



Further Information Guide

Macquarie Cash Management Account – 17 December 2018

The following information is incorporated by reference in the current *Macquarie Cash Management Account (Account) Product Information Statement* and must be read in conjunction with this document and the *Fees, limits and lodgement times*.

Important information about your application

Who can open an Account?

- Individuals over 18 years old
- Companies
- Incorporated or unincorporated bodies (eg strata bodies corporate, trade unions and sporting associations)
- Trustees for other entities
- Government bodies, and
- Registered co-operatives.

If you are opening an Account on behalf of a minor (ie acting as trustee) you should quote a Tax File Number or exemption reason to prevent tax being withheld from any interest payments.

If you are opening an Account on behalf of a minor or another entity, we require you to provide supporting documentation.

Residential, email and postal addresses

Please note we are required to collect a residential address for the Account holder(s).

We will send you a welcome email with all your personal Login Details including your Macquarie ID for online services.

Your postal address will be used to send cheque books and printed statements, if requested. Regardless of whether you specifically request printed statements or not, electronic statements will be available online and free of charge. This address can be care of a third party such as your Financial Services Professional.

Attorneys

If you are signing under power of attorney, please provide identification (eg driver's licence) with an attached original certified copy of the power of attorney and specimen signature(s) of the attorney(s) if not displayed on the document.

Privacy Statement

Your privacy is important to us. This statement explains how we will use and disclose your personal information and provides information about your privacy rights.

We may collect, hold, use and disclose personal information about you. We do this to:

- a. process your application, administer and manage the products and services sought by and provided to you, monitor, audit and evaluate those products and services, model and test data, communicate with and market to you, and deal with any complaints or enquiries
- b. monitor transactional patterns on your Account(s) that may materially affect your ability to meet your obligations under any credit facilities you hold with us.

You consent to us collating basic Account information such as transactional patterns, payment facility preferences, and general banking requirements, the details of which may be de-identified and used to prepare benchmarking statistics and reports on industry trends for dissemination to you and our other clients in your industry sector.

We collect and record personal information through our interactions with you, including by telephone, email or online. We may also collect personal information from public sources and third parties including information brokers and our service providers. Without this Information, we may not be able to process your application or provide you with an appropriate level of service.

Where you provide us with personal information about someone else you must first ensure that you have obtained their consent to provide their personal information to us based on this Privacy Statement.

We are required or authorised to collect your personal information under various applicable laws including the Anti-Money Laundering and Counter-Terrorism Financing Act, Taxation Administration Act, Income Tax Assessment Act, Corporations Act and the Foreign Account Tax Compliance Act (US), the Common Reporting Standards and any similar law of any country, and any related laws designed to implement those laws in Australia.

Disclosure of your information

We may exchange your personal information (including Account and transaction information) with other companies in the Macquarie Group, our credit reporting and debt collection agencies, other financial institutions (such as banks), your authorised agents, advisers and accountants and our service providers which are described further in our Privacy Policy. For example, we may disclose to other companies in the Macquarie Group Information necessary to enable an assessment of your total liabilities to us and that company.

We may also disclose personal information (including Account and transaction information) to regulatory authorities (eg tax authorities in Australia and overseas) in connection with their lawful information requests or to meet our legal obligations in any relevant jurisdiction.

In providing you with our services, we may also disclose and exchange personal information with third parties that operate outside of Australia (this includes locations in India, the Philippines and the countries specified in our Privacy Policy). Where this occurs, we take steps to protect personal information against misuse or loss.

You consent to us providing a banker's opinion or banker's reference to any other bank or financial institution, or to any third party from whom we receive a request for an opinion or reference about you at any time.

Marketing

We and other companies in the Macquarie Group may use your personal information to contact you on an ongoing basis by telephone, electronic messages (like email), online and other means to offer you products or services that may be of interest to you, including offers of banking, financial, advisory, investment, insurance and funds management services, unless you change your marketing preferences by telephoning us or visiting [macquarie.com.au/optout-bfs](https://www.macquarie.com.au/optout-bfs).

Your rights and further details

Under the Privacy Act, you may request access to your personal information that we hold. You can contact us to make such a request or for any other reason relating to the privacy of your personal information by telephoning us on 1300 550 415 or emailing privacy@macquarie.com. Please mark communications to the attention of our Privacy Officer.

You may also request a copy of our Privacy Policy which contains further details about our handling of personal information, including how you may access or update your personal information and how we deal with your concerns. The Privacy Policy can be found via [macquarie.com](https://www.macquarie.com).

Data to third parties

We may send information about your Account to third parties who require it to provide services in relation to your Account, in accordance with our Privacy Policy which is available online.

We do not accept liability for any loss incurred by you as a result of the use of information about your Account by third party service providers, unless such losses are due to our negligence or fraud.

Terms and conditions

These terms and conditions apply to the operation and features of the Account, subject to the relevant provisions of the *Banking Code of Practice* adopted by Macquarie Bank Limited.¹

1. Definitions

Capitalised terms have the following meanings:

- 1.1 **Account** means a Macquarie Cash Management Account.
- 1.2 **ADI** means any bank, building society, credit union or other authorised deposit-taking institution within the meaning of the *Banking Act 1959 (Cth)*.
- 1.3 **Adviser Initiated Payments** is an Electronic Banking service provided by us that enables an Authorised User to initiate and complete a Payment from your Account on your behalf, with your consent, via the use of a Secure Code, which must be provided verbally to your Authorised User.
- 1.4 **Authorised User** means a person authorised by you to access and/or transact on your Account(s) via Electronic Banking in accordance with clause 6.
- 1.5 **Biller** means an organisation which tells you that you can make payments to them through the BPAY[®] Scheme.
- 1.6 **BPAY Scheme** means a service which allows payments to be made electronically to Billers.
- 1.7 **Business Day** means every weekday except for Australian national public holidays.
- 1.8 **Destination Account** means the bank account with the BSB and account number into which the Payment, the subject of the Adviser Initiated Payment, is to be transferred.
- 1.9 **Electronic Banking** means all or any of Online Banking, Mobile Banking and Telephone Banking as relevant.
- 1.10 **Financial Services Professional** means an adviser, accountant, administrator, stockbroker, risk specialist, mortgage broker, intermediary or any person that acts on behalf of a Company.
- 1.11 **Lodgement time** means the time by which payments and deposits need to be made on a Business Day.
- 1.12 **Login Details** means the user information necessary to access your Account or information about your Account electronically. Login Details include, without limitation your Macquarie ID and any Secret Codes required to access Electronic Banking services.
- 1.13 **Macquarie ID** is a unique code allocated to you or an Authorised User by us which identifies you or the Authorised User and when used in conjunction with a Secret Code provides access to Electronic Banking.
- 1.14 **Macquarie Group** refers to Macquarie Bank Limited and its related entities.
- 1.15 **Materials** means any proprietary and confidential information including messages, files, data, software, images, photographs, illustrations and text contained on Online Banking and Mobile Banking.
- 1.16 **Mistaken Internet Payment** means a Pay Anyone Payment where the funds are paid into the account of an unintended recipient because a BSB, account number and/or other identifier that does not belong to the intended recipient was entered as a result of:
 - you or an Authorised User's error, or
 - you or an Authorised User being advised of the wrong BSB, account number and/or other identifier.
- 1.17 **Mobile Banking** means Macquarie's secure mobile banking service that allows you (and certain third parties authorised by you in accordance with clause 6) to access certain banking services through a smartphone application on compatible mobile phones or personal electronic devices.
- 1.18 **Mobile Device** means a mobile phone or another type of personal electronic device which is able to access Mobile Banking.
- 1.19 **Nominated Account** means a bank account held with Macquarie or another financial institution nominated by you in writing to transfer funds to, via Electronic Banking.
- 1.20 **Online Banking** means Macquarie's secure online banking services, Macquarie Online.
- 1.21 **Password** means a security password which is issued by us, or selected by you or an Authorised User which enables access to Electronic Banking.
- 1.22 **PayAnyone Payment** means a payment that can be made through Online Banking and Mobile Banking which is processed via direct entry involving the transfer of funds from an Account to another person's account held with Macquarie, or to an account held by you or another person with another ADI.
- 1.23 **Payment** means a payment of any type including by BPAY, funds transfer, Scheduled Funds Transfer, PayAnyone or by any other method allowed by Macquarie from time to time.
- 1.24 **PIN** means the optional four-digit code you or an Authorised User select to access either Telephone Banking or Mobile Banking.
- 1.25 **Recipient** means any person or entity who receives a payment by any payment method, including BPAY billers and people receiving money from you by funds transfer or PayAnyone.
- 1.26 **Scheduled Funds Transfer** means a funds transfer on a future date, including on a recurring basis.
- 1.27 **Secret Code** means individually and collectively any Login Details which we require you or an Authorised User to keep secret, including any Password, PIN or SMS Code.

¹ This is a banking service to which the Banking Code of Practice ("BCOP") applies. The BCOP is an industry code which sets standards of good banking conduct for banks, their staff and their representatives. The BCOP will come into affect and apply to these terms and conditions from 1 July 2019 if you are an individual or a small business (as defined in the BCOP).

- 1.28 **Secure Code** means a code we send by SMS to your mobile phone for you to provide consent and authorisation of a Payment from your Account initiated by your Authorised User via Adviser Initiated Payments.
- 1.29 **SMS** means a service of sending short messages to a Mobile Device.
- 1.30 **SMS Code** means a code we send by SMS to you or your Authorised User's Mobile Device.
- 1.31 **Telephone Banking** means Macquarie's telephone banking services.
- 1.32 **Third Party Website** means a website relating to a product or service which is not our product or service, but which may be displayed and accessible through Online Banking or Mobile Banking.
- 1.33 **We, our, us or Macquarie** refers to Macquarie Bank Limited.
- 1.34 **Withdrawal** means any withdrawal of funds from your Account.
- 1.35 **You** means you the Account holder(s). Where the context permits it also includes any person carrying out any Account transaction on your behalf, for example a person to whom you have given third party access.

2. Variations

We may change these terms and conditions and the other information contained in the Product Information Statement and *Fees, limits and lodgement times* in our reasonable discretion at any time. The minimum notice for any variations to your Account is set out in the below table.

3. Sufficient funds

- 3.1 Where you specify a future date for a withdrawal, we may decline any other withdrawal request that would leave insufficient funds to cover those obligations.

- 3.2 We may not accept transfer or payment instruction from you if the funds in your Account available for withdrawal are insufficient to cover the amount to be transferred.
- 3.3 We may dishonour any withdrawal, if there is insufficient funds in your Account at the time of withdrawal. We may determine the order of priority of monies paid.

4. Interest

- 4.1 For the current interest rate(s) applicable to you, please visit macquarie.com/personal, contact your financial services professional or check your statement. The rate is variable and is subject to change.
- 4.2 Interest is calculated by dividing the current interest rate by the number of days in the year (365 or 366 in a leap year) and multiplying by the daily closing balance, which is the credit balance of your Account at the end of a day.
- 4.3 Where we tell you that stepped interest applies to your Account, the interest earned is calculated according to the sum of the daily closing balance within each applicable step (depending on the amount in Account) multiplied by the interest rate applicable to that step divided by the number of days in the year.
- 4.4 Interest is calculated on Business Days for that day and all days up to the next Business Day, including any days belonging to the next month. The calculated interest for these days are added, and then rounded up or down, subject to clause 4.5, and accrued until payment.
- 4.5 Interest accruals are rounded up or down to the nearest cent:
 - 0.5 cent or more is rounded up, and
 - less than 0.5 cent is rounded down.
- 4.6 All interest payments will be paid on the last Business Day of the month for all interest accrued for that month.

Variations		
Minimum notice	Days	Method of notice
Introduce a new fee or charge, including but not limited to a fee relating to the use of Electronic Banking (other than a government charge payable directly or indirectly by you)	30	In writing or electronically
Increase a fee or charge (other than a government charge)	30	In writing, electronically, by press advertisement or in any other way permitted by law
Change the method by which interest is calculated	30	In writing or electronically
Change the frequency with which interest is debited or credited	30	In writing or electronically
Change to any other term or condition (apart from the introduction or variation of a government charge payable directly or indirectly by you)	No later than day of change	In writing, electronically, by press advertisement or in any other way permitted by law
Change increasing your liability for losses relating to transactions conducted via Electronic Banking	20 days	In writing or electronically
Impose, remove or adjust a daily or other periodical transaction limit that applies to the use of Electronic Banking	20 days	In writing or electronically
Government charges	In advance of the change or as soon as practicable after, unless the change has been publicised by the Government	In writing, electronically or by press advertisement

5. Instructions

- 5.1 Macquarie may, in its absolute discretion accept and refuse Account instructions, verbal, written or other electronic requests as Macquarie determines from time to time.
- 5.2 You acknowledge that Macquarie is entitled to rely on, and you will be liable for, any instructions which are received electronically, which appear to have been duly authorised by you. By providing instructions in this way you acknowledge there is an increased risk of fraud, you release us from, and agree to reimburse us for, any losses and liabilities arising from any payment or action we make in this respect, provided we have acted reasonably but without fraud and negligence.
- 5.3 We reserve the right to add further requirements at any time where we consider these to be reasonably necessary to protect your Account.
- 5.4 You authorise and direct us to act on any instructions given to us by a user or a person using your Login Details and you are liable for any such instructions. We may reasonably delay acting on, or may ask you for further information before acting on, an instruction.
- 5.5 You authorise us to accept any instruction that has not been cancelled by you and notified to us prior to us acting on that instruction.



Please be careful! There is a risk that fraudulent electronic withdrawal requests can be made by someone who has access to your Account number, your signature or your Login Details. From time to time we may verify these requests with you and reserve the right to deny the request.

6. Authorising a third party to access your Account

We offer a facility where you may authorise a company, firm or another person to have access to or withdraw from your Account. You can revoke these authorities at any time by contacting us on 1800 806 310. We will update this in accordance with the signing instructions on your Account.

There are six types of authority:

- Enquiry Authority
- Fee Authority
- Government/Tax Payment Authority
- General Withdrawal Authority
- Authorised Signatory, and
- Limited Third Party Authority.

The rights and obligations attaching to each level of authority are described in these terms.



Please consider carefully who you appoint as a third party authority on your Account as we may follow their instructions as if they were yours. It is important that you understand this risk and carefully consider what level of authority you give to them.

General terms which apply to all levels of third party authority

- 6.1 Only you may appoint a third party to access or withdraw from your Account.
- 6.2 If you appoint a third party to withdraw from your Account they will automatically be able to enquire on your Account also.
- 6.3 We can impose conditions at any time (acting reasonably).
- 6.4 You acknowledge and agree that these terms apply to the third party you appoint in the same way that they apply to you. You must ensure that every third party has read and complies with these.
- You will be in breach of these terms if any third party does not comply with these.
- 6.5 This authority takes effect on the date when we amend our records to note the appointment of the third party. This continues until we cancel it or you cancel it by contacting us. Cancellation takes effect on the date when we amend our records to note the change.
- 6.6 We will notify you if we cancel the appointment of a third party.
- 6.7 We will cancel the authority given to a third party if we are notified of the death, bankruptcy or loss of capacity of either you or the third party.
- 6.8 Third parties can not set up direct debits on your Account or give other third parties access or authority on your Account.
- 6.9 Where you give authority to a company or firm:
- a. the company or firm will give us details of people who can transact on its behalf
 - b. you acknowledge and agree that the company or firm may do this and the people they nominate can access your Account according to the authority you have given to them
 - c. we will only act on withdrawal requests from the company or firm, if the person requesting the withdrawal has been nominated by it in accordance with our procedures, and
 - d. the company or firm must contact us if any nominated person no longer has authority. If you change adviser or cease using one, you should ensure you contact us immediately to cancel their authority. Otherwise, that person may still be able to operate your Account.
- 6.10 You acknowledge and agree that if the third party appointed by you does not comply with these terms, we may unilaterally cancel the person's authorisation, suspend, freeze or block your Account.
- 6.11 You release us from all claims and liabilities in relation to your Account resulting from the appointment of any third party, including your Financial Services Professional or any person nominated by them, as well as their use of Adviser Initiated Payments.
- However we remain liable for any loss or liability which:
- a. arises as a result of our negligence, or
 - b. by operation of law we cannot exclude.

Terms relating to each of the levels of authority

6.12 Enquiry Authority

- a. You authorise the third party to have access to information about your Account.
- b. Enquiry Authority does not allow the third party to make withdrawals from your Account, changes to your Account details, close your Account or enable the use your cheque book.

6.13 Fee Authority

You authorise your Financial Services Professional to withdraw their fees from your Account. Where you choose to grant this level of authority, we recommend you regularly check your statement of advice, fee disclosure statement or other documentation that sets out your fee arrangement with your Financial Services Professional to ensure the correct amounts are being withdrawn.

6.14 Government/Tax Payment Authority

You authorise the third party to withdraw funds from your Account to make payments on your behalf directly to government departments or agencies.

6.15 General Withdrawal Authority

- a. You authorise the third party to make payments and withdrawals in accordance with the terms set out under 'Fee Authority' and 'Government/Tax Payment Authority' above.
- b. In addition, you authorise the third party to make payments and withdrawals for any purpose.
- c. General Withdrawal Authority does not authorise the third party to make any changes to your Account details, close your Account or enable the use of your cheque book.
- d. Your Financial Services Professional reserves the right to hold funds from the time the order is placed or the time of execution to settle trades.

6.16 Authorised Signatory

- a. You authorise the third party to make payments and withdrawals according to the General Withdrawal Authority terms above.
- b. In addition, this authority also allows the third party to use your cheque book, change your Account details (subject to the signing instruction) and to close your Account. This authority does not allow the authorised signatory to appoint other authorised signatories.

6.17 Limited Third Party Authority

- a. You authorise the third party to have access to information about your Account.
- b. You authorise the third party to establish a new Macquarie Bank Term Deposit in the same name as your Account and funds will be debited from your Account.
- c. Your authorised third party cannot otherwise transact, change details on your Account, use your cheque book, or close your Account.

6.18 Adviser Initiated Payments

Adviser Initiated Payments is a digital solution to enable your Financial Services Professional to initiate Payments on your behalf. You must provide a verbal authorisation of the Payment. Once you provide the Secure Code to your Financial Services Professional, they become an Authorised User on this transaction.

- a. When your Financial Services Professional request a Payment on your Account, we will send you a Secure Code via SMS to your mobile you provide to us.
- b. It is your responsibility to ensure that your mobile number that you provide us is kept up to date.
- c. Where you provide the Secure Code to your Financial Services Professional, you consent to the Payment being made to the Destination Account.
- d. If the Secure Code inputted by your Financial Services Professional matches the Secure Code that we have provided, then the Payment will be completed.
- e. We will provide you or a person you authorised with SMS and email confirmation of the authorised Payment. Please aware of any contact details attached to the Account as they will all receive this confirmation.
- f. Where an initiated Payment is a Scheduled Funds Transfer, it will remain in effect until it is revoked or otherwise terminated by you, your Financial Services Professional or by us.

6.19 Bulk transacting by a Financial Services Professional

Bulk transacting is an administration tool we provide to your Financial Services Professional. The tool helps them efficiently collect fees and make bulk payments from multiple Accounts that they or various Financial Services Professionals working for the same firm may have with us. We only permit this tool where you have provided the required level of authority over your Account to your Financial Services Professional. There are no fees or charges to you for the use of bulk transacting by your Financial Services Professional.



Please check the transactions on your Account carefully. If you suspect any error or unauthorised transaction please promptly notify us.

7. Cheque book

- 7.1 You must wait three Business Days before drawing against cheques you have deposited.
- 7.2 We may deduct fees for the operation of your cheque book from your Account, including fees for dishonoured cheques.
- 7.3 To the extent permitted by law, you release us from claims and liabilities in connection with any act or omission relating to the operation of your cheque book.
- 7.4 We may cancel your cheque book if you do not comply with any of these terms, but we will endeavour to give you reasonable notice. Please destroy any unused cheques.
- 7.5 We may dishonour a cheque you have written for a number of reasons, including where:
 - a. there are insufficient funds in your Account
 - b. the signature is not valid or the cheque is unsigned

- c. the cheque is presented over 15 months after its date
- d. alterations on the cheque have not been signed by you
- e. the cheque is presented before the date written on it
- f. you have asked us to cancel the cheque, or
- g. we have received notice of your death, loss of capacity or bankruptcy.

Dishonour cheque may be subjected to a fee set out in *Fees, limits and lodgement times*.



You must contact us immediately if you would like to cancel a cheque, your cheque book is lost or stolen, or you suspect an unauthorised cheque transaction. If you do not, you must be liable for cheque paid by us in good faith.

8. Liability for unauthorised transactions – cheques

An unauthorised cheque transaction is a transaction not authorised by you or your authorised third party, or is executed without your knowledge or consent.

- 8.1 You will not be liable for any unauthorised cheque transaction where:
 - a. there was fraudulent or negligent conduct by us
 - b. a forged, faulty, expired or cancelled cheque book was used, or
 - c. it is clear you have not contributed to the loss resulting from the unauthorised transaction.
- 8.2 You will be liable for losses resulting from unauthorised cheque transactions where we can prove that you contributed to the loss by:
 - a. acting fraudulently,
 - b. not keeping your cheque book secure, or
 - c. unreasonably delaying notifying us after becoming aware of the loss, theft or unauthorised use of your cheque book.

9. Electronic Banking

We provide secure Online Banking, Mobile Banking and automated Telephone Banking services, which enable you to access information about your Account, update aspects of that information and make payments to other accounts.

The first use of any Electronic Banking service will constitute your agreement to these terms.

9.1 Online Banking, Mobile Banking and Telephone Banking

a. Online Banking

Online Banking is a service which enables you or an Authorised User to access and/or transact on your Account over the internet.

b. Mobile Banking

Mobile Banking enables you or an Authorised User to access and/or transact on your Account, using a Mobile Device with internet connectivity. Mobile

Banking will be available to you by downloading Macquarie's Banking App to your Mobile Device. Full Mobile Banking functionality may not be available for your Account as at the date of this Further Information Guide.

c. Telephone Banking

Telephone Banking is a service which enables you or an Authorised User to access and/or transact on your Account via a touch tone telephone.

9.2 Access

To access Online Banking, Mobile Banking, or Telephone Banking, you or an Authorised User will need a Macquarie ID, Password and/or PIN.

a. Online Banking

For Online Banking, you and each Authorised User will either be required to set your own Password or change a temporary Password that we send you.

There may be times when Online Banking is unavailable from some computers and devices, for example, due to hardware or software restrictions or problems with internet connectivity. You and your Authorised Users are responsible for obtaining access to Online Banking. Specifically, you and your Authorised Users are responsible for all equipment necessary to access Online Banking. The system requirements to access Online Banking are set out in the Important Information Statement (available online).

b. Mobile Banking

To first access Mobile Banking you or an Authorised User will need to use a Macquarie ID and Password. You and any Authorised User can then select a four digit PIN for your Mobile Device and use it in place of using a Macquarie ID and Password each time.

If the technology is available on your Mobile Device, you may be able to sign into Mobile Banking using a fingerprint or other biometric authentication stored on your Mobile Device as an alternative to signing in with your Macquarie ID and Password or PIN. You may turn this option on or off at any time using the Settings menu within Mobile Banking.

c. Telephone Banking

To access Telephone Banking (sometimes referred to as Macquarie PhoneLink) you or an Authorised User will need to call 133 275. You or an Authorised User will then need to log on using a Macquarie ID and PIN and follow the instructions given.

9.3 Funds transfer

You or an Authorised User may be able to transfer funds from your Account to another bank account through Electronic Banking. Enhanced security measures may be required for certain payments. See clause 9.8 for further details.

We do not carry out checks to determine if the details provided in a funds transfer instruction are correct. For example, we do not check that the BSB and account

numbers provided correspond with the account name of the payee.

Once a funds transfer instruction has been accepted by us, it cannot be cancelled except if it is a Scheduled Funds Transfer.

Scheduled Funds Transfers

You or an Authorised User can arrange to make a Scheduled Funds Transfer.

Instructions for a Scheduled Funds Transfer will remain in effect until they are revoked or otherwise terminated by you or us.

You may modify or cancel a Scheduled Funds Transfer by making the required change(s) in Electronic Banking by the relevant cut off time. Scheduled Funds Transfers set up by written request cannot be changed via Online or Mobile Banking.

Please refer to the *Fees, limits and lodgement times* for scheduled processing times and relevant cut off time.

Mistaken payments

9.4

A Pay Anyone Payment that is made by you or an Authorised User to an unintended recipient is referred to as a Mistaken Internet Payment.

a. Mistaken Internet Payments made by you or an Authorised User

You or your Authorised Users should report Mistaken Internet Payments by calling us as soon as possible as delays may impact on our ability to recover the funds on your behalf.

We will need to collect information from you or an Authorised User that will allow us to investigate and determine whether a Mistaken Internet Payment has occurred. We will provide a reference number, or some other form of acknowledgement, which should be retained as evidence of the date and time of the report.

If we are not satisfied that a Mistaken Internet Payment has occurred, we will not take further action and you will be liable for the loss arising from the payment.

If we are satisfied that a Mistaken Internet Payment has occurred, we will send a request for the return of the funds to the ADI whose customer received the payment (known as the **receiving ADI**).

Sending this request to the receiving ADI requires us to disclose information to that ADI about your Account and the Mistaken Internet Payment.

If the receiving ADI is also satisfied that a Mistaken Internet Payment has occurred and there are sufficient funds available in the unintended recipient's account, the receiving ADI will attempt to recover the funds and return them to us and we will credit them to your Account. The following process will apply where:

- the Mistaken Internet Payment is reported to us within 10 Business Days after the payment is made, the receiving ADI is required to return the funds to us within 5 to 10 Business Days of receiving our request

- the Mistaken Internet Payment is reported to us between 10 Business Days and 7 months after the payment is made, the receiving ADI will give the unintended recipient 10 business days to establish that they are entitled to the funds, and if they do not, the receiving ADI will return the funds to us within 2 Business Days of the expiry of that period and
- the Mistaken Internet Payment is reported to us more than 7 months after the payment is made, the receiving ADI will ask the recipient if they agree to the return of the funds to us.

If the receiving ADI is satisfied that a Mistaken Internet Payment has occurred but there are insufficient funds in the unintended recipient's account, the receiving ADI will use reasonable endeavours to obtain a refund for you (for example, by facilitating repayment of the funds by the recipient through instalments).

If the receiving ADI is not satisfied that a Mistaken Internet Payment has occurred, it may (but it is not obliged to) seek the consent of the recipient to enable the return of funds to us.

You will be notified in writing, within 30 Business Days of receipt of the report of a Mistaken Internet Payment from your Account, of the outcome of our investigation. If you are not satisfied with how the report is handled by us, you can make a complaint.

b. Mistaken payments received by you

You may receive funds into your Account where you are not the intended recipient due to a sender entering the wrong details when making an internet payment. This clause applies to that situation.

If you become aware of any payments into your Account of which you are not the intended recipient, please contact us as soon as practical.

Where we receive a request for the return of funds from an ADI whose customer reports a mistaken payment into your Account, we are satisfied that a mistaken payment has occurred, and there are sufficient funds in your Account, we may:

- debit your Account with the amount of the mistaken payment without notifying you or obtaining your consent (if the sender reports the mistake within 10 Business Days of the payment), or
- restrict your access to the funds and give you 10 Business Days to establish that you are entitled to the funds before debiting the Account (if the sender reports the mistake after 10 Business Days but within 7 months of the payment).

Otherwise, we will seek your consent to return the funds.

If we are satisfied that a mistaken payment has occurred, but the balance of your Account is less than the amount of the mistaken payment, we will contact you to discuss how best to facilitate repayment to the sender.

Where we are unable to determine that the payment was a result of a mistaken payment, we may still contact you to seek your consent to the return of the funds.

Notwithstanding the above provisions, if you are a recipient of income support payments from Centrelink, we will only seek to recover the funds from you in accordance with the Code of Operation for Centrelink Direct Credit Payments.

9.5 BPAY payments

You or an Authorised User may be able to make BPAY payments to Billers (which may include us) from your Account through Electronic Banking. Macquarie is a member of the BPAY Scheme and will tell you if it is no longer a member.

BPAY payments can be made from your Account and can be made immediately or on a date up to 12 months in the future.

Some Billers will not accept BPAY payments from certain account types and others may have restrictions on the amount that can be paid by BPAY.

Enhanced security measures may be required for certain BPAY payments. See clause 9.8 for further details.

You can request access to your information held by BPAY by emailing privacy@bpay.com.au, or by referring to the procedures set out in the BPAY privacy policy which can be found at www.bpay.com.au/Privacy.aspx. BPAY's privacy policy contains information about how you may complain about a breach of the *Privacy Act 1988 (Cth)*, and the process by which your complaint will be handled.

a. Processing instructions

To make a BPAY payment from your Account, you or an Authorised User will need to provide the following details:

- the Account from which the BPAY payment is to be made
- the Biller code, and
- the Customer Reference Number (CRN).

We'll debit your Account with the bill amount that you specify.

Except for a scheduled payment (please refer to the *Fees, limits and lodgement times*), a BPAY payment instruction cannot be cancelled.

If we are advised that a BPAY payment cannot be processed by a Biller, we will notify you, credit your Account with the amount of the BPAY payment and take all reasonable steps to assist you in any further attempt to make the BPAY payment.

When we make a BPAY payment we are not acting as your agent or the agent of the Biller to whom the payment is directed.

b. Scheduled BPAY payments

You and your Authorised Users can arrange for a BPAY payment to be made up to 12 months in the future. Some Billers do not allow for recurring

payments to be set up; we will notify you at the time of setting up the transaction if this is the case.

A scheduled BPAY payment may not be processed for a number of reasons, including:

- the Biller no longer participates in the BPAY Scheme
- there are insufficient cleared funds in your Account on the day the payment is scheduled, or
- the payment would cause your daily BPAY transaction limit to be exceeded.

For scheduled processing times, please refer to the *Fees, limits and lodgement times*.

c. Mistaken BPAY payments

Care should be taken by you and Authorised Users to enter the correct amount and Biller's details. If the amount entered is greater than intended, you or the Authorised User must contact the Biller to obtain a refund. If less, another BPAY payment can be made to make up the difference.

If you or an Authorised User told us to pay the wrong Biller and we cannot recover the amount within 20 Business Days, we will seek this amount from you. The receipt by a Biller of a mistaken or erroneous payment does not satisfy the debt owed between you and the Biller.

You should check your Account carefully and promptly report to us any BPAY payments you think are errors or that were not authorised by you or an Authorised User. The longer the delay in notifying us of the error, the more difficult it may be to correct this. You may need to liaise directly with the Biller to correct the error if, for example, because of delay, we no longer have sufficient information to investigate it.

For us to investigate a BPAY payment from your Account that may be unauthorised, you or an Authorised User must first give us your consent, addressed to the Biller who received that BPAY payment, authorising us to obtain information about your account with that Biller, or the BPAY payment. You will need to include your CRN and any other information we require. If you do not give us the consent, the Biller may not be permitted under law to disclose to us the information we need to investigate or rectify that BPAY payment.

If a BPAY payment was made to a person or for an amount not instructed by you or an Authorised User, and your Account was debited with the payment, we will credit that amount back to your Account.

Disputes in relation to unauthorised, fraudulent or wrong BPAY payments will be handled in accordance with the Macquarie Complaints Policy. Your liability for unauthorised and fraudulent BPAY payments will be determined in accordance with clause 9.9. No chargeback rights are available in respect of a BPAY payment from your Account.

Subject to law and to clause 9.9 as relevant, we are not liable for any consequential loss or damage you may suffer as a result of using the BPAY Scheme, other than due to our negligence.

d. **Fraud-induced BPAY payments**

You must tell us promptly if you think that you have been fraudulently induced to make a BPAY payment. We will attempt to rectify any such matters in relation to your BPAY payments in the way described in this clause.

If a BPAY payment is induced by the fraud of a biller or person involved in the BPAY scheme, then that biller or person should refund you the amount of the fraud-induced payment. However, while we would assist you to pursue a refund, if that person does not refund you the amount of the fraud-induced payment, you must bear the loss unless some other person involved in the BPAY scheme knew of the fraud or would have detected it with reasonable diligence, in which case that person must refund you the amount of the fraud-induced payment that is not refunded to you by the person that induced the fraud. You must exercise care about the biller you deal with, the security of your Login Details and the accuracy of your instructions to us.

9.6 **General information on transactions**

When you or an Authorised User make a transfer or a payment on your Account through Electronic Banking, the following general conditions apply:

- a. we will confirm the receipt of instructions to transact (although not the transaction itself)
- b. you should check your Account records carefully and report to us as soon as you become aware of any payments that you think have been made in error or which were not authorised (see clause 9.9 for liability for unauthorised payments)
- c. you should notify us promptly if you become aware of any delays or mistakes in processing transactions
- d. you authorise us, and we are entitled, to act upon any instruction received via Electronic Banking in conjunction with the correct Login Details and other terms agreed between you and us
- e. we will not be obliged to effect a payment instruction if:
 - i. it is not made in accordance with these terms and conditions or the payment is prohibited by these terms and conditions
 - ii. the information given to us, or requested by us, is incomplete and/or inaccurate
 - iii. we are restricted or prohibited by law, regulation, industry code, or the requirement of a government or similar authority from permitting the payment to occur
 - iv. the instruction is not accepted by our system
 - v. there is a technical failure of equipment, our system or outside our system, which causes a delay in the transmission or acceptance of the instruction
 - vi. the financial institution to which the payment is to be made does not accept it or delays accepting it
 - vii. your or an Authorised User's right to participate in Electronic Banking is suspended
 - viii. there are insufficient cleared funds in the Account from which the payment is to be made

to cover the amount of the payment on the day the payment is instructed to be made, or

- ix. the request would cause you to exceed any daily limit (on the day the payment is instructed to be made) we impose on your Account or your use of Electronic Banking
- f. we will perform a payment instruction as soon as possible, however we do not guarantee that any transaction we are instructed to make will be made on the day or at the time requested, and
- g. we have absolute discretion to determine the order in which we give effect to payment instructions received.

9.7 **Fees and charges**

There are no establishment or ongoing fees for accessing or using Electronic Banking.

However, access and use of the Electronic Banking services may involve third party fees, including from:

- internet service providers
- telecommunications providers for downloading or using Mobile Banking, or
- call costs associated with accessing Telephone Banking.

You should refer to the relevant third parties for details of their fees and charges.

There may also be fees and charges that apply to transactions conducted on your Account through Electronic Banking – refer to the *Fees, limits and lodgement times* for details.

Enhanced security measures

9.8

For certain activities on your Account, you or an Authorised User may be asked to comply with our enhanced security measures. Such circumstances may include when you or the Authorised User make a funds transfer to a new recipient, or make a BPAY payment to a new Biller.

Our enhanced security measures provide an additional layer of security to protect you and us from unauthorised transactions and fraud. The measures may change from time to time at our discretion and include any appropriate method of authentication, or contacting you to verify the transaction or activity on your Account.

Two-factor authentication, often referred to as "2FA", is an authentication process which uses two different layers of security to verify your identity. For instance, for Online Banking the first layer of authentication relates to your Login Details and a second layer of authentication is imposed when you or the Authorised User initiate certain transactions or perform certain activities on your Account. This additional layer of security may include, but is not limited to, the requirement to input an SMS Code, or answer security questions.

You or an Authorised User will be instructed to contact us to complete a transaction or other Account activity if any enhanced security measure is not successfully satisfied.

9.9 Liability for unauthorised transactions

You are not liable for loss arising from Electronic Banking transactions carried out using Login Details without your or an Authorised User's knowledge or consent (**unauthorised transactions**) that occurs after we have been informed that the security of a Secret Code has been breached.

9.10 Security

a. Security and Fraud

We are committed to providing the highest quality of financial services within a trusted environment. Please read the Security and Fraud statement available online, [macquarie.com/au/about/disclosures/security-and-fraud](https://www.macquarie.com/au/about/disclosures/security-and-fraud).

b. Equipment security

You and your Authorised Users must take all reasonable steps to protect the security of your respective computer hardware and software, and Mobile Device. Reasonable steps include:

- for computer hardware and software: protecting your computer from viruses and maintaining passwords
- for Mobile Devices: setting screen lock passwords and ensuring that others do not have access to the use of your Mobile Device.

You and your Authorised Users should log out from Online Banking and Mobile Banking at the end of each session.

For security purposes, we reserve the right at any time to log you and any Authorised Users out of Online Banking and Mobile Banking.

Where you or an Authorised User remove some system level restrictions on a Mobile Device by, for example, 'jailbreaking' or 'rooting' the Mobile Device, you release us from any loss arising from fraudulent activity carried out on the Mobile Device, including in respect of your Account.

It is important that, if you wish to use a fingerprint or other biometric authentication stored on your Mobile Device to log in to Mobile Banking, no such authentication other than your own are stored on your Mobile Device. If someone else's fingerprint is stored on your Mobile Device, that person may be able to view your Accounts and perform transactions in Mobile Banking. We will treat as authorised, and you will be responsible for, any Mobile Banking transactions performed using a fingerprint or other biometric authentication stored on your Mobile Device.

c. Security guidelines

The security of you and your Authorised User's Secret Codes is very important, as whoever has access to them may be able to perform transactions on your Account. These guidelines are designed to help you keep your and your Authorised User's Secret Codes secure.

By following these guidelines, you and your Authorised Users can assist in preventing unauthorised transactions on your Account.

These guidelines do not determine your liability for unauthorised transactions. Your liability will be determined under clause 9.9 and any applicable codes of practice to which we subscribe.

To protect your Secret Codes you and your Authorised Users should:

- not disclose any Secret Code to anyone, including a family member or friend
- take care to prevent anyone seeing a Secret Code entered into a computer, Mobile Device or telephone
- try to commit all Secret Codes to memory and not record them by any means (including by storing them on a computer or Mobile Device, or any article that could be accessed or stolen along with a computer or Mobile Device) without making a reasonable attempt to disguise them
- not choose a Secret Code which can be easily guessed including, for example, a Secret Code that uses repeated characters, consecutive numbers, or a Secret Code that represents a recognisable part of your or their name, birth date, telephone number or driver's licence number, and
- change all Secret Codes at regular intervals.

The following are not reasonable attempts at disguising a Secret Code:

- recording it in reverse order, as a telephone number or as a date (including a birth date) or as an amount, or
- recording the Secret Code in any other way that can be easily identified.

d. Reporting loss, theft or misuse of Secret Codes and devices

You or an Authorised User must immediately notify us if it is suspected that the security of a Secret Code or Mobile Device has been breached. You or an Authorised User must also promptly notify us of any unauthorised transactions on your account.

If we are unable to be contacted by phone because our lines are unavailable, you will not be liable for unauthorised transactions which could have been prevented had we been contactable, provided we are told within a reasonable time after our telephone facilities become available again.



Please contact us 24 hours a day, 7 days a week, by calling us on 13 31 74.

9.11 Suspension and termination

We may, acting reasonably, suspend and/or terminate your or an Authorised User's use of and access to Electronic Banking for any of the following reasons:

- breach or suspected breach of these terms and conditions or any other incorporated agreements or guidelines
- where we believe that use of Electronic Banking may cause loss to you or us
- to comply with our obligations under any applicable laws (including any Anti-Money Laundering or

Counter-Terrorism Financing laws and sanctions) or a court order

- fraud or suspected fraud
- requests by law enforcement or other government agencies, or
- unexpected technical or security issues or problems.

We will endeavour to give you reasonable notice of suspension or termination of your Account.

Please contact us to suspend your or an Authorised User's access to Electronic Banking.

9.12 Notices and Mobile Banking notifications

Where you agree that we may give all notices and other communications in connection with these terms and conditions electronically, we will do so:

- by emailing them to your last known email address or sending them through SMS to your last known mobile telephone number, or
- by making them available online.

Where communications are made available online, we may notify you of this fact by email or SMS.

You should check your emails and SMS messages regularly.

We may use push notification technology to deliver certain information concerning your Account directly to your compatible Mobile Device – for example when you make a transaction on your Account. You can turn these notifications on or off at any time using the Settings menu within Mobile Banking. If you have Mobile Banking notifications turned on, we may use this service to deliver: information concerning your Account, service or security announcements, advise that a new version of Mobile Banking is available, and/or marketing and other communications as described above.

Mobile Banking notifications are offered for your convenience and, when received in relation to a particular transaction, are not a receipt for that transaction. Depending on the notification settings you have chosen on your Mobile Device, other people with access to your Mobile Device may be able to view Mobile Banking notifications for your Accounts availability of the Mobile Banking notification service at any time, on a temporary or permanent basis, without notice to you.

9.13 Updating your contact details and tax residency information

You must ensure that the contact details and tax residency information that you provide to us, including your mobile number, email address and whether you become or cease to be a foreign tax resident, remain up to date.

If your details change, you must let us know as soon as possible by contacting us.

9.14 Availability of Electronic Banking

We will use reasonable efforts to ensure that access to Electronic Banking is available on a 24 hour continuous basis. However, this may not always be possible.

9.15 Marketing and other communications

You acknowledge that use of Electronic Banking may involve certain communications from us, such as service announcements, administrative messages and marketing material and that these communications are considered part of the Electronic Banking service.

9.16 Macquarie Marketplace Terms of Use

When you select 'Purchase' you're agreeing to the below terms of our Macquarie Marketplace service:

- Macquarie Marketplace is a distributor of third-party retailers' eGift cards. Macquarie earns a margin on the purchase of the cards
- your purchase of an eGift card is final – the purchased eGift card cannot be returned or cancelled
- retailers are responsible for all aspects of their eGift cards and programs and we cannot resolve any dispute between you and the relevant retailer
- you are responsible for the use and safety of your eGift card so please treat your eGift card like cash and keep your eGift card email secure.

10. Direct Debit Request Service Agreement

By completing a *Direct Debit Request* form, you authorise and request us to debit funds from the account you nominate, in accordance with the following terms:

- a. the account held by your nominated financial institution must be in the same name or names as your account
- b. where the due date for a debit does not fall on a Business Day, your nominated financial institution may vary the timing of the debit. If you are uncertain as to when a debit will be processed, you should ask that financial institution
- c. you must allow two Business Days for funds deposited through the Direct Debit service to be cleared
- d. third parties authorised to transact on your account can not set up a Direct Debit on your behalf, but are allowed to reduce or cancel the existing regular Direct Debit on behalf of you
- e. you must notify us immediately if you know or suspect any unauthorised transactions have occurred in relation to your Direct Debits. You should also notify your other financial institution as soon as possible
- f. you must notify us immediately, and confirm that notice as soon as is possible, if you believe that there has been an error in debiting your account. If we conclude as a result of our investigations that your account has been incorrectly debited, we will respond to your query by adjusting your account accordingly. We will also notify you of the amount by which your account has been adjusted. If we conclude as a result of our investigations that your account has been correctly debited we will respond to your query by providing reasons and evidence of this finding
- g. you must ensure that there are sufficient cleared funds in your nominated account(s) to honour your Direct Debit request

- h. you must ensure that the authorisation given to debit your nominated account is identical to the account signing instructions held by the financial institution where your nominated account is held
- i. your nominated financial institution(s) may decide the order of priority of payment by it of any monies
- j. your nominated financial institution(s) may at any time by notice terminate this request by notifying you or us in writing
- k. we may, by 14 days prior notice in writing to you, vary the timing of future debits, or any of the terms of this clause
- l. you can modify or defer your use of the Direct Debit service at any time by contacting us. Your request will normally be processed within seven days
- m. you can stop a particular debit or cancel your Direct Debit at any time by contacting us with seven days notice. You can also contact your nominated financial institution
- n. when your account is closed, all regular deposits under the Direct Debit service will cease
- o. your use of the Direct Debit service may be automatically cancelled if three consecutive direct debit payments are dishonoured due to insufficient funds in your nominated account. If this occurs, we will notify you that your use of the service has been cancelled. We will also charge to your account the cost of any dishonour costs
- p. you acknowledge that we may be required to reveal details of your Direct Debit Request to our service providers to assist with the checking of any incorrect or wrongful debits to your nominated account. In all other circumstances, we will keep all information relating to your Direct Debit arrangements private and confidential unless otherwise required by law
- q. you authorise the external financial institution(s) nominated on the *Direct Debit Request* form to confirm the BSB, account number and account name to us if required
- r. direct debit requests through the Bulk Electronic Clearing System (BECS) are not available on all accounts. You should check your account details against a recent statement. If you are uncertain about these matters, you should contact your nominated financial institution, and
- s. the provider of your nominated bank account may charge you fees if your Direct Debit request dishonours

11. Suspension

- 11.1 We may suspend, freeze or block the operation of your Account at any time in our reasonable discretion. Examples of where this may occur include the following:
 - a. if you or the third party appointed by you breach any of the terms
 - b. if we reasonably consider that you or any third party authorised by you acts fraudulently or is in breach of any law
 - c. if we reasonably believe that your Account is being used in a way that may cause loss to you or us

- d. if we believe that it is necessary to do so to comply with the law or applicable code.

12. Anti-Money Laundering

- 12.1 You must not knowingly do anything to put us in breach of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, rules and other subordinate instruments (AML/CTF Laws). You will notify us if you are aware of anything that would put us in breach of AML/CTF Laws.
- 12.2 If requested you must provide additional information and assistance and comply with all reasonable requests to facilitate our compliance with AML/CTF Laws, an equivalent law in an overseas jurisdiction, and/or its internal policies and procedures.
- 12.3 You undertake that you are not aware and have no reason to suspect that:
 - a. any deposit to the Account is derived from or related to money laundering, terrorism financing or similar activities (Illegal Activities), or
 - b. proceeds of withdrawals from the Account will fund Illegal Activities.
- 12.4 You acknowledge that we are subject to AML/CTF Laws and/or its internal policies and procedures.
- 12.5 In certain circumstances we may be obliged to suspend, freeze or block an account where it is used in connection with Illegal Activities or suspected Illegal Activities. Freezing or blocking can arise as a result of the account monitoring that is required by AML/CTF Laws and/or its internal policies and procedures. If we freeze or block your Account because we believe on a reasonable basis that we are required to do so in order to comply with AML/CTF Laws and/or our internal policies and procedures, we are not liable to you for any consequences or losses whatsoever including where we are found liable to a third party in connection with the freezing or blocking of your Account.

13. Combining your accounts

- 13.1 We may, at any time combine the balances of two or more of your accounts held with Macquarie. For example, we may do this if one of your accounts is overdrawn or in debit and the other is in credit. However, we will not do this if for example, where:
 - a. we know the accounts are not held by you in the same capacity (for example, where you have personal account and also an account as trustee for someone else)
 - b. we have agreed to keep your accounts separate, or
 - c. we are bound by a code of conduct not to do so (such as the *Code of Operation for Centrelink Direct Credit Payments*).
- 13.2 We will inform you if we have combined any of your accounts. You should not treat your accounts as combined unless we have agreed to such an arrangement. In the event that your accounts are combined, we may continue to apply separate interest rates to percentages of the combined balance in accordance with previous arrangements.

- 13.3 We may close any or all of your accounts as if the combined accounts had at all times been a single account.

14. Changes to your Account

- 14.1 You promise that all particulars given to us are accurate and complete.
- 14.2 You agree to promptly notify us of any change in:
- your name, address, mobile number or email address
 - the authority of any third party, or
 - the contents of any application form or any other documents you provide us.
- 14.3 We will not be responsible for any errors or losses associated with changes to your Account where we have received no or inadequate prior notice.

15. Taxation

- 15.1 Your Tax File Number (TFN) is collected in accordance with the *Income Tax Assessment Act 1936* and the *Taxation Administration Act 1953*. Provision of a TFN or Australian Business Number (ABN) is not compulsory, however, if you do not quote your TFN (including both TFNs for joint accounts) or ABN or claim an exemption, tax may be withheld from the interest paid to you at the highest marginal tax rate plus the Medicare Levy. Declining to quote a TFN is not an offence.
- 15.2 If you are a non-resident of Australia for taxation purposes, you must provide us with your overseas residential address. Tax may be withheld on the interest you earn on your Account whilst you are a non-resident.

16. Costs and expenses

- 16.1 You agree to pay us all reasonable costs and expenses incurred by us in connection with:
- the exercise and preservation of our rights under these terms, and
 - any legal proceedings or disputes between you and a third party where we become involved in such proceedings or disputes.

These costs and expenses are payable on demand or when we debit the Account for them.

17. Your rights and our rights

- 17.1 To the extent allowed by law, you give up any right to set off any amounts we owe you against amounts you owe us.
- 17.2 If any provision of these terms becomes illegal, invalid or unenforceable in any jurisdiction, this will not affect:
- the validity or enforceability in that jurisdiction of any other provision of these terms, or
 - the validity or enforceability in other jurisdictions of that or any other provision of these terms.
- 17.3 We may close your Account if we believe you have:
- acted fraudulently
 - unlawfully misused your Account
 - acted in a way that could damage the reputation of the Macquarie Group
 - otherwise breached these terms.
- 17.4 We also retain the right not to accept an application that we decide we do not wish to accept.

18. Law and jurisdiction

These terms shall be governed in accordance with the laws of New South Wales.

If you are not a resident of Australia:

- you submit to the non-exclusive jurisdiction of the courts exercising jurisdiction in the state of New South Wales and any other court of any other jurisdiction notified to you by us for this purpose
- you agree, on request by us, to appoint an agent for service of process in Australia, and
- you consent to the service of process out of any courts in Australia by mailing this to you at your address given in the application form or to any appointed process agent.

19. General

- 19.1 We may assign or otherwise deal with our rights under these terms in any way we consider appropriate provided that we act reasonably.
- 19.2 If anything under these terms and conditions is required to be done on a day that is not a Business Day, Macquarie will, at its discretion, process these on the last preceding Business Day or the following Business Day.
- 19.3 Unless otherwise indicated, terms used in these terms and conditions have the same meanings as in the Product Information Statement.

20. Trustee representations, warranties and undertakings

This clause applies if you are trustee of a trust (the trust named in the application form being referred to as the Trust).

- 20.1 You, both as trustee of the Trust and in your own right, make the following representations and warranties:
- the relevant trust instrument is valid and complies with all applicable laws
 - you are properly appointed as trustee of the Trust, and
 - you comply with the terms of the Trust and your duties and powers.
- 20.2 Where you incur any obligation in any way relating to any asset which you hold as trustee, you incur that obligation both in your own right and in your capacity as trustee.

21. Foreign tax residency information – FATCA and CRS

- 21.1 You must not knowingly do anything to put Macquarie in breach of:
- sections 1471 to 1474 of the US Internal Revenue Code of 1986 (commonly known as FATCA), any associated regulations or official guidance, any agreement with the US Internal Revenue Service relating to FATCA or any Australian laws, regulations or official guidance relating to an intergovernmental agreement between the United States and Australia in connection with FATCA (FATCA Laws) or our internal policies and procedures; or
 - our obligations in relation to Common Reporting Standard under the *Taxation Administration Act 1953 (Cth)* (commonly known as CRS), any associated regulations or official guidance, the OECD Multilateral Competent Authority Agreement on Automatic Exchange of Account Information or

- any Australian laws, regulations or official guidance in connection with CRS (CRS Laws) or our internal policies and procedures.
- 21.2 You agree to provide to Macquarie all the information or assistance we may request at any time, (whether as part of the application process or otherwise) to ensure that we are able to comply with our obligations under the FATCA Laws, CRS Laws or our internal policies and procedures.
- 21.3 In making an application, you consent to Macquarie disclosing in connection with the FATCA Laws, CRS Laws or Macquarie's internal policies and procedures any of your Personal Information (as defined in the *Privacy Act 1988 (Cth)*).
- 21.4 Macquarie retains the right not to provide products or services to you where we decide, in our sole discretion, that we do not wish to provide, including where information has not been provided as required to comply with FATCA Laws or CRS Laws.
- 22. Electronic Message Service**
- 22.1 The Electronic Message Service (EMS) is a mechanism by which you are able to electronically receive information regarding contributions from your employer to your Self Managed Super Fund (SMSF), as required under the superannuation law. By providing our electronic service address to your employer, you are agreeing to be bound by these terms.
- 22.2 A contribution message (Message) is an electronic message sent to us by your employer providing details relating to a contribution payment made to your SMSF. Your employer is responsible for the content and accuracy of the information provided in the Message.
- 22.3 Receiving a Message does not ensure a contribution payment has been made. We recommend checking the sender of the message to be sure.
- 22.4 The EMS can be provided either by us or a third party service provider until there is a change in the law.
- 22.5 As part of the EMS we will accept Messages and may notify you when these become available by email or online. Relevant details of your contribution payments will be available via Electronic Banking and to any Financial Services Professionals with authority on your Account.
- 22.6 We will reject any Messages that cannot be matched to an Account.
- 22.7 We do not provide and are not responsible for:
- reconciling contribution payments to Messages or Messages to trustees of the SMSF, or
 - any reporting or consolidation of Messages, or
 - removing any Messages which are incorrect.
- In addition to the above, we are not responsible for any errors in the Message which do not allow us to match the Message to your SMSF.
- 22.8 You are responsible for:
- complying with all applicable laws relating to your SMSF, and
 - contacting the message sender if there are any errors with the information contained in the Message.
- 22.9 By providing our electronic message address to your employer you are providing consent for us to collect, hold, use and disclose any personal information contained in the Message in accordance with our Privacy Policy.

For more information about the Macquarie Cash Management Account:

Clients contact your Financial Services Professional, visit [macquarie.com/cma](https://www.macquarie.com/cma), email transact@macquarie.com or call 1800 806 310 (or +61 7 3233 8136, for overseas queries).

Financial Services Professionals visit [macquarie.com/advisers](https://www.macquarie.com/advisers), email adviser@macquarie.com or contact us on 1800 808 508.
