write or save the passcode on any access card, mobile phone, computer or device, even if disguised
- Never record any passcode on a device used to carry out ePayments, unless a reasonable attempt has been made to protect the security of the passcode. (see: *Section 6.3*)
- Never write the passcode on anything which is kept with or near any access card, mobile phone, computer or device.
- 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 any electronic equipment
- Keep a record of the access card number and the Card Hotline telephone number for your area with your usual list of emergency telephone numbers
- Check your statements regularly for any unauthorised use

- Immediately notify us when you change your address and ensure your contact details including email address and mobile phone number, are correct and up to date at all times.
- ALWAYS access the telephone banking or internet banking service only using the OFFICIAL phone numbers and URL addresses
- NEVER access internet banking via a link in an email, SMS or other electronic message.
- If accessing internet banking on someone else's PC, laptop, tablet or mobile phone, ALWAYS DELETE your browsing history
- ALWAYS REJECT any request to provide or to confirm details of your passcode. We will NEVER ask you to provide us with these details

IF YOU FAIL TO ENSURE THE SECURITY OF YOUR ACCESS CARD, ACCESS FACILITY AND PASSCODES YOU MAY INCREASE YOUR LIABILITY FOR UNAUTHORISED TRANSACTIONS

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

Visa card
BPAY®

Osko® payments including NPP and PayTo

Internet Banking
Mobile Banking

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

Visa card

Visa card allows you to make payments at any retailer displaying the Visa card logo, anywhere in the world.

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

- check your account balances (at participating ATMs)
- withdraw cash from your account
- make purchases at retailers, including over the phone and on the internet
- transfer money between accounts (at participating ATMs)
- deposit cash into your account via Bank@Post

We may choose not to give you a Visa card if your banking history with the Credit Union is not satisfactory or if you are under 18 years.

Limit on Visa credit card use

You must not transact:

- For the purpose of gambling;
- In connection with unlawful activities; and
- With an unregistered foreign cryptocurrency exchange or broker

We may also restrict any transaction if we have reasonable grounds, including if the transaction will breach these conditions of use or any law.

IMPORTANT INFORMATION ABOUT CHARGEBACKS FOR VISA CARD

If you wish to dispute a Visa Card transaction you should notify us as soon as possible. Under the card scheme rules we can seek a refund of Visa Card purchases from the merchant's financial institution in certain circumstances, such as non-delivery of goods or

services ordered, unauthorised purchases, or payments under a regular payment arrangement that you had already cancelled. This is called a 'chargeback'. The card scheme rules impose strict timeframes on requesting chargebacks. We will need to investigate a disputed transaction to determine if we have a right to a chargeback. You must provide us with any information or material we request to investigate the transaction and support the chargeback request. If we determine that we have a right to a chargeback we will seek it without delay.

It is in your own interest to notify us as soon as possible if you become aware of circumstances which might entitle us to claim a chargeback on your behalf.

However, you should seek to resolve the issue with the merchant first. Please note that chargebacks do not apply to BPAY payments.

Section 2. Definitions

- a) **access card** means an ATM card, debit card or credit card and includes our Visa card
- b) **AFCA** means the Australian Financial Complaints Authority
- c) **ATM** means automatic teller machine
- d) **BECS Procedures** means the Bulk Electronic Clearing System Procedures as existing from time to time
- e) **business day** means a day that is not a Saturday, a Sunday, a public holiday or bank holiday in the place concerned.
- f) **device** means a device we give to a user that is used to perform a transaction. Examples include:
 - i. ATM card
 - ii. Debit card or credit card whether physical or virtual
 - iii. Token issued by us that generates a passcode.
- g) **Direct debit** means a "Direct Debit Request" as defined in the BECS Procedures
- h) **facility** means an arrangement through which you can perform transactions
- i) **identifier** means information that a user:
 - i. knows but is not required to keep secret
 - ii. must provide to perform a transaction

Examples include an account number, member number or PayID. An identifier also includes a token generated from information that would otherwise be an identifier.

- j) **manual signature** means a handwritten signature, including a signature written on paper and a signature written on an electronic tablet
- k) **mandated payment service** Known as "PayTo". This is the NPP service which enables us to process NPP Payments from your account in accordance with and on the terms set out in a payment agreement you have established with a Merchant or Payment Initiator that subscribes to the service
- l) **NPP** means the New Payments Platform operated by NPP Australia Limited
- m) **NPP Payments** means electronic payments cleared and settled by participating financial institutions via the NPP
- n) **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. internet banking password
 - iii. telephone banking password
 - iv. code generated by a physical security token
 - v. code provided to a user by SMS, email or in a mobile application

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

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

- o) **pay anyone banking facility** means a facility where a user can make a payment from one bank account to a third party's bank account by entering, selecting or using a Bank/State/Branch (BSB) and account number, PayID or other identifier, but does not include BPAY® or PayTo payments.
- p) **payment agreement** means an agreement established by you and an approved Merchant or Payment Initiator by which you authorise us to make payments from your account. Payment agreements include Migrated Direct Debit mandates
- q) **payment initiator** an approved payment service provider who, acting on behalf of you or a merchant, is authorised by you to initiate payments from your account.
- r) **PayTo** means a mandated payment service
- s) **regular payment arrangement** means either a recurring or an instalment payment agreement between you (the cardholder) and a Merchant in which you have preauthorised the Merchant to bill your account account using your debit card or credit card details at predetermined intervals (eg. monthly or quarterly) or at intervals agreed by you. The amount may differ or be the same for each transaction
- t) **transaction** means a transaction to which these ePayment Conditions of Use apply, as set out in Section 3
- u) **unauthorised transaction** means a transaction that is not authorised by a user. It does not include any transaction that is performed by you or another user, or by anyone who performs a transaction with the knowledge and consent of you or another user
- v) **user** means you or an individual you have authorised to perform transactions on your account, including:
 - i. a third party signatory to your account
 - ii. a person you authorise us to issue an additional card to
- w) **we, us, or our** means MoveBank
- x) **you** means the person or persons in whose name this account and access facility is held

Section 3. 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 Without limiting clause 3.1, these ePayment Conditions of Use apply to the following transactions:

- a) electronic card transactions, including ATM, credit card and debit card transactions that are not intended to be authenticated by comparing a manual signature with a specimen signature
- b) telephone banking and bill payment transactions
- c) pay anyone banking facility transactions
- d) online transactions performed using a card number and expiry date
- e) online bill payments (including BPAY®)
- f) direct debits
- g) transactions using mobile devices

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 acknowledgement 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 a 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
- 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 to 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 pre-arranged 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).

Note: If you or another user breaches these passcode security requirements, we may not be required to indemnify you for loss arising from that breach. See Section 5.

6.3. For the purpose of clauses 6.2(b) to 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, computer or other personal electronic device 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.

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

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

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

- b) **Receiving ADI** means an ADI whose customer has received an internet payment
- c) **Unintended recipient** means the recipient of funds as a result of a mistaken internet

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

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

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

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

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

9.5. 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:

- 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 to 9.5, or as described in the box overleaf

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.

9.9. If you receive a mistaken internet payment into your account and we are required under the ePayments Code as receiving ADI to return the funds to the payer's ADI then we will, without seeking your consent, transfer the funds from your account. If there are insufficient funds in your account you must co-operate with us to facilitate repayment of the funds.

INFORMATION ABOUT A RECEIVING ADI'S OBLIGATIONS AFTER WE REQUEST RETURN OF FUNDS

The information set out in this box is to explain the process for retrieving mistaken payments under the ePayments Code, setting out what the processes are, and what you are entitled to do. This information does not give you any contractual entitlement to recover the mistaken payment from us or to recover the mistaken payment from the receiving ADI.

Process where sufficient funds are available and report is made within 10 business days

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

Process where sufficient funds are available and report is made between 10 business days and 7 months

- The receiving ADI must complete its investigation into the reported mistaken payment within 10 business days of receiving the request.
- If satisfied that a mistaken internet payment has occurred, the receiving ADI must:
 - a) prevent the unintended recipient from withdrawing the funds for 10 further business days, and
 - b) notify the unintended recipient that it will withdraw the funds from their account, if the unintended recipient does not establish that they are entitled to the funds within 10 business days commencing on the day the unintended recipient was prevented from withdrawing the funds
- If the unintended recipient does not, within 10 business days, establish that they are entitled to the funds, the receiving ADI must return the funds to the sending ADI within 2 business days after the expiry of the 10 business day period, during which the unintended recipient is prevented from withdrawing the funds from their account.
- If the receiving ADI is not satisfied that a mistaken internet payment has occurred, it may seek the consent of the unintended recipient to return the funds to the holder.
- The sending ADI must return the funds to the holder as soon as practicable.

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

- If the receiving ADI is satisfied that a mistaken internet payment has occurred, it must seek the consent of the unintended recipient to return the funds to the user.
- If not satisfied that a mistaken internet payment has occurred, the receiving ADI may seek the consent of the unintended recipient to return the funds to the holder.
- If the unintended recipient consents to the return of the funds:
 - a) The receiving ADI must return the funds to the sending ADI; and
 - b) The sending ADI must return the funds to the holder as soon as practicable

Process where sufficient funds are not available

- Where the sending ADI and the receiving ADI are satisfied that a mistaken internet payment has occurred, but there are not sufficient credit funds available in the account of the unintended recipient to the full value of the mistaken internet payment, the receiving ADI must exercise discretion, after appropriate weighing of interests of the sending consumer and unintended recipient and information reasonably available to it about the circumstances of the mistake and the unintended recipient, in deciding whether it should pursue return of the total value of the mistaken internet payment, pursue the return of a partial amount of the mistaken internet payment, or not pursue any return of funds.
- The above processes where sufficient funds are available will also apply where insufficient funds are available, but only in relation to the value of the insufficient funds available.

Section 10. Using Internet or Mobile Banking

- 10.1. We do not warrant that:
 - a) The information available to you about your accounts through our internet or mobile banking service is always up to date
 - b) You will have 24 hours a day, 7 days per week, access to internet or mobile banking
 - c) data you transmit via internet or mobile banking or internet banking is totally secure
- 10.2. We may cancel your access to Internet Banking if you do not access this service by the use of your Access Code.
 - a) within 30 days of our provision of that Access Code, or
 - b) for a period of 90 days.
- 10.3. We may require 2 factor authentication to be activated prior to allowing or continuing access to internet banking.

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 report contact us during business hours or the access card Hotline at any time. Please refer to How to Contact Us on page 2 for contact details.
- 11.2. We will acknowledge your notification by giving you a reference number that verifies the date and time you contacted us. Please retain this reference number.
- 11.3. 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 email as soon as possible
 - b) by telephoning the Visa Card Hotline number for the country you are in

Visa Card Hotline	
Australia	Overseas
During business hours 1300 362 216	Brisbane business hours +61 7 3221 2216
Outside business hours 1800 621 199	Outside business hours Visa card Hotline number for the country you are in

Section 12. How to Report Unauthorised use of Internet or Mobile Banking

- 12.1. If you believe that your passcodes for internet or mobile banking transactions have been misused, lost or stolen, or, where relevant, your passcode has become known to someone else, you must contact us immediately. Please refer to How to Contact Us on page 2 for our contact details. We will acknowledge your notification by giving you a reference number that verifies the date and time you contacted us. Please retain this reference number.
- 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 and before using it.
- 13.2. We will 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
 - c) what the daily cash withdrawal limits are
 Please refer to the Summary of Accounts, Access Facilities and Transaction Limits 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 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 card outside Australia

- 14.1. All transactions made in a foreign currency on the Visa card will be converted into Australian currency by Visa Worldwide and calculated at a wholesale market rate selected by Visa from within a range of wholesale rates or the government mandated rate that is in effect one day prior to the Central Processing Date (that is, the date on which Visa processes the transaction).
- 14.2. All transactions made in a foreign currency or with a merchant located overseas (even if in Australian currency) on the Visa card are subject to a conversion fee.
- 14.3. Please refer to the Fees and Charges Schedule brochure for the current conversion fee
- 14.4. Some overseas merchants and electronic terminals charge a surcharge for making a transaction using your Visa card. Once you have confirmed that transaction you will not be able to dispute the surcharge. The surcharge may appear on your statement as part of the purchase price
- 14.5. Some overseas merchants and electronic terminals allow the cardholder the option to convert the value of the transaction into Australian dollars at the point of sale, also known as Dynamic Currency Conversion. Once you have confirmed the transaction you will not be able to dispute the exchange rate applied.

Section 15. Additional Access Card

- 15.1. You may authorise us, if we agree, to issue an additional access card to an additional cardholder provided this person is over the age of 18 (unless we agree to a younger age).
- 15.2. You will be liable for all transactions carried out by this cardholder.
- 15.3. We will give each additional cardholder a separate passcode.
- 15.4. You must ensure that any additional cardholders protect their access card and passcode in the same way as these ePayment Conditions of Use require you to protect access card and passcode.
- 15.5. To cancel the additional access card you must notify us by telephone, in person at the branch or in writing. Please refer to How to Contact Us on page 3 for our contact details.
- 15.6. You will not be liable for the continued use of the additional access card after its cancellation

Section 16. Use after Cancellation or Expiry of Access Code

- 16.1. You must not use your access card:
 - a) Before the valid date or after the expiration date shown on the face of access card
 - b) after the access card has been cancelled
- 16.2. 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 17. Exclusions of Access Card Warranties and Representations

- 17.1. We do not warrant that merchants or ATMs displaying access card signs or promotional material will accept access card.
- 17.2. 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 access card.
- 17.3. We are not responsible for any defects in the goods and services you acquire through the use of the Visa card. You acknowledge and accept that all complaints about these goods and services must be addressed to the supplier or merchant of those goods and services.

Section 18. Cancellation of Access card or of access to Internet and Mobile Banking, Bpay or Osko

- 18.1. You may cancel your access card, your access to internet or mobile banking, BPAY or Osko at any time by calling our contact centre or visiting our branch.
- 18.2. We may, acting reasonably, immediately cancel or suspend your access card or your access to internet or mobile banking, BPAY or Osko at any time:
 - a) for security reasons,
 - b) if you breach these Conditions of Use,
 - c) if we reasonably suspect that you, or someone acting on your behalf, is being fraudulent,
 - d) in the case of Osko, if we reasonably suspect that you are using Osko in a manner that is likely to affect our ability to continue providing Osko to you or our other customers,
 - e) in the case of Osko, if we cease to be a participant in Osko
 - f) for any other reason set out in Closing Accounts, Cancelling Access Facilities & Delaying, Blocking, Freezing or Refusing Transactions on page 12.
- 18.3. We may cancel your access card or your access to internet or mobile banking, BPAY or Osko for any reason by giving you 30 days' notice. The notice does not have to specify the reasons for cancellation.
- 18.4. In the case of access card, you will be liable for any transactions you make using your access card before the access card is cancelled but which are not posted to your account until after cancellation of access card.
- 18.5. In the case of internet or mobile banking, BPAY or Osko, if, despite the cancellation of your access to the relevant access method, you carry out a transaction using the relevant access method, you will remain liable for that transaction.
- 18.6. Your access card or your access to telephone internet or mobile banking, BPAY or Osko 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 internet or mobile banking, BPAY or Osko access
 - c) you alter the authorities governing the use of your account or accounts to which the access card applies or which has internet or mobile banking BPAY or Osko access (unless we agree otherwise)
- 18.7. In the case of access card, we may demand the return or destruction of any cancelled access card

Section 19. Using Bpay

- 19.1. You can use BPAY to pay bills bearing the BPAY logo from those accounts that have the BPAY facility.
- 19.2. 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 (eg. your account number with the biller), the amount to be paid and the account from which the amount is to be paid.
- 19.3. We cannot effect your BPAY instructions if you do not give us all the specified information or if you give us inaccurate information.

19.4. 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 20. Processing Bpay Payments

20.1. 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
- 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.

20.2. A BPAY payment instruction is irrevocable.

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

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

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

20.6. Please note that you must provide us with written consent addressed to the biller who received that BPAY payment.

20.7. 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.

20.8. 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, that is, a day in Sydney when banks can effect settlements through the Reserve Bank of Australia
- b) otherwise, on the next banking business day after you direct us to make it

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

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

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

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

- a) advise you of this
- b) credit your account with the amount of the BPAY payment
- c) take all reasonable steps to assist you in making the BPAY payment as quickly as possible

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

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

20.12. 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 21. Future Dated BPAY Payments

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

- 21.1. You may arrange BPAY payments up to 60 days in advance of the time for payment. If you use this option, you should be aware of the following:
 - 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, and you may be charged a dishonour fee
 - 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 contact us if there are any problems with your future-dated payment
 - e) You must contact us if you wish to cancel a future-dated payment after you have given the direction but before the date for payment. You cannot stop the BPAY payment on or after that date.

Section 22. Consequential Damage for BPAY Payments

- 22.1. 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.
- 22.2. 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 23. Using Osko

- 23.1. You can use Osko® to make payments from those accounts that have the Osko facility to:
 - a) make an Osko payment
 - b) make scheduled and recurring Osko payments
 - c) pay bills bearing the Osko logo.
- 23.2. When you tell us to make an Osko payment you must tell us the payee's PayID or the details of the payee's account, the amount to be paid and the account from which the amount is to be paid.
- 23.3. We cannot effect your Osko instructions if you do not give us all the specified information or if you give us inaccurate information.

Section 24. Processing Osko Payments

- 24.1. We will attempt to make sure that your Osko payments are processed promptly by participants in Osko, and you must tell us promptly if:
 - a) you become aware of any delays or mistakes in processing your Osko payment,
 - b) you did not authorise an Osko payment that has been made from your account; or
 - c) you think that you have been fraudulently induced to make an Osko payment.
- 24.2. A Osko payment instruction is irrevocable.
- 24.3. Except for scheduled and recurring Osko payments, you cannot stop an Osko payment once you have instructed us to make it and we cannot reverse it.
- 24.4. We will treat your Osko payment instruction as valid if, when you give it to us, you use the correct access method.

- 24.5. You should notify us immediately if you think that you have made a mistake (except for a mistake as to the amount you meant to pay).
- 24.6. If we are advised that your payment cannot be processed by a biller, we will:
 - a) advised you of this;
 - b) credit your account with the amount of the Osko payment; and
 - c) take all reasonable steps to assist you in making the Osko payment as quickly as possible.

Section 25. Scheduled and Recurring Osko Payments

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

- 25.1. You may schedule Osko payments up to 60 days in advance of the time for payment and you can also schedule recurring Osko payments. If you use this option, you should be aware of the following:
 - a) you are responsible for maintaining, in the account to be drawn on, sufficient cleared funds to cover all scheduled and recurring Osko payments (and any other drawings) on the day(s) you have nominated for payment or, if the account is a credit facility, there must be sufficient available credit for that purpose,
 - b) if there are insufficient cleared funds or, as relevant, insufficient available credit, the Osko payment will not be made and you may be charged a dishonour fee,
 - c) you are responsible for checking your account transaction details or account statement to ensure that the scheduled or recurrent Osko payment is made correctly,
 - d) you should contact us if there are any problems with your scheduled or recurrent Osko payments,
 - e) you must contact us if you wish to cancel a scheduled or recurrent Osko payment after you have given the direction but before the date for payment.

Section 26. Regular Payment Arrangements

- 26.1. You should maintain a record of any regular payment arrangement that you have entered into with a Merchant.
- 26.2. To change or cancel any regular payment arrangement you should contact the Merchant or us at least 15 days prior to the next scheduled payment. If possible, you should retain a copy of this change/cancellation request.
- 26.3. 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.
- 26.4. 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 27. Authority to Recover Mistaken or Misdirected Payments

- 27.1. Where we and the sending financial institution determine that an Osko or other NPP Payment made to your account is either a Mistaken Payment or a Misdirected Payment, we may, without your consent, and subject to complying with any other applicable terms and conditions, deduct from your account, an amount up to the original amount of the Mistaken Payment or Misdirected Payment. We will notify you if this occurs.
- 27.2. In this Section 27:
 - Misdirected Payment** means an NPP Payment using a PayID, erroneously directed to an incorrect account because the financial institution that registered the PayID has not registered or maintained the correct information

Mistaken Payment means an NPP Payment by a payer who is a 'user' as defined in the ePayments Code, erroneously directed to the wrong account as a result of the payer's error (for example, by inputting incorrect payee account details, either by accident or because the payee gave them the incorrect account details)

Section 28. Digital Wallet

When this Section applies

28.1. This Section applies when you, or an additional cardholder, add an Eligible Card to a Digital Wallet on a Supported Device. This Section applies in addition to the terms and conditions that apply to the Account and Eligible Card.

Digital Wallet Services

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

Your Security Obligations

28.3. You, and each additional cardholder, must take reasonable steps to secure the Supported Device and any PIN or other passcode registered to the Supported Device in the same way as you would your Eligible Card and related passcode, in accordance with these Conditions of Use.

Device Security

28.4. You, and each additional cardholder, must:

- ensure that only your, or the additional cardholder's, biometric identifier (e.g. fingerprint) is registered on the Supported Device ;
- not allow any other person's biometric identifier to remain, or be, registered on the Supported Device;
- not select a PIN or other passcode registered to the Supported Device that is easily guessed (e.g. your date of birth);
- not share any PIN or other passcode registered to the Supported Device with any person;
- not write or record the PIN or other passcode on the Supported Device, or on anything:
 - carried with the Supported Device
 - liable to loss or theft simultaneously with the Supported Device unless you, or the additional cardholder make a reasonable attempt to protect the security of the PIN or other passcode
- not leave the Supported Device unattended, and lock it when not in use;
- before disposing of a Supported Device, remove or unlink the Eligible Card from it

28.5. If you, or an additional cardholder:

- allow another person's biometric identifier to remain, or be, registered on the Supported Device; or
- share any PIN or other passcode registered to the Supported Device with any person, then you are taken to have authorised that person to carry out transactions using the Supported Device and you will be responsible for their use of the Eligible Card

Lost or Stolen Devices or Unauthorised Use

28.6. You should immediately notify us if:

- a Supported Device is lost or stolen;

- b) you suspect that any PIN, passcode or other security credential registered to a Supported Device has become known to someone else;
- c) you suspect that someone else has used or could use a Supported Device to carry out a transaction on your Account without permission.

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

If your Supported Device is lost or stolen you should immediately remove or unlink your Eligible Card from the Digital Wallet where possible.

Privacy

28.7. We may share and exchange with the Digital Wallet provider and the relevant card scheme network (e.g. Visa or eftpos) personal information about you in relation to your set up and use of the Digital Wallet, to allow you to use the Eligible Card in the Digital Wallet.

Changes to this Section

28.8. We may change this Section at any time and notify you of the changes in accordance with these Conditions of Use. You agree to us providing notification electronically.

Termination

28.9. We may suspend or terminate the use of an Eligible Card in a Digital Wallet without notice at any time, including if:

- a) You, or an additional cardholder, breach this Section;
- b) We reasonably suspect an unauthorised transaction has occurred or for other security reasons;
- c) We are required by a regulatory or government body.

Definitions

28.10. In this Section:

Account means your account with us to which an Eligible Card is linked

Digital Wallet means any digital wallet service provided by a third party including without limitation Apple Pay as provided by Apple Inc. and Google Pay as provided by Google Inc.

Eligible Card means a debit or credit card issued by us that can be added to a Digital Wallet

Supported Device means any device or equipment that can be used to access your Account using a Digital Wallet, and is not given by us e.g. mobile phone, smart watch

Section 29. Creating and Using your PayID

- a) **account** means your account with us
- b) **Eligible Account** means your savings account with us
- c) **Misdirected Payment** means an NPP Payment erroneously credited to the wrong account because of an error in relation to the recording of the PayID or associated account information in the PayID service
- d) **mistaken payment** means an NPP Payment, made by a payer who is a 'user' for the purposes of the ePayments Code, which is erroneously credited to the wrong account because of the payer's error
- e) **NPP** means the New Payments Platform operated by NPP Australia Limited
- f) **NPP Payments** mean payments cleared and settled via the NPP
- g) **Organisation ID** means an identifier for a customer that is a business customer or organisation, constructed by us as <business name> and/or description of business/campaign/product and/or <geographic location/state>
- h) **PayID** means the identifier you choose to use to receive NPP Payments

- i) **PayID Name** means the name we give you or the name selected by you (with our approval) to identify you to Payers when your PayID is used to make an NPP Payment
- j) **PayID service** means the central payment addressing service which is available for addressing NPP Payments
- k) **PayID Type** means the type of identifier you select from receiving NPP Payments, which may be your telephone number, mobile number, email address, Australian Company Number, Australian Business Number or Organisation ID
- l) **Privacy Law** means the Privacy Act 1988 (Cth) and regulations made under the Act
- m) **We, us and our** means MoveBank Limited
- n) **You and your** means a person who, at the time a PayID service is provided is an individual or a business organisation that is our customer (or prospective customer)

29.2. Making and receiving NPP Payments using PayID

- a) The PayID service is the NPP Payment addressing service that enables payers to make NPP Payments to you using an alternative identifier instead of your account details.
- b) Before you can create your PayID to receive NPP Payments into your account, you have to satisfy us that you either own or are authorised to use your chosen PayID and you have an Eligible Account.
- c) Whether you choose to create a PayID for your account or not, you and each Authorised User, may use a payee's PayID to make particular types of NPP Payments to the payee from your account provided that:
 - i. we and the payee's financial institution support the NPP Payment service,
 - ii. the payee's account is able to receive the particular NPP Payment; and
 - iii. the PayID is not locked.
- d) For terms of:
 - i. how PayID may be used for particular NPP Payment services, your obligations to input correct PayID details and to check the payee's PayID Name before sending an NPP Payment see our website; and
 - ii. your rights in relation to the investigation and recovery of Mistaken Payments, Misdirected Payments and unauthorised (including fraudulent) NPP Payments, refer to section 9 of the ePayments section of Account & Access Facility Conditions of Use.

29.3. Choosing a PayID and PayID Name

- a) You may create a PayID as long as it is a supported PayID Type. Some PayID Types, for example Organisation IDs, are restricted to business customers and organisations. Only eligible customers will be able to create a PayID that is a restricted PayID Type.
- b) You must satisfy us that you own or are authorised to use your chosen PayID before you can use it to receive NPP Payments. This means we may ask you to provide evidence to establish this to our satisfaction, whether you are already registered for any other mobile or online banking or online payment services with us or not.
- c) Depending on the policy of a payer's financial institution, your PayID Name may be displayed to payers who send NPP Payments to you. At the same time, you create your PayID, we will either enable you to:
 - i. confirm your selection of a PayID Name for display to payers; or
 - ii. select an alternative PayID Name, such as your business name, for display.
- d) We will not permit selection of a PayID Name that is likely to mislead or deceive a payer into sending you NPP Payments intended for another payee, or which for any reason is inappropriate.

29.4. Creating your PayID

You can create a PayID for receiving NPP Payments by logging into internet banking.

- a) We will not create a PayID for you without your consent.
- b) You may choose to create more than one PayID for your account.

- c) If your account is a joint account, you and each other joint account holder can create a unique PayID for the account.
- d) If you have Authorised Users on your account, each Authorised User may create a unique PayID for the account.
- e) Once a PayID is created and linked to your account, it may not be used in relation to any other account with us or with any other financial institution. See clause 28.5 for details on transferring PayIDs.
- f) The PayID service does not support duplicate PayIDs. If you try to create a PayID for your account which is identical to another PayID in the service, you will see the following message Unable to Register PayID. You can contact us to discuss duplicate PayIDs on 1300 362 216. We cannot disclose details of any personal information in connection with duplicate PayIDs.

29.5. Transferring your PayID to another account

- a) You can transfer your PayID to another account with us, or to an account with another financial institution by submitting a request to us through internet banking.
- b) A transfer of your PayID to another account with us will generally be effective immediately unless we notify you otherwise.
- c) A transfer of your PayID to another financial institution is a two-step process initiated by you and completed by that financial institution. First, ask us to put your PayID into a transfer state and then complete the transfer via your new financial institution. Until the transfer is completed, NPP Payments to your PayID will be directed to your account with us. If the other financial institution does not complete the transfer within 14 days, the transfer will be deemed to be ineffective and your PayID will remain with your account. You can request transfer of your PayID at any time.
- d) A PayID which we have temporarily disabled cannot be transferred: see clause 28.8.

29.6. Transferring your PayID from another Financial Institution to your account

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

29.7. Closing a PayID

- a) To close your PayID, log into internet banking.
- b) You must notify us immediately if you no longer own or have authority to use your PayID.

29.8. Locking and Unlocking a PayID

- a) We monitor PayID use to manage PayID misuse and fraud. You acknowledge and consent to us locking your PayID if we reasonably suspect misuse of your PayID or use of your PayID to procure NPP Payments fraudulently.
- b) Request to unlock a locked PayID may be made by logging into internet banking.

29.9. NPP Payments

- a) We will ensure that your PayID and account details are accurately recorded in the PayID service.

29.10. Privacy

- a) By creating your PayID you acknowledge that you authorise:
 - i. us to record your PayID, PayID Name and account details (including full legal account name) (PayID Record) in the PayID service,
 - ii. NPP Participants which are payers' financial institutions to use your PayID information for the purposes of constructing NPP payment messages, enabling payers to make NPP Payments to you, and to disclose your PayID Name to payers for NPP Payment validation.

29.11. To the extent that the creation and use of the PayID Record constitutes a disclosure, storage and use of your personal information within the meaning of the Privacy Law, you acknowledge and agree that you consent to that disclosure, storage and use

Section 30. Creating a Payment Agreement

- 30.1. PayTo allows payers to establish and authorise Payment Agreements with Merchants or Payment Initiators who offer PayTo as a payment option.
- 30.2. If you establish a Payment Agreement with a Merchant or Payment Initiator that offers PayTo payment services, you will be required to provide that the Merchant or Payment Initiator with your personal information including your BSB and account number or PayID. You are responsible for ensuring the correctness of the account number or PayID you provide for the purpose of establishing a Payment Agreement. Any personal information or data you provide to the Merchant or Payment Initiator will be subject to the privacy policy and terms and conditions of the relevant Merchant or Payment Initiator.
- 30.3. Payment Agreements must be recorded in the Mandate Management Service in order to be processed. The Merchant or Payment Initiator is responsible for creating and submitting a record of each Payment Agreement to their financial institution or payments processor for inclusion in the Mandate Management Service. The Mandate Management Service will notify us of the creation of any Payment Agreement established using your Account or PayID details. Then we will notify you of the creation of the Payment Agreement, the Merchant or Payment Initiator and the payment amount and frequency if these are provided. We will also seek your consent to make payments. You may confirm or decline any Payment Agreement presented for your approval. Your confirmation or decline will be recorded against the Payment Agreement in the Mandate Management Service. Where a confirmation is recorded in these circumstances the Payment agreement will be deemed to be effective.
- 30.4. Payment instructions in connection with a Payment Agreement, received from the Merchant's or Payment Initiator's financial institution will only be processed if you have confirmed the associated Payment Agreement. Payment instructions may be submitted to us for processing immediately after you have confirmed the Payment Agreement so you must take care to ensure the details of the Payment Agreement are correct before you confirm them. We will not be liable to you or any other person for loss suffered as a result of processing a payment instruction submitted under a Payment Agreement that you have confirmed.
- 30.5. 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.
- 30.6. If you believe the payment amount or frequency or other detail presented is incorrect, you may decline the Payment Agreement and contact the Merchant or Payment Initiator and have them amend and resubmit the Payment Agreement creation request.

Section 31. Amending a Payment Agreement

- 31.1. Your Payment Agreement may be amended by the Merchant or Payment Initiator from time to time, or by us on your instruction.
- 31.2. We will notify you of proposed changes to a Payment Agreement requested by the Merchant or Payment Initiator. Such amendments may include variation of the payment amount, where that is specified in the Payment Agreement as a fixed amount, or payment frequency. The Mandate Management Service will notify us of the amendment request. You may confirm or decline any amendment request presented for your approval. We will promptly record your decision in the Mandate Management Service. Changes that you confirm will be deemed effective immediately, and those declined will result in the Payment Agreement continuing on its existing terms. Amendment requests which are not confirmed or declined within 5 calendar days of being sent to you, will expire. If you do not authorise or decline the amendment request within this period of time, the amendment request will be deemed to be declined.
- 31.3. If you believe the details of the amendment request are incorrect, you may contact the Merchant or Payment Initiator and have them resubmit the amendment request. We are not

authorised to vary the details in an amendment request submitted by a Merchant or Payment Initiator

31.4. Once a Payment Agreement has been established, you may tell us to amend your name or Account details in the Payment Agreement only. Account details may only be replaced with the BSB and account number of an account you hold with us. If you wish to amend the Account details to refer to an account with another financial institution, you may give us a transfer instruction (See 33 Below) We may decline to act on your instruction to amend your Payment Agreement if we are not reasonably satisfied that your request is legitimate. You may not request us to amend the details of the Merchant or Payment Initiator, or another party.

Section 32. Pausing your Payment Agreement

32.1. You may tell us to pause and resume your Payment Agreement. We will act on your instruction to pause or resume your Payment Agreement promptly by updating the record of the Payment Agreement in the Mandate Management Service. The Mandate Management Service will notify the Merchant's or Payment Initiator's financial institution or payment processor of the pause or resumption. During the period the Payment Agreement is paused, we will not process payment instructions in connection with it. We will not be liable for any loss that you or any other person may suffer as a result of the pausing of a Payment Agreement that is in breach of the terms of an agreement between you and the relevant Merchant or Payment Initiator.

32.2. Merchants and Payment Initiators may pause and resume their Payment Agreements. If the Merchant or Payment Initiator pauses a Payment Agreement to which you are a party, we will promptly notify you of that, and of any subsequent resumption. We will not be liable for any loss that you or any other person may suffer as a result of the pausing of a Payment Agreement by the Merchant or Payment Initiator.

Section 33. Transferring your Payment Agreement

33.1. When available, you will be able to ask us to move a Payment Agreement to an account you hold with another financial institution. We will provide you with a Transfer ID to provide to your new financial institution to enable them to complete the transfer.

33.2. Your new financial institution will be responsible for having you authorise the transfer of the Payment Agreement and also updating the Payment Agreement in the Mandate Management Service. The updated Payment Agreement will become effective upon being updated in the Mandate Management Service.

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

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

Section 34. Cancelling your Payment Agreement

34.1. You can instruct us to cancel a Payment Agreement on your behalf using your internet banking. We will promptly update the record of the Payment Agreement in the Mandate Management Service. The Mandate Management Service will notify the Merchant's or

Payment Initiator's financial institution or payment processor of the cancellation. We are not liable for any loss suffered by you, the Merchant or the Payment Initiator as a result of you cancelling a Payment Agreement.

34.2. Merchants and Payment Initiators may cancel Payment Agreements. We will promptly notify you if this happens. We are not liable for loss resulting from the cancellation of your Payment Agreement by the Merchant or Payment Initiator.

Section 35. Migration of Direct Debit arrangements

- 35.1. Merchants and Payment Initiators can migrate existing Direct Debit arrangements you have in place to a Payment Agreement. You will not be required to consent to or authorise these migrations, nor will you be asked to provide consent.
- 35.2. As with other Payment Agreements, you can amend, pause/resume, cancel or transfer your Migrated Direct Debit Mandates in accordance with these terms and conditions.
- 35.3. Once the migration is completed, it is the responsibility of the Merchant or Payment Initiator to cancel the existing Direct Debit arrangement.

Section 36. General – your responsibilities

- 36.1. You must carefully consider any Payment Agreement creation or amendment request including Migrated Direct Debit mandates before agreeing to them. We will not be liable for any loss you suffer for processing a payment in accordance with the terms of a Payment Agreement.
- 36.2. You must tell us immediately if you no longer hold or have authority to operate the Account from which a payments under a Payment Agreement or Migrated Direct Debit Mandate have been or will be made.
- 36.3. You must promptly respond to any notification that you receive from us regarding the pausing or cancellation of a Payment Agreement or Migrated Direct Debit Mandate for misuse, fraud or for any other reason. We will not be liable for any loss you suffer for not responding promptly to such a notification.
- 36.4. You must ensure that you comply with the terms of any agreement that you have with a Merchant or Payment Initiator, including any termination notice periods. You are responsible for any loss suffered if you cancel or pause a Payment Agreement which puts you in breach of your obligations to the Merchant or Payment Initiator. We act as a payments facilitator, any disputed payments should be referred to your Merchant in the first instance.
- 36.5. You are responsible for ensuring that you have sufficient funds in your Account to meet the requirements of all your Payment Agreements and Migrated Direct Debit Mandates. We will not be responsible for any loss that you suffer as a result of your Account having insufficient funds and may charge fees for declined transactions in accordance with our Schedule of Fees. Fees additionally may be payable to third parties under their terms and conditions.
- 36.6. If you receive a Payment Agreement creation request or become aware of payments being processed from your Account that you are not expecting, or experience any other activity that appears suspicious or erroneous, please report such activity to us via phone, email or the secure messaging service.
- 36.7. If you receive a Payment Agreement creation request or become aware of payments being processed from your Account that you are not expecting, or experience any other activity that appears suspicious or erroneous, please communicate this activity to us urgently.
- 36.8. From time to time you may receive a notification from us requiring you to confirm that all of your Payment Agreements and Migrated Direct Debit Mandates are accurate and up to date. You must promptly respond to any such notification. Failure to respond may result in us pausing the Payment Agreement/s or Migrated Direct Debit Mandate/s.
- 36.9. We are not liable for duplicated payments. These must be discussed with your Merchant.

- 36.10. We recommend that you allow notifications from the MoveBank app to your smartphone to ensure that you're able to receive and respond to Payment Agreement creation requests, amendment requests and other notifications in a timely way.
- 36.11. Use of the facilities that we provide to you in connection with establishing and managing your Payment Agreements and Migrated Direct Debit Mandates is required to meet our Acceptable Use Policy. You are responsible for ensuring that: (i) all data you provide to us or to any Merchant or Payment Initiator that subscribes to PayTo is accurate and up to date; (ii) you do not use PayTo to send threatening, harassing or offensive messages to the Merchant, Payment Initiator or any other person; and (iii) any passwords/PINs needed to access the facilities we provide are kept confidential and are not disclosed to any other person.
- 36.12. All intellectual property, including but not limited to the PayTo trademarks and all documentation, remains our property, or that of our licensors (**Our Intellectual Property**). We grant to you a royalty free, non-exclusive license (or where applicable, sub-license) for the Term to use Our Intellectual Property for the sole purpose of using PayTo in a way that is consistent with the terms of this agreement. You can not modify Our Intellectual Property or use it in a manner that is inconsistent with this purpose.
- 36.13. Where an intellectual property infringement claim is made against you, we will have no liability to you under this agreement to the extent that any intellectual property infringement claim is based upon: (a) modifications to Our Intellectual Property by or on behalf of you in a manner that causes the infringement; (b) use of any item in combination with any hardware, software or other products or services in a manner that causes the infringement and where such combination was not within the reasonable contemplation of the parties given the intended use of the item; (c) your failure to use corrections or enhancements to Our Intellectual Property that are made available to you (except where the use of corrections or enhancements would have caused a defect in PayTo or would have had the effect of removing functionality or adversely affecting the performance of PayTo); and (d) your failure to use Our Intellectual Property in accordance with this agreement.
- 36.14. We may cease providing PayTo at any time and at our sole discretion. We may also amend these terms at any time by providing you with reasonable notice of any change. If you don't accept any proposed change you may stop using these services.
- 36.15. We will accurately reflect all information you provide to us in connection with a Payment Agreement or a Migrated Direct Debit Mandate in the Mandate Management Service.
- 36.16. We may monitor your Payment Agreements or Migrated Direct Debit Mandates for misuse, fraud and security reasons. You acknowledge and consent to us pausing or cancelling all or some of your Payment Agreement or Migrated Direct Debit Mandates if we reasonably suspect misuse, fraud or security issues or to otherwise protect your or our legitimate interests. Subject to our legal obligations, we will promptly notify you of any such action to pause or cancel your Payment Agreement.
- 36.17. If you become aware of a payment being made from your Account that is not permitted under the terms of your Payment Agreement or Migrated Direct Debit Mandate or that was not authorised by you, please contact us as soon as possible and submit a claim. We will respond to all claims promptly and if the claim is founded, we will refund your Account. We will not be liable to you for any payment made that was in fact authorised by the terms of your Payment Agreement or Migrated Direct Debit Mandate
- 36.18. No liability is accepted for delayed or failed payments caused by service interruptions to PayTo, NPP or other banking services. We will endeavour to process impacted payment requests when services resume.
- 36.19. For large value Banking transactions including PayTo arrangements, we reserve the right at our absolute discretion to obtain your consent via non-digital means.
- 36.20. By confirming a Payment Agreement and / or permitting the creation of a Migrated Direct Debit Mandate against your Account with us, you acknowledge that you authorise us to

collect, use and store your personal information and details of your Payment Agreement(s) and Migrated Direct Debit Mandates in the Mandate Management Service, and that these details may be disclosed to the financial institution or payment processor for the Merchant or Payment Initiator, for the purposes of creating payment instructions and constructing NPP Payment messages and enabling us to make payments from your Account.

Complaints

If you wish to make a complaint, please speak with our staff at the branch or by calling 1300 362 216.

You may also make a complaint:

- By emailing info@movebank.com.au
- Through the Contact Us form on our website

We will handle your complaint fairly and try to resolve it as soon as possible. If we cannot resolve the issue on the spot, we will do our best to complete our investigation and inform you of our decision within 21 days. We will let you know if we need more time.

For more information about our complaint handling process we have a guide to our dispute resolution system available on our website or on request.

Australian Financial Complaints Authority

If you are not satisfied with our response, or handling of your complaint, you may refer the matter to the Australian Financial Complaints Authority (AFCA). AFCA provides a free and independent external resolution service. You can contact AFCA at:

Postal Address: Australian Financial Complaints Authority Limited
GPO Box 3
Melbourne Vic 3001

Website: afca.org.au
Email: info@afca.org.au
Telephone: 1800 931 678

Customer Owned Banking Code of Practice Compliance

If you have a complaint about our compliance with the Customer Owned Banking Code of Practice, you can contact the Customer Owned Banking Code Compliance Committee. Please be aware that the Committee is not a dispute resolution body and cannot provide financial compensation. You can contact the Committee at:

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

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



Member Contact Centre

T. 1300 362 216 W. movebank.com.au E. info@movebank.com.au
M. GPO Box 648, Brisbane QLD 4001

Railways Credit Union Limited trading as MOVE Bank ("MOVE")

AFSL / Australian credit licence 234536

ABN: 91 087 651 090