# Internet Banking
## Terms and Conditions

This document must be read in conjunction with IMB's Product Disclosure Statement (PDS) a copy of which can be obtained from www.imb.com.au, from any IMB branch or by calling 133 462. This document **does not** contain all the terms and conditions applicable to an Account or all the information we are required by law to give an account holder. For each account to which you have access through IMB's Internet Banking facility, please refer to the **Member Guide to Transaction Banking - Product Disclosure Statement** ('PDS') for the full terms and conditions relating to that product.

The sections from IMB's Product Disclosure Statement (PDS) that specifically apply to the use of IMB's Internet Banking facility for the products and payment facilities listed on Page 1 and 2 of IMB's **Member Guide to Transaction Banking - Product Disclosure Statement** ('PDS') are extracted in this document.

IMB's PDS consists of the following:

a) **Member Guide to Transaction Banking – Product Disclosure Statement**
b) **PDS - Fees, Charges and Limits**
c) **PDS - Interest Rates for IMB Products**
d) **Any other Supplementary PDS issued by IMB**

IMB offers an Internet Banking facility through its website at www.imb.com.au. You can use the Internet Banking facility to:

- obtain information on your Accounts;
- transfer money between your Accounts;
- deposit money to third party Accounts;
- to make BPAY® and Osko® Payments; and
- to manage PayTo® Agreements.

IMB may also make available Mobile Banking which allows you to access the Internet Banking facility in a user friendly way from your mobile device.

These Internet Banking Terms and Conditions do not apply if you use IMB's Mobile Banking App to access your Accounts. For the terms and conditions that apply to IMB's Mobile Banking App, **please refer to the Mobile Banking App Terms and Conditions on our website.**



**133 462 | imb.com.au**

Document dated: 27 January 2026
Changes effective: 27 January 2026

These Internet Banking Terms and Conditions adopt the paragraph numbering corresponding to the paragraph numbering contained in IMB's **Member Guide to Transaction Banking – Product Disclosure Statement**.

Section **5**

# Terms & Conditions

These set out the terms on which we make our products available.

Contents | Page

## Part A: General Conditions of Use

### 1. Important words

**Access Code** means your personal Access Code or password or any other similar information issued to You by IMB which may be required in order to access your Accounts or perform certain actions and which is required to be kept secret. This includes but is not limited to PINs, your App PIN, your Internet Banking password, your Teleservices Password, One Time Passwords and SMS 2FA or Two Factor Authentication mechanisms

**Access Device** means any instrument issued by Us for You to access your Account, including but not limited to a Card, token or biometric reader

**Access Facility** means an arrangement We authorise You to use to instruct Us, through Electronic Equipment or an electronic Interface, to debit or credit an Account

**Access Identifier** means information issued to You by IMB which may be required in order to access your Account or conduct a transaction but which is not required to be kept secret. This includes but is not limited to Account numbers, Card numbers, Card expiry dates and PayID

**Account** means an Account We establish in your name or in your name jointly with another person/s or in the name of a business in the case of an approved business entity

**Account Details** means our record of your Account including BSB, Account number, Account name, your full legal account name, any other name You use and Account activity

**Account Holder** means the person or entity who owns the Account

**Additional Cardholder** means a person to whom a Card has been issued at your request under clause 56.6 of this PDS

**Agreed Line Of Credit** means the Account limit or credit arrangement existing on a Linked Account, as You and We agree from time to time

**ANZ** means Australia and New Zealand Banking Group

**App PIN** means an Access Code You may use to access the Mobile Banking App. An App PIN may also be a Biometric Identifier stored on your Mobile Device which is used to access the Mobile Banking App

**ATM** means an automatic teller machine owned by Us or another third party

**Authentication** means a mechanism by which IMB confirms the identity of the party involved in the transaction

**Authentication Limit** is the daily cumulative dollar value limit of transactions that can be performed within the Internet Banking facility without the requirement for Authentication

**Authorised Deposit-Taking Institution** or **ADI** has the same meaning as Authorised Deposit-Taking Institution in the Banking Act 1959 (Cth)

**Authority To Operate** or **ATO** means a person who has Authority to Operate on another person's or entity's Account and may also be referred to as an 'authorised agent'

**Biller** means a person or Organisation which issues bills that You can pay using BPAY

**Biometrically-enhanced Digital Identification Verification** means the verification of your identity under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) using both electronic data and biometric analysis

**Biometric Identifier** means your fingerprint(s), face or other unique biological or physical characteristic used to identify You

**BPAY** means BPAY Pty Ltd ABN 69 079 137 518

**BPAY Payment** means a payment to a Biller made using BPAY

**Business Day** means a day when We are open for normal business in New South Wales other than a Saturday or Sunday or a National or New South Wales Public Holiday

**Card** means any Visa Card or Cashcard We issue to You or an Additional Cardholder for use on your Account

**Cheque Services Provider** means our representative for the purpose of clearing, exchanging and settling cheques. Our current representative is ANZ

**Clearing Account** means the Account conducted for our members with our Cheque Services Provider

**Confirmation of Payee** or **CoP** is a service that enables You to check whether the account name of the BSB and account number entered matches the account information held by the recipient's financial institution

**Default Fee** means the Default Fee payable under clause 10.4 of Section 5, Part A of this PDS

**Delegated User** means a person with an Authority to Operate whose access to the Account Holder's Accounts is limited at the discretion of the ATOs on that Account. Delegated Users can only be authorised to operate on your Account via Internet Banking and view your accounts via the Mobile Banking App

**Device** means a physical and/or electronic device capable of being used to store an Access Code. This includes but is not limited to calculators, personal computers, diaries, personal organisers, mobile phones and portable computers

**Digital Identification Verification** means the verification of your identity under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) using electronic data

**Duplicate Osko Payment** means a correctly directed Osko Payment which has been inadvertently made more than once by You

**EFT Transaction** means a transfer of funds initiated by an instruction You give via an Access Facility using an Access Device, Access Identifier and/or Access Code (including a PIN) to debit or credit an Account

**EFTPOS** means a point of sale electronic banking facility available at retail or wholesale outlets

**Electronic Equipment** means a Device that You use to access or effect a transaction in Internet Banking or the Mobile Banking App including but not limited to a PC, mobile phone, smart phone or tablet computer

**Email** means electronic mail message

**Error Osko Payment** means an Osko Payment made by an Osko Payer who is not a 'User' for the purposes of the ePayments Code which is erroneously credited to the wrong Account because of the Osko Payer's error

**eStatement** means your statement as provided to You in Internet Banking and/or the Mobile Banking App

**Extreme Carelessness** means a degree of carelessness that greatly exceeds what would normally be considered careless behaviour

**Financial Institution Cheque** means a cheque instructing payment from IMB rather than from a Member's account

**Foreign Cheque** means a cheque drawn on an overseas financial institution

**Interface** means any Access Facility permitting transactions on your Account by the combined use of an Access Device and an Access Code (including a PIN), by the combined use of an Access Identifier and an Access Code (including an Internet Banking password) or by use of an Access Device, Access Code or Access Identifier alone. It includes ATMs, Tiff, PINpads, internet, telephone and EFTPOS outlets and any other Interface We make available from time to time and, where the context in this PDS requires it, also includes non-electronic facilities for conducting the transactions above

**Internet Banking Password** means the Access Code You use in conjunction with your member number to access Internet Banking

**Internet Banking Transaction** means any transaction on a nominated Account that is conducted through IMB's Internet Banking facility. It includes BPAY Payments, Osko Payments, payments to third party Payees, internal payments to You or other IMB members and batch payments. It does not include transactions made using the Mobile Banking App

**Linked Account** means any Account which is linked to your Card

**Loan Contract** means the documents making up a Loan Contract for a Loan Product

**Loan Product** means a loan or credit product provided by IMB and includes but is not limited to a Personal Credit Line facility, an IMB home loan, IMB Reverse Mortgage or Aged Care Loan, IMB Equity Line, Package Equity Line or Equity Line Advantage, IMB Professional Equity Line, IMB Business Banking Overdraft Facility or Commercial Credit Line, Commercial Loan & Fully Drawn Commercial Loan

**Mandate Management Service** or **MMS** means the database of Payment Agreements operated by NPP Australia Limited

**Merchant** means a merchant with which You have an established or, would like to establish, a Payment Agreement

**Migrated DDR Mandates** means an existing Direct Debit arrangement that is converted to a PayTo Agreement

**Misdirected Osko Payment** means an Osko 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

**Mistaken Internet Payment** means a payment by a User to a third party Payee using an internet banking facility including Internet Banking and the Mobile Banking App where funds are paid into the Account of an Unintended Recipient because the User enters or selects a PayID or BSB number and/or Account number that does not belong to the named and/or intended recipient as a result of:

- the User's error, or
- the User being advised of the wrong PayID or BSB number and/or Account number.

This does not include payments made using BPAY and PayTo

**Mobile Banking App** means the facility You use to access your Accounts and conduct transactions via a dedicated application for a Mobile Device

**Mobile Banking App Transaction** means any transaction on a nominated Account that is conducted through the Mobile Banking App. It includes BPAY Payments, Osko Payments, payments to third party Payees and internal payments to You or other IMB members

**Mobile Device** means portable Electronic Equipment and includes but is not limited to a mobile phone, smart phone or tablet computer

**Negotiable Interest Term Account** or **NITA** is a type of Term Deposit account where interest rates and terms are negotiable for amounts over a specified minimum amount. The current minimum amount is set out in the document entitled PDS - Interest Rates for IMB Products.

**Nominated Email Address** means the Email address You nominate to receive information from IMB including information regarding BPAY View® if You are registered for BPAY View

**NPP** means the New Payments Platform operated by NPP Australia Limited

**NPP Payment** means a payment cleared and settled via the NPP. It includes an Osko Payment

**Online Account Opening** means the online account opening application process available on IMB's website

**Organisation** means a natural person (i.e. an individual) acting in their capacity as a trustee, sole trader or partner of a partnership; a body corporate in its personal capacity or as a trustee; a government agency; an unincorporated body or association; or a firm or partnership

**Organisational Osko Payer** means an Osko Payer that is an Organisation

**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>

**Osko** means the Osko payment service provided by BPAY as described in Part G of this PDS

**Osko Adjustment** means a transaction initiated by Us or You to adjust or reverse an Osko Payment which has already been cleared and settled

**Osko Overpayment** means a correctly directed Osko Payment where the amount has inadvertently been submitted for an amount greater than intended

**Osko Payment** means an NPP Payment made by or on behalf of an Osko Payer to an Osko Payee using Osko

**Osko Payment Return** means an NPP Payment made by or on behalf of an Osko Payer who has received an Osko Payment and which is made in response to a request for a return of that payment by the original Osko Payer's financial institution

**Osko Payee** means a customer who uses Osko to receive Osko Payments or Osko Adjustments

**Osko Payer** means a customer who uses Osko to make Osko Payments or Osko Adjustments

**Osko Payment Direction** means a direction from an Osko Payer to effect an Osko Payment or Osko Adjustment

**Osko Transaction** means an Osko Payment or Osko Adjustment

**OTP** means One Time Password which is received by You by either SMS to your mobile phone or by calling IMB on 133 462 or by Push Notification or within the Mobile Banking App or in any other manner specified for a particular product or facility for the purpose of performing certain actions such as logging into Internet Banking, changing your personal details or authenticating Payees or Billers or payments which require Authentication and is valid only for the Internet Banking or Mobile Banking App session in which the OTP is requested

**Payee** means a person or entity to whom You request Us to make a payment using funds from your Account

**PayID** means a smart address for NPP Payments composed of a permitted PayID Type linked to a nominated Account

**PayID Name** means the name We give You to identify You to Osko Payers when your PayID is used to make an NPP Payment

**PayID Service** means the central payment addressing service which is available for addressing NPP Payments

**PayID Type** means a piece of recognisable and memorable information that can be linked to a nominated Account to create a PayID. Supported PayID Types include phone number and Email address or as otherwise advised from time to time

**Payment Agreement** means an agreement between You and an approved Merchant or Payment Initiator. Payments from your Account are processed per the terms set out in the agreement

**Payment Facility** means any method of payment approved by IMB and includes but is not limited to a BPAY Payment, Osko Payment, Card, Cheque, Direct Debit, Direct Credit, EFT Transaction, Internet Banking, the Mobile Banking App, Telephone Banking, Periodical Payment and PayTo Payment

**Payment Initiator** means an approved payment service provider who, whether acting on behalf of You or a Merchant, is authorised by You to initiate payments from your Account

**PayTo** means the service which enables Us to process NPP Payments from your account per terms set out in a Payment Agreement You have established with a Merchant or Payment Initiator that subscribes to the service

**PayTo Payment** means an NPP Payment We make pursuant to a Payment Agreement

**Personal Information** includes a person or Organisation's name, contact details, date of birth, gender, relationships, account details, transactional history, financial position, place of employment, credit history, identifiers assigned by the government such as your tax file number, Australian Business Number or Australian Company Number and any other information or opinion about a person whose identity is apparent or can be ascertained from that information or opinion

**PIN** means a Personal Identification Number, word or combination of letters and/or numbers used in conjunction with a Card

**PINpad** means an electronic Device which allows You to identify yourself using your PIN rather than your signature or another form of identification

**Power of Attorney** or **POA** or **Attorney** means a person who has been appointed as a person's attorney pursuant to a Power of Attorney document and is authorised to operate on that person's account as well as liaise with Us in relation to that person's other financial and business dealings with Us and may also be referred to as an 'authorised agent'

**Push Notification** means an electronic alert delivered via the Mobile Banking App to your Mobile Device

**Receiving Institution** means an ADI whose customer has received an internet payment

**Schedule** means the personalised Schedule prepared for You (where your Account has a Personal Credit Line facility attached) setting out details of your Account, any Linked Account and other information

**Secure Email** means the Email Account You access through your Internet Banking and which IMB will from time to time communicate with You through

**Sending Institution** means an ADI whose customer has made an internet payment

**SMS 2FA** or **Two Factor Authentication** is a term used to describe any Authentication mechanism where more than one thing is required to authenticate a User

**Teleservices Password** means the password You are required to provide to IMB staff before discussing your Accounts over the phone through IMB's Call Centre or when obtaining an OTP

**Tiff** or **TellerInfinity** means a self service teller machine available at selected IMB branches

**Unauthorised Transaction** means a transaction which is not authorised by the User or is executed without the User's knowledge or consent

**Unintended Recipient** means the recipient of funds as a result of a Mistaken Internet Payment

**User** means You or an individual who is authorised by You to perform transactions on an Account, including but not limited to a person authorised under clause 7.3

**View Only** means the level of access that an Account owner can grant to an ATO or Delegated User which limits the ATO or Delegated User's access to viewing the Accounts only (no transacting can take place)

**WBC** means Westpac Banking Corporation

**We** or **Us** or **IMB** means IMB Ltd trading as IMB Bank ABN 92 087 651 974

**You** means each person named as an Account Holder but does not include an Additional Cardholder. If there is more than one Account Holder, You means each Account Holder separately and every two or more Account Holders jointly. You also includes your successors and assigns

Words importing persons shall extend to and include corporations; words importing the masculine gender shall extend to and include the feminine and neuter gender; and words importing the singular or plural number shall extend to and include the plural or singular number respectively.

## 2. Changes to this PDS

### 2.1. Changes We may make

Acting reasonably, having regard to our legitimate business interests, We may change any of this PDS at any time without your consent. Without limiting the changes We may make, We may make changes to the parts of this PDS relating to:

- Interest rates (except that We cannot change the interest rate that applies to a Term Deposit or a NITA during the term of the investment if prepayment is not requested);
- The frequency that interest is debited or credited;
- The method of calculating interest or the balance tiers which determine the interest rate;
- Fees and charges (including introducing a new fee or charge and changing the amount, frequency and method of calculation of fees and charges);
- Your liability for EFT Transactions;
- Withdrawal and transaction limits;
- The types of transactions You can perform or ways You can access or transact on your Account;
- Eligibility requirements for your Account;
- The features of your Account or the products or services (including Payment Facilities) available for your Account;
- Minimum balance requirements to hold your Account or waive the monthly account keeping fee (including imposing, adjusting or removing these requirements);
- If your Account has a Personal Credit Line facility attached, the credit limit by reducing or cancelling it, or the amount, method of calculation, frequency or time for repayment of repayments.

The circumstances in which We may make changes include but are not limited to the following:

- To add, change or remove features of your Account or the products or services (including Payment Facilities) available for your Account;
- To respond to changes in the cost of providing your Account or the products or services (including Payment Facilities) available for your Account;
- To discontinue a product and change the terms of the product to reflect a different product with similar features to the discontinued product;
- To reflect a change in our systems or processes, including for security reasons;
- To reflect changes to our structure or financial position, including our cost of funds and liquidity;
- To comply with any change or anticipated change in any relevant law, code of practice, guidance or general banking practice;
- To reflect any decision of a court, ombudsman or regulator;
- To reflect industry, market or best practice;
- To manage risks (including fraud, operational, credit or regulatory risk) or for prudential reasons;
- To correct a mistake, omission or ambiguity;

- To streamline the administration of your Account or the products or services (including Payment Facilities) available for your Account;
- To make this PDS clearer.

### 2.2. Notice of change

We will give You at least 30 days' notice prior to the change taking effect if We:

a) Increase or introduce a new fee or charge (other than a government charge);
b) Change the frequency that interest is debited or credited;
c) If your Account has a Personal Credit Line facility attached, change the amount, method of calculation, frequency or time for repayment of repayments;
d) Change the method of calculating interest or the balance tiers which determine the interest rate;
e) In relation to an EFT Transaction:
    i) Impose or increase charges relating solely to the use of an Access Device (such as a Card) or Access Code (such as a PIN), or the issue of an additional Access Device or Access Code or replacement Access Device or Access Code;
    ii) Increase your liability for losses; or
    iii) Impose, remove or adjust a daily transaction limit or other periodic transaction limit; or
f) Make any other change We reasonably believe is unfavourable to You (other than a change in an interest rate, or reduction or cancellation of a credit limit).

If We make any of the changes listed in the paragraph above, We will notify You in one of the following ways:

- By writing to You directly or notifying You by placing a notice in a major national newspaper, depending on the nature of the change;
- Electronically (where the ePayments Code permits);
- By placing a notice in your statement of Account or other material We send to You.

Unless otherwise specified in this PDS, We will notify You of any other changes on or before the day the change takes effect in one of the following ways:

- By placing a notice in a major national newspaper;
- In writing, or by placing a notice in your statement of Account or other material We send to You;
- By placing information on our website imb.com.au, or on your Internet Banking log on page, by Push Notification or within the Mobile Banking App, and notifying You in writing that the information is there;
- By sending You a Secure Email; or
- In any other way agreed to by You,

except where We reasonably believe the change is not unfavourable to You, in which case We will notify You in one of these ways before or when We provide your next statement.

We need not give You notice when changes are necessitated by an immediate need to restore or maintain the security of the system or individual Accounts or to comply with our obligations at law or any industry code. This includes for the prevention of systematic or individual criminal activity, including fraud.

If You are unhappy with a change, You can close your Account in accordance with this PDS.

## 13. Timing of transactions

Acting reasonably, We may assign any date We consider appropriate to a debit or credit to your Account (except that, in the case of a debit, the date must not be earlier than the date on which the relevant transaction occurs).

However, We credit payments to your Account (including cash deposited at ATMs) as soon as practicable after We receive them. This is not necessarily the same day that You pay.

We may subsequently adjust debits and credits to the Account so as to accurately reflect the legal obligations of You and Us (for example, because of an error or because a cheque is dishonoured). If We do this, We may make consequential changes (including to the interest charges).

Unless the law prevents Us from doing so, You agree that We may adjust debits and credits in your Account where it is clear that You are not the intended recipient, where We are under court order or other valid legal instruction to do so, or You are otherwise not entitled to funds in your Account.

BPAY authorisations which are given after 4pm on a Business Day or at any time on a non-Business Day will be processed on the next Business Day after the authorisation was given. Where You authorise a payment outside of these times or on a non-Business Day, We will hold the amount You have requested for payment in a payment file, but will not process the payment until the next Business Day.

**IMPORTANT.** You will not earn interest on the funds subject to your authorised payment where it is made outside business hours, and is held by Us for processing on the next Business Day.

## 18. Assignment

Acting reasonably, We may assign or otherwise deal with our rights under this agreement in any way We consider appropriate. You agree that We may disclose any information or documents We consider desirable to help Us exercise this right. You also agree that We may disclose information or documents at any time to a person to whom We assign our rights under this agreement.

# Part E: Electronic Banking, Cards, Personal Credit Line

This part of this PDS only applies to You if You have a Card or Personal Credit Line facility attached to your Account, or if You use any Access Code, Access Identifier, Access Facility or Access Device to operate your Account.

## 53. Internet Banking - Terms and Conditions

### 53.1. Introduction to Internet Banking

This Clause 53 and Clause 55 set out the terms and conditions that apply to You if You use IMB's Internet Banking facility to access your IMB Accounts. Clauses 53 and 55 do not contain all the information that applies to Internet Banking. Parts of clause 53 also apply to Mobile Banking App use. Further information about this service is found in other sections of this PDS. You can register for Internet Banking if Internet Banking is available on the Account/s You hold with IMB.

If You open an Account as a new member on or after 1 August 2015, You will automatically be registered for Internet Banking unless You tell Us otherwise. If You are an existing member You must be registered for Internet Banking before You can open an Account through IMB's website using the online account opening process.

You receive and agree to these Internet Banking Terms and Conditions on your own behalf and as an agent for anyone operating your Account through Internet Banking. Your agents will also be required to agree to these Terms and Conditions when they register as an Internet Banking User.

A copy of the Internet Banking Terms and Conditions is also available at imb.com.au and can be accessed from within Internet Banking.

You are required to read and understand these Internet Banking Terms and Conditions before using IMB's Internet Banking facility. It is important that You read and fully understand these Internet Banking Terms and Conditions as they set out your rights and responsibilities when using IMB's Internet Banking. We recommend that You print and keep a copy of these Internet Banking Terms and Conditions for future reference.

We do not warrant that our Internet Banking facility will be available and functional at all times. We warrant that We will comply with the requirements of the ePayments Code.

### 53.2. Fees & Charges

We may charge You and debit your Account with any fees and charges which apply to Internet Banking. Other fees and charges may be payable under your specific Account terms and conditions.

Details of the current fees and charges are set out in the **PDS - Fees, Charges and Limits,** which is available on our website at imb.com.au, at an IMB Branch or by contacting IMB on 133 462.

### 53.3. Benefits of using IMB Internet Banking

When You open an Account on which Internet Banking access is available, You will automatically be registered for Internet Banking. If You open an Account as a new member on or after 1 August 2015, You will automatically be registered for Internet Banking. Internet Banking allows You to complete transactions any time, 24 hours a day 7 days week (subject to system availability and maintenance and any applicable daily transaction limits).

The following services are available on some of our Accounts through Internet Banking:

- Account balance enquiry;
- transaction history enquiry;
- search for transaction details;
- transfer funds between nominated Accounts;
- have your bills delivered to You electronically via BPAY View;
- make payments to accounts with Us and other Australian financial institutions;
- Schedule transfers and payments to be paid on a future date or on a recurring periodic frequency (e.g. monthly);
- send secure messages to Us and receive secure messages from Us;
- manage your Internet Banking and Account alerts;
- manage your transaction limits up to any maximum transaction limit set by Us;
- update your personal details;
- access eStatements;
- change your statement preference;

- manage your PayTo Agreements;
- manage your Cards, including activating new Cards, changing your PIN and temporarily or permanently blocking Cards.

### 53.4. Risks associated with using Internet Banking

**53.4.1** There is a risk of Unauthorised Transactions occurring via Internet Banking on your Account as a result of computer use, human error or fraud. Please see clauses 55.5, 55.6 and 59 of these Terms and Conditions for information about:

a) keeping your member number and Internet Banking Access Code secure; and
b) when You will be liable for Unauthorised Transactions.

**53.4.2** Once You have processed a transaction through Internet Banking, it cannot be stopped.

**53.4.3** You are responsible for ensuring that all details You enter for BPAY Payments, Osko Payments and third party payments are correct. If your instructions are incorrect, We will attempt to recover any incorrect payment on your behalf, but if We are unable to do so, We are not responsible for that payment. Please refer to clauses 55.5 and 60 of these Terms and Conditions for further details.

### 53.5. Internet Banking Registration

**53.5.1** To access IMB's Internet Banking facility, You must be registered for Internet Banking. You can register for Internet Banking at any IMB Branch, by calling IMB on 133 462 or by accessing the Internet Banking registration form from IMB's website at imb.com.au, and sending the completed form to PO Box 2077, Wollongong NSW 2500. If You open an Account as a new member on or after 1 August 2015, You will automatically be registered for Internet Banking unless You tell Us otherwise.

**53.5.2** A valid Australian mobile phone number must be provided upon registration if You wish to have access to SMS 2FA which will allow You to complete certain activities within Internet Banking. If You open an Account as a new member on or after 1 May 2015 and You provide your mobile phone number, You will be automatically registered for SMS 2FA unless You tell Us otherwise. If You open an Account as a new member through IMB's website, using the online Account opening process, You will be required to provide a mobile phone number and You will be automatically registered for SMS 2FA.

**53.5.3** You are responsible for ensuring You inform Us of any changes to the mobile phone number You have nominated to access SMS 2FA.

**53.5.4** If You are unable to use SMS 2FA, You will not be able to utilise some of the services within Internet Banking. You will still be required to authenticate Payees or Billers and payments by calling IMB's Call Centre and obtaining an OTP when this is required.

**53.5.5** You must log on to Internet Banking within 2 days of receiving your Access Code. If You do not log on to Internet Banking within the prescribed timeframe, your Internet Banking registration will be cancelled.

**53.5.6** Approval of an application for access to IMB's Internet Banking facility is at IMB's discretion.

### 53.6. One Time Passwords (OTP)

Payee in the following clauses 53.6 to 53.11 includes a PayID Payee. This clause also applies to Mobile Banking App use.

**53.6.1** You may be required to authenticate transactions that We have identified at our complete discretion as requiring Authentication.

**53.6.2** You may be required to complete Authentication for certain actions or a Payee or Biller before You can perform a transfer or make a payment to that Payee or Biller.

**53.6.3** You may be required to complete Authentication for other actions, such as logging into Internet Banking, changing your personal details, activating and maintaining Cards and associated PINs and registering and maintaining your PayID before You can perform those actions.

**53.6.4** Authentication requires You to enter an OTP in the Internet Banking or Mobile Banking App session You are logged into before We will process the instruction.

**53.6.5** Depending on the action requiring Authentication You can receive an OTP from IMB:

a) where You are registered for SMS 2FA, via an SMS to your registered mobile phone number; or
b) by calling IMB and providing your Teleservices Password;
c) in any other way We advise in relation to a specific action or facility; or
d) Push Notification or within the Mobile Banking App (where functionality is available).

**53.6.6** You register for OTPs to be delivered via SMS to your mobile phone by registering for SMS 2FA. This phone number is used by IMB to send an OTP to your mobile phone when You wish to perform certain types of transactions, activate or maintain Cards and associated PINs or to authenticate a Payee or Biller. Where available, OTPs may also be delivered to your Mobile Device via Push Notification.

**53.6.7** If You are not registered for SMS 2FA and You need to authenticate an action, You may be able to (depending on the action requiring Authentication) obtain an OTP by calling IMB on 133 462 and providing your Teleservices Password. You must register for a Teleservices Password with IMB before You can start obtaining OTPs from IMB's Call Centre. You may be able to obtain an OTP from IMB's Call Centre to Authenticate actions that require Authentication.

**53.6.8** IMB may provide You with an OTP in another secure way, including but not limited to via Secure Email, depending on the facility You are using and/or the action requiring Authentication. We will advise You how You can receive an OTP at the time You use the relevant facility or are required to authenticate the relevant action.

**53.6.9** You will be required to provide an OTP for each Payee or Biller that You are required to authenticate.

**53.6.10** An OTP is only valid during the Internet Banking or Mobile Banking App session You are logged into when the request for an OTP is made and is no longer valid after You log out of that session or if You cancel the transaction or do not complete relevant action.

### 53.7. Logging onto Internet Banking - First Time

**53.7.1** To log on to Internet Banking your Access Code must be used in conjunction with your member number. During the registration process for Internet Banking, your Access Code will be generated and provided to You. For your security, when You first log on to Internet Banking, You must change your Access Code.

**53.7.2** You will need to follow these steps on your first log on to Internet Banking:

a) in the Internet Banking log on page enter:
   i) your member number; and
   ii) the OTP into the access code field. You will have received your OTP via SMS sent to your registered mobile phone number or if You are not registered for SMS 2FA, from our Branch staff or over the phone from our Call Centre when You register for Internet Banking.

b) when You are logged in to Internet Banking, You will be immediately prompted to change your Access Code. You will be required to use the new Access Code You choose when You log on to Internet Banking anytime in the future. You can also change this Access Code at any time from the access tab within Internet Banking;

c) You will be prompted to accept these Internet Banking Terms and Conditions before You can proceed. It is important that You read and understand these Internet Banking Terms and Conditions before agreeing to them as they set out your rights and responsibilities when using Internet Banking.

### 53.8. Authenticating Payees and Billers

You may be required to authenticate a Payee or Biller before You can perform a transfer or make a payment to that Payee or Biller. You will only be required to authenticate a Payee or Biller once, after which You can perform a transfer or make a payment to that Payee or Biller (within any applicable transaction limits) without the need to authenticate that Payee or Biller again.

### 53.9. Authentication Limits and Transaction Limits

**53.9.1** IMB may set a maximum daily amount (the Authentication Limit) that can be paid or transferred within Internet Banking to a Payee or Biller that is not an authenticated Payee or Biller. Payments to authenticated Payees or Billers remain subject to any maximum daily transaction limit. Payments You make via the Mobile Banking App are included in your maximum daily transaction limit.

**53.9.2** You may request that IMB change (i.e. increase or decrease) any daily Authentication Limit or maximum daily transaction limit, however, You agree that by doing so, You may be liable for further losses which exceed any daily Authentication Limit for unauthenticated Payees or Billers or maximum daily transaction limit. Your liability for Unauthorised Transactions on your Accounts via Internet Banking is determined in accordance with the ePayments Code. IMB may decline to authorise any request for a change to any Authentication Limit or maximum daily transaction limit in its absolute discretion.

**53.9.3** Where You make a change to a forward dated payment (including any periodic payments You set-up) to an 'Authenticated Payee' You will be required to authenticate all of the following actions:

a) any changes to the details of any Payees who You have previously authenticated;
b) changes to any of the details (i.e. payment date) of any forward dated payments You have previously set up.

**53.9.4** Some changes to Payee or Biller details will not require Authentication.

**53.9.5** For our or your security, IMB may reduce the Authentication Limit or daily transaction limit at any time, without notice, including where there is a risk to the security of Internet Banking, or the risk of fraud to You or Us. The Authentication Limit or daily transaction limit may be restored at IMB's discretion acting reasonably having regard to our or your security.

### 53.10. eStatements - personal Accounts

If your statement preference is set to online You agree that IMB will send You an Email notification to your Nominated Email Address advising You that your eStatement is available to view in Internet Banking and the Mobile Banking App.

If your statement preference is set to online it is your responsibility to check your Emails regularly for the Email notifications and to access your eStatement promptly. You must keep your Nominated Email Address current and accessible and advise Us as soon as possible of any change. If We become aware that an Email notification has failed to deliver because the Nominated Email Address is invalid or We get an error response, We will let You know and prompt You to update your details or remedy any problems with your Nominated Email Address. If You do not update your details or remedy the problems with your Nominated Email Address, We may recommence sending You paper statements.

You can change your statement preference at any time by changing your preference in Internet Banking, the Mobile Banking App, contacting Us on 133 462 or attending a Branch.

### 53.11. eStatements - business Accounts

If the statement preference for the business is set to online You agree that IMB will send an Email notification to the Nominated Email Address of the business advising You that the eStatement is available to view in Internet Banking and the Mobile Banking App.

Statements for business members will be available to be accessed from within Internet Banking and the Mobile Banking App by those ATOs authorised by the business to have access to those statements.

It is the responsibility of the business member to check Emails to their Nominated Email Address regularly for notifications and to access the statement promptly. The business must keep its Nominated Email Address current and accessible and advise Us as soon as possible of any change. If We become aware that an Email notification has failed to deliver because the Nominated Email Address is invalid or We get an error response, We will advise and prompt the business to update its details or remedy any problems with the Nominated Email Address. If the details are not updated or the problems with the Nominated Email Address not remedied, We may recommence sending paper statements.

Only appropriately authorised representatives of the business member can manage the statement preference for the business and allow ATOs access to the business' eStatement from within Internet Banking and the Mobile Banking App. To manage statement preferences, please contact Us.

### 53.12. Management of Cards in Internet Banking

The general terms and conditions relating to your Cards are available at Clause 56. The terms and conditions contained in this clause 53.12 and 53.13 relate only to your use of Internet Banking to maintain your Card facility.

**53.12.1** IMB provides the ability within Internet Banking for Internet Banking users to perform certain actions on Cards where they are the cardholder. This means that You are unable to perform the above action on Cards that are not held by You in your name; this includes Cards held by Additional Cardholders, other signatories or fellow joint account holders. Additional Cardholders may use Internet Banking facility to perform the actions listed below if they are registered as an Internet Banking user. If You have any concerns regarding Cards held by other cardholders or Additional Cardholders on your Account or an Account to which You are a signatory to, please contact Us on 133 462.

**53.12.2** This functionality allows Internet Banking users to:

a) activate new Cards in their name;
b) set a new PIN or change an existing PIN linked to the Card;
c) temporarily or permanently block a Card in circumstances where the Card is lost or stolen;
d) unblock a temporarily blocked Card;
e) advise of disputed transactions that have occurred on the Card.

The security of Access Codes, such as PINs or Internet Banking passwords are extremely important. The guidelines in clause 58 are designed to help keep Access Codes, Devices and any Electronic Equipment used to access Internet Banking or Card facilities secure. Please refer to clause 58.

### 53.13. Temporarily or Permanently Blocking Your Card in Internet Banking

**53.13.1** You must tell Us and ensure that any Additional Cardholder tells Us as soon as possible if a Card is lost or stolen or suspect that a PIN or Access Code is known to someone else. You may do this through the Internet Banking functionality outlined below, or through the process outlined in clause 56.20, 58 and 59 below.

**53.13.2** You or an Additional Cardholder are able to temporarily block a Card via Internet Banking. This block will be effective once all required steps in Internet Banking are finalised and a receipt is issued. Temporarily blocked Cards are able to be unblocked via Internet Banking. You will be liable for transactions performed on your Card after the Card is unblocked, in accordance with Clause 56 and 59.

**53.13.3** You or an Additional Cardholder are able to permanently block a Card via Internet Banking. This block will be effective once all required steps in Internet Banking are finalised and a receipt is issued. You are unable to unblock a permanently blocked Card. To order a new Card please contact Us on 133 462.

### 53.14. Open Banking – Consumer Data Right (CDR)

Open Banking allows eligible IMB members to share some of their IMB CDR data with accredited organisations. In certain circumstances your IMB CDR data may also be shared by another eligible person. This may include:

- A joint Account Holder with whom You jointly share an eligible IMB joint account.

  Please note: in accordance with CDR legislation, CDR data sharing from eligible IMB joint accounts (where all Account Holders are eligible individuals) will be enabled by default (set automatically to what is known as the pre-approval option pursuant to the CDR regime). This means that any eligible IMB joint Account Holder can share joint account CDR data from that account with any accredited data recipients at any time without the other joint Account Holders' approvals whilst the pre-approval option is effective. However, if You withdraw your approval, eligible IMB joint account CDR data cannot be shared without permission from all joint Account Holders. Joint Account Holders can disable CDR data sharing at any time via IMB Internet Banking. For further information on the process, please visit IMB's website.

- A secondary user appointed on an eligible IMB account You hold.

  This may include either an Authority To Operate (ATO or 'authorised agent') or Power of Attorney (POA or Attorney or 'authorised agent'). By default, secondary users are not able to automatically share IMB CDR data and must first be enabled by the Account Holder. Account Holders can view and maintain (which includes either enabling or disabling ATOs or POAs) the CDR data sharing arrangements they have for their secondary users at any time via IMB Internet Banking. For further information on the process, please visit IMB's website.

  Please note: in relation to a POA, an Attorney acting under a POA does not become the CDR consumer in respect of that CDR data. Accordingly, in the absence of any express CDR related clause in a POA document, IMB will require the Account Holder to provide a separate explicit secondary user instruction in order to constitute the proper appointment of the Attorney as a secondary user for the purposes of sharing CDR data.

- One or more nominated representatives of an eligible organisation (which includes business members like partnerships, companies, trusts, associations and government entities).

  This may include for example, an ATO or Delegated User for an account but may be any other eligible individual properly authorised by a business member. Nominated representatives are not able to automatically share IMB CDR data and must first be enabled by the eligible organisation by providing an authorisation to IMB in the form prescribed by IMB.

  Please note: once properly authorised, a nominated representative will have the ability to share and manage CDR data for ALL accounts owned by the business member.

Importantly, any changes that Account Holders make with respect to CDR data sharing arrangements will not automatically change the transactional banking access or other arrangements that Account Holders have in place within IMB's Internet Banking (and vice versa). Account Holders will have to implement any changes to both the CDR data sharing arrangement and transaction arrangements separately.

For further information about Open Banking (including how You can make a request to share your IMB CDR data, a full list of eligible accounts and IMB's CDR Policy), please visit IMB's website.

## 55. Internet Banking and Mobile Banking App – General Terms and Conditions

### 55.1. Your Agreement to Receive Information Electronically

**55.1.1** By using IMB's Internet Banking facility or the Mobile Banking App and accepting these Terms and Conditions, You agree to IMB communicating with You electronically in relation to Internet Banking and the Mobile Banking App and the Internet Banking or Mobile Banking App Terms and Conditions and/or in relation to any other matter which IMB deems appropriate and for which We are permitted to communicate with You electronically.

**55.1.2** IMB may contact You via Secure Email within Internet Banking or Push Notification to provide You with notices as required under the ePayments Code, as well as other information that We are required to provide You or otherwise wish to draw your attention to from time to time. If You do not check your Secure Email regularly, You may not become aware of important information related to Internet Banking, the Mobile Banking App or other IMB matters.

**55.1.3** You acknowledge that by agreeing to receive information electronically, You will not receive this information in paper form or any other form or by any other method, unless You request it from IMB.

**55.1.4** Further to the situations described in clause 55.1.2, to the extent permitted by law, We may also give You notices as required by law and/or other information to which We wish to draw your attention from time to time, by one or more of the following means:

a) personally;
b) by sending it by post to the address nominated by You;
c) by sending it to a fax number or Email address nominated by You;
d) by electronic notice posted on our website at imb.com.au, or on your Internet Banking log on page or within the Mobile Banking App, and notifying You in writing that the information is there;
e) by newspaper advertisement;
f) by Secure Email; or
g) Push Notification.

**55.1.5** If a notice is sent by post, delivery of the notice is deemed to be effected on the date it would be received in the ordinary course of post.

**55.1.6** If a notice is sent by facsimile or electronic transmission, delivery of the notice is deemed:

a) to be effected by properly addressing and transmitting the facsimile or electronic transmission; and
b) to have been delivered on the day following its despatch.

If notice is placed by way of newspaper advertisement, delivery of the notice is deemed to be effected on the date the notice is placed in the newspaper.

**55.1.7** If a notice is posted on our website, your Internet Banking log on page, by Push Notification or within the Mobile Banking App, delivery of the notice is deemed to be effected on the date You are deemed to be notified in writing that the information is there.

**55.1.8** Unless required by law, notice may be given by Us to joint Account Holders by giving the notice to the primary joint Account Holder only.

### 55.2. Termination and Suspension of Internet Banking or Mobile Banking App access and refusal of transactions

**55.2.1** We may cancel your access to Internet Banking or the Mobile Banking App at any time after giving You at least 30 days' written notice.

Acting reasonably, having regard to our legitimate business interests, We may in some circumstances cancel your access to Internet Banking or the Mobile Banking App, or refuse to give effect to an Internet Banking transaction or a Mobile Banking App transaction requested by You, without prior notice, including but not limited to where:

a) Your Accounts have been closed;
b) We believe the use of Internet Banking or the Mobile Banking App, or the Internet Banking or Mobile App transaction, may cause loss to You or Us;
c) We believe that the quality or security of Internet Banking or the Mobile Banking App is inadequate;
d) We are required to do so by law or a court order;
e) We deem your use or the transaction to be inappropriate;
f) We reasonably consider that your use of the facility has become dormant;
g) We are otherwise obliged to discontinue providing Internet Banking or the Mobile Banking App or to refuse to give effect to the Internet Banking or Mobile Banking App transaction;
h) You, your ATOs or a Delegated User or someone acting on your behalf or under your direction is suspected of being involved in fraudulent activity when dealing with Us or any third party; or
i) in relation to your access to the Mobile Banking App or a Mobile Banking App transaction, You are no longer registered for Internet Banking, your Internet Banking access has been cancelled or Internet Banking access is unavailable.

**55.2.2** If We have not given You advance notice, We will inform You in writing after We cancel your access. If You want to use Internet Banking or the Mobile Banking App at a later time, You may ask Us to allow You to register again. IMB, in its absolute discretion, may decline your request if, for any reason, it does not consider it reasonable to restore your access.

**55.2.3** You can cancel your registration for Internet Banking by telling Us, at any time, that You wish to do so. If You want to use Internet Banking at a later time, You may ask Us to register You again.

**55.2.4** You can cancel your registration for the Mobile Banking App at any time by removing your registered Mobile Devices within the Mobile Banking App and deleting the Mobile Banking App from your Mobile Device or by telling Us You wish to do so.

**55.2.5** You can cancel your access to your Accounts via Internet Banking or by telling Us You wish to do so. You can cancel your ATOs and Delegated Users' access to your Accounts by telling Us You wish to do so.

## 55.3. Types of Internet Banking and Mobile Banking App Users

There are 3 types of Internet Banking and Mobile Banking App Users who can access Accounts through Internet Banking and the Mobile Banking App:

a) an Account Holder;
b) an ATO who is a signatory on an Account and has authority to operate an Account; and
c) a Delegated User, who can be granted access to an Account only by the Account Holder/s (applies to business Accounts only).

## 55.4. 'Authority to Operate' and 'Delegated User'

### 55.4.1 Authority to Operate (ATO)

If You appoint an ATO to your Account, they may access that Account via Internet Banking and the Mobile Banking App.

The following conditions apply to ATOs:

a) each ATO You appoint must apply to IMB to be a member and meet IMB's identification requirements before they will be able to access your Account;
b) Internet Banking transactions and other instructions must be authorised by the required number of ATOs (i.e. where an Account requires more than 1 to sign);
c) ATOs are required to accept the Internet Banking Terms and Conditions prior to accessing Internet Banking and the Mobile Banking App Terms and Conditions prior to using the Mobile Banking App;
d) You are responsible for all the transactions performed by any ATOs that You appoint, as if You made them yourself;
e) ATOs will have access to the Accounts to which You have appointed them as ATO, as if they were the owner of the Account; and
f) You should consider carefully whether to appoint an ATO as You will be solely responsible for their actions.

### 55.4.2 Delegated User

This section applies to business members who have registered for Internet Banking and have appointed Delegated Users to have access to their Accounts.

An Account owner can authorise a person to have limited access to their Account/s via Internet Banking. This Delegated User will also have View Only access to those Accounts via the Mobile Banking App. The level of access to these Accounts (i.e. transaction limits) is managed by the ATOs You have authorised on those Accounts.

If You authorise a person to have limited access to your Accounts via Internet Banking, the following conditions apply:

a) the Delegated User will have access to your Account through Internet Banking and the Mobile Banking App only (i.e. they cannot perform a transaction on your Account via any other channel);
b) each Delegated User You authorise must apply to IMB to be a member and meet IMB's identification requirements before they will be able to access your Account;
c) upon registering for Internet Banking, each Delegated User will be issued with a member number and Access Code. These details will be required for the Delegated User to gain access to Internet Banking;
d) Delegated Users are required to accept these Internet Banking Terms and Conditions, prior to accessing Internet Banking;
e) Delegated Users who have registered for the Mobile Banking App will only be able to view your Account/s via the Mobile Banking App. Delegated Users will be required to accept the Mobile Banking App Terms and Conditions prior to accessing the Mobile Banking App;
f) You cannot appoint a Delegated User to access your Account unless You have authorised at least one ATO on that Account;
g) notwithstanding clause 55.3, the ATOs on your Account will manage the access of Delegated Users on your Account as follows:
    i) if more than one ATO is required to authorise Internet Banking transactions and other requests on the Account, then that number of ATOs, as nominated by You in the Account form, is required to authorise a Delegated Users access to your Accounts;
    ii) Delegated Users will have access to the Accounts to which the ATOs on your Account authorise them to have access, as if they were the owner of the Account;
    iii) the ATOs on your Account have authority to limit the level of access of a Delegated User including what Accounts a Delegated User can view and access; and
    iv) an ATO cannot grant a Delegated User greater access than the ATOs own level of access.
h) You are responsible for all the transactions made by any Delegated Users that You appoint, as if You made them yourself;
i) You must tell IMB, in writing, if You wish to cancel/revoke a Delegated Users access to your Account/s; and
j) You acknowledge that where a Delegated User has access to more than one of your Accounts and an ATO removes a Delegated User from one Account, they will be automatically removed from all of your Accounts to which they have access. If You wish for a Delegated User to remain on any of your other Accounts, the ATOs on these Accounts will need to restore the Delegated Users access by re-authorising their access via Internet Banking.

**55.4.3 Where You authorise Delegated Users to access your Account/s via Internet Banking, the following conditions apply to their access level:**

a) the Delegated User will only be able to view the Account/s via the Mobile Banking App;
b) You are required to indicate on your Member Form whether You wish for the Delegated Users to have 'Full' or 'View Only' Internet Banking access to Accounts You authorise them to access via Internet Banking;
c) You cannot vary the access level (View Only or Full access) for different Account/s You authorise Delegated Users to access via Internet Banking. The access level You choose will apply for all Account/s You have authorised a Delegated User to have access to via Internet Banking; and
d) the access level of your Delegated Users will be the same access level (View Only or Full) as the ATOs on that Account, subject to any further limitations the ATOs on that Account impose on the Delegated Users on that Account.

### 55.5. Checking your payment instructions

**55.5.1** You must take care to identify the correct BSB and Account number or PayID for a Payee, otherwise, the payment may be made to the incorrect Account.

**55.5.2** We are not required to, and do not, check that the BSB number, Account number, PayID or credit card account number correspond with the financial institution and account name of the Payee, provided by You.

**55.5.3** Any error in these details may result in a transfer being made to an incorrect Payee or the transfer not being made at all. We are not responsible for any inaccuracy in instructions given by You.

**55.5.4** Your instruction may not be processed if:

a) all necessary information is not provided;
b) there are insufficient available funds in your Account from which the funds are to be transferred;
c) the amount of the transfer is less than the minimum deposit requirements of the account type to which the funds are to be transferred where that account is an IMB Account;
d) the amount of the transfer is less than the minimum withdrawal requirements of the account type from which the funds are to be transferred;
e) there is a restriction against the Account from which the funds are to be transferred which prevents the funds transfer; or
f) We are restricted or prohibited by law from permitting the transfer to occur.

**55.5.5** Only in limited circumstances can We stop or countermand a transaction that has been processed.

### 55.6. Your security

It is your responsibility to obtain and maintain any Electronic Equipment, including any Mobile Device which You will need to have access to Internet Banking or the Mobile Banking App or effect a transaction within Internet Banking or via the Mobile Banking App. You must make every effort to ensure that your Access Codes and Electronic Equipment used to access Internet Banking and the Mobile Banking App are not misused, lost or stolen or defective in some way. If You fail to ensure the security of your Access Code or Electronic Equipment, You may be liable for transactions that occur on your Account.

You must take all reasonable steps to protect the security of your Electronic Equipment, ensuring that your Electronic Equipment does not have any viruses, trojans or other malware or any form of program or mechanism for recording your Access Identifiers, Access Codes or any other details required to access Internet Banking or the Mobile Banking App.

The guidelines in clause 58 are designed to help keep your Access Codes, Devices and any Electronic Equipment used to access Internet Banking or the Mobile Banking App secure. By following these guidelines, You can assist in preventing misuse of your Access Codes, Devices or any Electronic Equipment used to access Internet Banking or the Mobile Banking App.

Liability for Unauthorised Transactions will be determined in accordance with the ePayments Code and not under the guidelines in clause 59.

## 56. Cards

### 56.1. Issue of Cards

Each Card is for the sole use of the person authorised to use it and is only valid from the valid from date (if shown) to the valid end date (if shown) on it. If there is more than one Account Holder, then You are jointly and severally bound to comply with this PDS, and are liable for all amounts which are owing to Us at any time on the joint Account.

Each Card remains the property of IMB. You must return the Card as soon as We ask You to do so. We may cancel the Cards at any time in accordance with clause 56.16 or issue replacement Cards at any time for any reason. You must sign your Card as soon as You receive it.

We may charge a fee in relation to the issue of Cards. Refer to the **PDS - Fees, Charges and Limits** for details.

#### 56.1.1 Visa Debit Cards
Visa Debit Cards are available, in IMB's absolute discretion, to Account Holders aged 15 years or over who hold an eligible IMB Account. For details of eligible Accounts, see Part B.

#### 56.1.2 Updated Card Details to Merchants
If You provide your Card details to a merchant for a recurring payment, and your Card is reissued (e.g. due to expiry or replacing a compromised Card), the merchant may be provided the updated Card details where they participate in the Visa Account Updater service. You may opt-out of this service by contacting Us.

If a merchant is using a digital token or tokenised credentials, opting out of the Visa Account Updater service may not stop recurring payments with that merchant. In those instances, You must contact the merchant to request to cancel the recurring payment.

### 56.2. Accepting this agreement

#### 56.2.1 Accounts with no Personal Credit Line facility
Unless You have already accepted this agreement, the first time You or an Additional Cardholder use the Card or any other means to transact on your Account, You will automatically be accepting this agreement. This agreement then applies to all transactions on your Account.

If You do not want to accept this agreement, do not use your Card or permit an Additional Cardholder to use their Card. Instead, return all Cards to Us (cut in half for your protection), and contact IMB on 133 462 or call into one of our Branches to inform Us of your non-acceptance.

#### 56.2.2 Accounts with Personal Credit Line facility
Unless You have already accepted this agreement, the first time You or an Additional Cardholder use the Card or any other means to transact on your Account after the Personal Credit Line facility has been attached, You will automatically be accepting this agreement. This agreement then applies to all transactions on your Account.

If You do not want to accept the terms and conditions in this agreement relating to your Personal Credit Line facility, do not transact on your Account or permit an Additional Cardholder to transact on your Account after the Personal Credit Line facility is attached. You must then contact IMB on 133 462 or call into any IMB Branch to inform Us of your non-acceptance.

### 56.3. Other conditions
All terms and conditions applying to your Linked Accounts also apply when You or an Additional Cardholder use the Card on these Accounts.

### 56.4. Privacy
In addition to the privacy information contained in Part A of this PDS, the following information may apply to your Account.

#### 56.4.1 Account Users
If You have a Personal Credit Line facility attached to your Account, and your Account is in more than one person's name, each of You agrees that each person may use the Account and have access to Account information without any other Cardholder's consent.

#### 56.4.2 Monitoring of EFT Transactions
In some cases, surveillance devices such as cameras and video cameras may be used to monitor EFT Transactions at Interfaces.

### 56.5. Encoding
To gain access to the convenience of electronic banking Interfaces, including ATMs and EFTPOS, your Card will be encoded and your PIN will be linked to your registered Account. This will be completed by Us prior to issuing your Card.

Caution! When your Card is magnetically encoded and the Card is exposed to a strong magnetic field or comes into contact with a plastic security access Card, the encoded information may be destroyed. The Card may then be unusable in electronic Interfaces.

### 56.6. Additional Cardholder
You may nominate any person to be your agent to operate on your Account. If approved, We will issue that person with a Card linked to your Account.

You should ensure that any Additional Cardholder has read and understood this PDS. If your Additional Cardholder does not comply with this PDS, You will be in default.

You are liable to pay for (or to repay) any credit provided to any Additional Cardholder. Your Account will be debited with all transactions made by any Additional Cardholder. Accordingly, You are responsible for all these transactions as if You had made them yourself.

You must tell Us in writing if You want to cancel an additional Card or stop an additional Card from being used. We may not cancel the right to use the Card until it is returned to Us. You remain responsible for all transactions made with an additional Card until it is returned to Us.

You consent to Us giving an Additional Cardholder information about your Account.

## 56.7. Using the Card

### 56.7.1 Using the Card to obtain goods and services at a merchant

You can normally use the Card to obtain goods and services at merchants (such as shops, restaurants and theatres) in Australia and overseas where the Card symbol is displayed, as follows:

a) all Cards can be used in Australia;
b) your Cashcard can be used at any ATM or EFTPOS device and Bank@Post outlets; and
c) your Visa Card can be used throughout the world at participating merchants.

The fact that the Card symbol is displayed at a merchant's premises does not mean that We guarantee that all goods and services available there may be obtained by using the Card. We are not responsible if a merchant refuses to accept the Card, does not allow cash withdrawals or places other limitations on using the Card.

We have no control over the hours a merchant may be open for business. The hours during which an Interface will be available may therefore vary in accordance with the merchant's opening hours.

Where You use your Card to complete a transaction using contactless technology, or You swipe or dock your Card through or in an electronic card reader, or manually take an imprint of your Card (or allow a merchant to do any of these things), or You give a merchant your Card details over the telephone or internet, You acknowledge that by doing so this may affect your available balance by reserving the amount of the transaction.

You understand that the "contactless" and "small ticket" transaction services allow selected merchants to accept transactions on Cards without requiring them to obtain the Cardholder's signature or PIN, for transactions up to $100 AUD and $35 AUD respectively (or such other amount advised by Us or the merchant from time to time).

### 56.7.2 Using the Card to obtain goods and services via mail order, internet and telephone.

You can use the Card to obtain goods and services through mail order, internet and by telephone, where the merchant accepts that form of payment.

### 56.7.3 Authorisation

You must check that the correct amount is entered in an Interface or written in the total box on a voucher before You authorise the transaction or sign the voucher.

Some transactions need authorisation from Us. Acting reasonably, having regard to our legitimate business interests, We may choose not to authorise a proposed transaction, including but not limited to where We reasonably consider that there is a risk of loss or fraud through the use of particular merchants.

We are not responsible for goods or services obtained by using the Card, unless the law makes Us liable. Therefore, if You have any complaints about goods or services, You must take them up with the merchant.

### 56.7.4 Using the Card to obtain cash withdrawals

Subject to our daily cash withdrawals limits, You can obtain cash from your Account at any of our Branches up to the sum of your available credit limit and any deposit balance on your Card Account by presenting your Card at the counter and completing a withdrawal voucher.

You can also use the Card in combination with your PIN to obtain cash from any of our ATM and EFTPOS Interfaces and the ATM and EFTPOS Interfaces of any associated organisations (ask at any Branch for details).

You may also be able to obtain a cash withdrawal on your Account by presenting your Card at a Branch counter of some of these associated Organisations provided You wish to obtain a Visa cash advance only.

When obtaining cash at a Branch of any financial institution, You may be required to produce suitable identification which identifies the holder of the Card (such as photographic driver's licence or passport).

You may obtain cash with your Visa Card from any ATM or from any bank Branch throughout the world displaying the Visa logo.

The minimum amount of cash You can obtain using the Card may vary depending on which financial institution and ATM Interface You use the Card at. Some merchants who have Interfaces may also allow You to withdraw cash from your Linked Accounts at the same time as You pay for goods or services.

You may be able to transfer amounts from a nominated Account to another Account You have with Us. Those amounts transferred will be treated as cash transfers but do not form part of your daily cash limit. This service is only available for some Accounts, details are available from any of our Branches.

### 56.8. Vouchers

You agree that the amounts shown on each sales voucher and withdrawal slip are sufficient evidence of the cash price of the goods or services to which the voucher or withdrawal slip relates.

### 56.9. Using the Card - to access a Linked Account

You can use your Card and PIN or Access Code to gain access to your Linked Accounts at Interfaces.

### 56.10. Using the Card - Additional Cardholders

Each Additional Cardholder may use their Card on the same terms as those which apply to You under this clause 56.

### 56.11. Daily limits at ATMs

The maximum amount of cash You and an Additional Cardholder can obtain with the Card and PIN through ATMs on any one day is shown in the **PDS - Fees, Charges and Limits** and in Part A of this PDS. For this purpose each day ends at midnight New South Wales time.

### 56.12. Using an Interface

When You or an Additional Cardholder use the Card and PIN or Access Code at an Interface, You authorise Us to act on the instructions entered into the Interface.

If it is not possible to carry out the instructions You or an Additional Cardholder give an Interface on your Account, the transaction may be directed to a Linked Account.

Money is at your risk from when it becomes visible or available to You or an Additional Cardholder at an ATM.

### 56.13. How We process transactions if You use the Card outside Australia

Visa Card transactions are converted from the currency of the transaction to the Australian dollar equivalent or to United States dollars then to the Australian Dollar equivalent as at the date they are processed by Visa International at rates determined by Visa International.

This amount, plus the Visa Foreign Currency Conversion Fee of 1% which is charged on every transaction involving foreign currency, together with any other charges will then be debited to your Account.

A fee may be payable for each withdrawal processed overseas. We recommend that You check the relevant fees and charges from time to time.

All transactions are listed on your statement in the currency of the transaction and the Australian dollar equivalent.

### 56.14. What You must pay

You must pay Us for all amounts debited to the Card Account.

These include:

a) amounts shown on sales vouchers for goods and services obtained from a merchant either directly or by mail, internet, or telephone order;
b) the amount of all cash withdrawals;
c) interest charges;
d) government taxes, duties and charges payable by Us in connection with the Account (whether or not You are primarily liable to pay them) (details of some current government charges are given in the Schedule); and
e) our fees or charges referred to in clause 10.

If You overdraw your Account for any reason, or if You exceed the credit limit shown in your Loan Contract or personal credit line Schedule, the overdrawn amount will be treated as unplanned credit and the provisions of clause 7.1 will apply. You must repay any overdrawn amount immediately with interest and any costs incurred or administrative fees charged by Us. Where your Account is overdrawn, We may also charge You a Default Fee (see clause 10.4).

In addition, enforcement expenses and other enforcement costs may become payable by You in the event of a breach (see clause 7.1).

You are also liable for unauthorised use of your Card as set out in clause 59.

### 56.15. Closing your Account

You may close your Account at any time by telling Us in writing, returning all Cards on the Card Account (cut in half for your protection) and by complying with clause 56.17.

### 56.16. Cancellation and return of Cards

We may cancel any Card at any time after giving You at least 30 days' written notice.

Acting reasonably, having regard to our legitimate business interests, We may also cancel any Card without prior notice. Without limiting the reasons why We may do so, this may happen if:

- We reasonably consider You induced Us to issue your Card by fraud;
- We believe the Card is being used in a way that may cause loss to You or Us;
- We have reason to believe the security of the Card has been compromised; or
- We detect suspicious or unusual transaction activity.

The Card cannot be used if it is cancelled by Us. You must return all Cards on the Account (cut in half for your protection) immediately if:

- We close your Account;
- We cancel your Card; or
- We request You to do so.

### 56.17. Payment on closure or cancellation

We may charge You a fee for closing your Account that is a reasonable estimate of the costs of closure.

If You or We close your Account, or if We cancel your Card in any circumstances, You must immediately:

a) Return all Cards on your Account; and
b) Pay the full amount owing on demand from Us (this amount includes amounts for transactions not yet processed on the Account, government taxes and duties and other charges for the period up to closure or cancellation and any of our fees and charges incurred before closure or cancellation).

(Clause 59 applies if a Card is used without your knowledge or consent during that period.) You acknowledge that there is no agreement, arrangement or understanding between You and Us that We may demand repayment only when a particular event occurs or does not occur.

Also, You must repay any credit provided between the time of closure or cancellation and the time We receive back all Cards.

### 56.18. ATMs of other Organisations

Other Organisations can determine from time to time what transactions can be carried out at their ATMs. You should ask Us or the relevant Organisation for more information.

We do not warrant the ATMs of other Organisations are always available and fully functional. We do not accept any liability for any transaction made (or attempted to be made) at ATMs of other Organisations except to the extent that our systems or equipment are involved in the transaction. If our systems or equipment are involved in the transaction and You knew (or should have known) that the system was not working properly but went ahead and used it anyway, We may only have to correct any errors and refund relevant fees.

Where You use a non-IMB ATM You may be required to pay a direct charge to the ATM operator. You will be advised of any direct charge when You conduct the transaction at the ATM. Alternatively, if We have an alliance relationship with a particular ATM operator, We may have arrangements whereby You will not pay a direct charge, but may instead pay a transaction fee. Refer to the **PDS – Fees, Charges and Limits** for fees relating to ATM transactions.

### 56.19. Interface transactions


Our Visa Cards can be used to obtain cash in local currency at most overseas Interfaces displaying the Visa logo. Some keyboards at Interfaces do not display the letters of the alphabet as shown. The number which is equivalent to your PIN must be keyed to complete a transaction.

### 56.20. Lost Cards or PIN or Access Code revealed

You must tell Us and ensure that any Additional Cardholder tells Us as soon as possible if a Card is lost or stolen or You suspect that a PIN or Access Code is known to someone else or You suspect any unauthorised telephone or other use of the Account.

You may notify Us in Australia by contacting IMB on 133 462 8am to 8pm, Monday to Friday, Saturdays 9am to 4pm, or an after hours hotline on 1800 800 521.

In the case of a lost or stolen Visa Card, if You are overseas You may telephone the Visa Emergency Assistance Centre on +1 303 967 1090. You will need to give Us all relevant information You may have, so that We can suspend Card and Access Code access to your Account and Linked Accounts. You must confirm in writing any notice You give Us by telephone.

When You report the matter You may be given a notification number (or other form of acknowledgment). You should retain that number as confirmation of the date and time of your report.

In Australia if You are unable to report to Us because our facilities are unavailable during particular periods, You are not liable for any Unauthorised Transaction which could have been prevented if You had been able to tell Us. However, You must tell Us within a reasonable time after our facilities become available again.

## 58. Security of Cards, PINs and Access Codes

This section applies to all forms of electronic banking and the use of Cards.

The security of your Card, Access Code and/or PIN, and the Card, Access Code and/or PIN of Additional Cardholders is very important. You must make every effort to see that your Card, Access Code and any record of your PIN is not misused, lost or stolen. You must keep your Access Codes and PIN secret. Your Card is for your personal use only. You must not give your Card to another person to use or perform a transaction on your behalf. If You fail to observe the security requirements set out in this PDS You may incur increased liability for unauthorised use of your Card, Access Code or PIN (please refer to clause 59).

### 58.1. Protecting your PIN or Access Code

To protect your PIN or Access Code, You must:

a) try to memorise it;
b) destroy our letter telling You the PIN or Access Code;
c) not keep a record of your PIN or Access Code, or if You have a record ensure it is reasonably disguised (see clause 58.2 for further guidance);
d) not keep a record of your PIN or Access Code together with a record of your member number;
e) not keep a record of your PIN or Access Code stored in your Electronic Equipment;
f) not keep a record of your disguised PIN or Access Code on your Card;
g) not select a PIN or Access Code that is the same as, or similar to, any other code or PIN You have for any Account or Access Facility You have with Us;
h) if You select a PIN or Access Code, not select a number or word that can be easily associated with You, such as your date of birth, your marriage date, telephone number, bank Account number, car registration numbers, social security numbers, family members names, license number or children's birth dates or any other number that can be associated with You;
i) make sure nobody watches You enter your member number, PIN or Access Code into an Interface;
j) not enter your PIN or Access Code into a web page which has been accessed by a link from an Email, even if the Email may appear to have been sent by IMB;
k) only access IMB Internet Banking through IMB's website at imb.com.au;
l) check your Account statements regularly and report any Unauthorised Transactions promptly;
m) not disclose your PIN or Access Code or make it available to any other person (including a family member or friend); and
n) change your Access Code regularly.

### 58.2. What is NOT a reasonable attempt to disguise a PIN or Access Code

If You record your PIN or Access Code You must make a reasonable attempt to disguise it. The following are examples of what is NOT a reasonable attempt to disguise your PIN or Access Code:

a) recording your PIN or Access Code in reverse order;
b) recording your PIN or Access Code as a telephone number or part of a telephone number;
c) recording your PIN or Access Code as a telephone number in its correct sequence;
d) recording your PIN or Access Code among other numbers or letters with any of them marked to indicate the PIN or Access Code;
e) recording the PIN or Access Code disguised as a date; or as an amount;
f) recording your PIN or Access Code (in sequence or disguised format) and describing it as a PIN or Access Code or in any way that can be linked to your Card or electronic banking (e.g. IB code 0000 or IMB code 0000);
g) recording your PIN or Access Code using alphabetical characters or numbers (Example: A=1, B=2, C=3 etc); and
h) recording your PIN or Access Code in any low security electronic Device such as (but not limited to):
    i) calculators
    ii) personal computers
    iii) electronic organizers
    iv) mobile phones and smart phones
    v) diaries

There may be other forms of disguise which may also be unsuitable because of the ease of another person discerning your PIN or Access Code.

You must not act with Extreme Carelessness in failing to protect the security of all PINs and/or Access Codes.

### 58.3. Additional Cardholders

We also give each Additional Cardholder a PIN or Access Code. You must ensure that each Additional Cardholder protects their Card and stores their PIN or Access Code as safely as clause 58 requires You to protect and store yours.

### 58.4. If You think that your security has been compromised

**58.4.1** You must tell Us as soon as possible if:

a) You suspect that your PIN or Access Code is known to someone else or You suspect any unauthorised use of it; and/or
b) a Device or a piece of Electronic Equipment has been lost or stolen or You are aware or suspect that it has become subject to unauthorised use.

You may notify Us by calling IMB 133 462.

**58.4.2** You will need to provide Us with all the relevant information You may have, so that We can take appropriate actions to prevent any Unauthorised Transactions on your Accounts.

**58.4.3** If your Internet Banking password is stolen, You suspect that your Internet Banking password is known to someone else, or You suspect any unauthorised use of your Internet Banking password, You must immediately log on to Internet Banking and change your Internet Banking password.

**58.4.4** If You forget your PIN or Access Code You must inform IMB by calling 133 462 and have your PIN or Access Code replaced.

**58.4.5** If your Internet Banking registration is cancelled, or your Mobile Banking App access is cancelled, any future dated payments that You had authorised using Internet Banking will not be cancelled. You will need to arrange with IMB to have these payments cancelled.

**58.4.6** You will not be liable for any Unauthorised Transactions which occur after You notify Us of the loss, disclosure or theft of your PIN or Access Code subject to clauses 59.3 and 59.4 of this PDS.

### 58.5. Providing notification

**58.5.1** Where You are required to notify Us of the misuse, loss or theft of a piece of Electronic Equipment or that the security of the PIN or Access Code forming part of the Access Facility has or may have been breached, notification is deemed effective if provided by You by telephone to IMB on 133 462 or via Secure Email from Internet Banking. We will acknowledge all notifications You make to Us in accordance with this clause.

**58.5.2** If You are unable to notify Us because our facilities are unavailable (eg. outside of operating hours) You are not liable for any Unauthorised Transactions that have occurred and could have been avoided if You were able to notify Us. However, You must notify Us within a reasonable time after our facilities become available again.

## 59. Liability for Unauthorised Transactions

This section applies to all forms of electronic banking and the use of Cards.

An Unauthorised Transaction is a transaction which is not authorised by You or is a transaction that is executed without your knowledge or consent. No transaction entered into by You, an Authority to Operate, Delegated User, an Additional Cardholder or any other person acting with your knowledge or consent can be an Unauthorised Transaction for the purpose of this clause 59.

If You detect an Unauthorised Transaction, You should contact Us immediately on 133 462 between 8am to 8pm, Monday to Friday, 9am – 4pm Saturday or by Secure Email from Internet Banking. We will acknowledge any report You make to Us of a suspected Unauthorised Transaction.

This section provides guidelines in relation to your liability for Unauthorised Transactions. Please note, however, that liability for losses resulting from Unauthorised Transactions are ultimately determined in accordance with the ePayments Code, rather than these guidelines.

### 59.1. When You will not be liable for an Unauthorised Transaction and will get your money back

You will not be liable for:

a) losses that are caused by the fraudulent or negligent conduct of our employees or agents or companies involved in networking arrangements or merchants or their agents or employees;
b) losses related to any component of an Access Facility, Access Device, Access Identifier or Access Code which is forged, faulty, expired or cancelled;
c) losses relating to transactions that took place before You received your Access Device or Access Code;
d) losses that are caused by the same transaction being incorrectly debited more than once to the same Account;
e) losses resulting from Unauthorised Transactions occurring after You notify Us that your Card or a Device or any component of an Access Facility has been misused, lost or stolen or the security of your Access Code has been breached;

f) losses relating to conduct We expressly authorised that contributed to the Unauthorised Transaction;
g) losses arising from an Unauthorised Transaction where it is clear that You have not contributed to the loss and/or
h) losses relating to Unauthorised Transactions made using an Access Device where an Access Code was not required to complete the transaction, except where You unreasonably delay notifying Us of the loss or theft of the Access Device.

If, after our investigations, any of the above circumstances are deemed by Us to apply to You; We will reimburse the money that has been taken from your Account as a result of the Unauthorised Transaction.

### 59.2. When You will be liable and You won't get your money back

**59.2.1** Where clause 59.1 does not apply, You will be liable for losses resulting from Unauthorised Transactions where We can prove that You, on the balance of probability, contributed to the loss, as follows:
a) through fraud;
b) where You do any of the following:

i) voluntarily disclose any of your Access Codes or PIN to anyone (including to a family member or friend);
ii) keep a record of your Access Code on the outside of one or more of your Access Devices (e.g. your Card), pieces of Electronic Equipment forming part of an Access Facility (e.g. your smart phone), a Device, or on an article carried with any of the above items which is liable to loss or theft simultaneously with the item or is stored within the Device or piece of Electronic Equipment; or
iii) keep a record of your Access Code on any articles, without making a reasonable attempt to disguise them and that article;
iv) by selecting an Access Code which represents your birth date after We have asked that You not select such an Access Code and explained the consequences of doing so; or
v) by otherwise acting with Extreme Carelessness in failing to protect your Access Code.

c) by leaving your Card in an ATM (as long as the ATM incorporated reasonable safety standards that mitigate the risk of a Card being left in the ATM).

**59.2.2** Under clause 59.2.1, You will be liable for all actual losses which occur prior to You notifying Us that a Card, Device or a piece of Electronic Equipment forming part of an Access Facility has been misused, lost or stolen or the security of the Access Codes (including a PIN) and/or Access Identifiers forming part of the Access Facility have been breached.

**59.2.3** Notwithstanding clause 59.2.2, You will not be liable for:
a) the portion of losses incurred on any one day which exceed the applicable daily transaction limit(s);
b) the portion of the losses incurred in a period which exceeds any other periodic transaction limit(s) applicable to that period;
c) the portion of the total losses incurred on any Account which exceeds the balance in either that Account or your Linked Accounts; or
d) all losses incurred on any Accounts which We have agreed could not be accessed using the Card, PIN, Access Code, Access Identifier or Access Facility.

### 59.3. Your liability for unreasonably delaying notification

**59.3.1** If We can prove that You contributed to a loss caused by an Unauthorised Transaction by unreasonably delaying notifying Us after becoming aware, or where You should reasonably have become aware of:
a) the misuse, loss or theft of an Access Device or piece of Electronic Equipment forming part of the Access Facility; or
b) the security of the PIN or Access Code forming part of the Access Facility being breached; or
c) the misuse, loss or theft of an Access Device forming part of the Access Facility when an Unauthorised Transaction occurred in a situation that required an Access Device but not an Access Code;

You will be liable for all actual losses which occur between when You became aware or should reasonably have become aware and when You notified IMB.

**59.3.2** Notwithstanding clause 59.3.1, You will not be liable for:
a) the portion of losses incurred on any one day which exceed the applicable daily transaction limit(s);
b) the portion of the losses incurred in a period which exceeds any other periodic transaction limit(s) applicable to that period (for example where losses exceed the daily transaction limit for the Access Facility);
c) the portion of the total losses incurred on any Account which exceeds the balance in either that Account or your Linked Accounts;
d) all losses incurred on any Accounts which We have agreed could not be accessed using the Card, PIN, Access Code, Access Identifier or Access Facility.

### 59.4. When You have limited liability

Where your PIN or Access Code was required to perform an Unauthorised Transaction and it is not clear whether You contributed to the loss caused by an Unauthorised Transaction, the amount of your liability will be limited to the lesser of:

a) $150;
b) the balance of your Account(s) (including any Agreed Line Of Credit) from which money was transferred and which We have agreed may be accessed using the PIN or Access Facility at the time of the transaction; or
c) the actual loss at the time We were notified (where relevant) that the Card or Device or piece of Electronic Equipment forming part of the Access Facility has been misused lost or stolen or that the security of your PIN or Access Code has been breached (excluding that portion of the loss incurred on any one day which exceeds any applicable daily transaction or other periodic transaction limit(s).

### 59.5. Liability caused by equipment malfunction

**59.5.1** If the electronic banking system malfunctions, alternative manual procedures may be available from the merchant for retail point of sale transactions by using your Card and signing your authorisation of the transaction.

**59.5.2** We are responsible for any loss from a transaction caused by failure of an IMB electronic Interface to complete a transaction accepted by that electronic Interface in accordance with your instructions. We will correct the loss by making any necessary adjustment to the appropriate Account (including adjustment of interest or fees incurred as a result of the malfunction).

**59.5.3** We are responsible for any loss caused by failure of an IMB Interface to complete a transaction accepted by that Interface in accordance with your instructions.

**59.5.4** Notwithstanding clause 59.5.2 or 59.5.3, if You were aware, or should have been aware, that an Interface was unavailable for use or malfunctioning, our responsibility will be limited to correcting errors in the nominated Account and refunding any charges imposed as a result.

### 59.6. User instructions/OTP failure

We will be liable if an IMB Interface does not accept your or a User's instructions or an IMB Interface fails to accept your or a User's valid OTP.

### 59.7. Additional Cardholders

These exceptions apply equally if an Additional Cardholder contributes to the unauthorised use or Unauthorised Transactions in any of the ways listed in the exceptions.

### 59.8. Dispute Resolution procedure

**59.8.1** The procedures in this Clause 59.8 apply to complaints and reports concerning matters covered by this Part E of the PDS (including any apparent error in a transaction, Unauthorised Transaction or an error on your statement). They also apply to complaints and reports concerning BPAY (clause 61) and Osko (clause 62) if You are an individual, except for transactions using a facility designed primarily for use by a business, and established primarily for business purposes. If You have a complaint or a report of an Unauthorised Transaction, You must tell Us promptly. We will accept a complaint or a report of an Unauthorised Transaction, if it is received up to six years from the day on which You became aware, or should reasonably have become aware, of the circumstances giving rise to the complaint but the sooner You bring your complaint to our attention, the more likely We are to be able to resolve it quickly.

**59.8.2** If We are able to resolve the issue for You, We will do so immediately. If We can't resolve your issue on the spot, or before close of business on the fifth Business Day, We will provide You with a written response – whether We offer You the resolution You requested or not.

If You are not satisfied with our response to your complaint, please contact the IMB staff member who responded to your complaint to discuss the issue further.

Alternatively, or if You are not satisfied with the IMB staff member's response, to enable Us to better consider your complaint, We encourage You to direct your complaint in writing to:

**Member Relations IMB Ltd PO Box 2077, Wollongong NSW 2500**

When We receive your complaint, We will advise You in writing that We have received it.

In the case of certain complaints, We may also request additional information from You to help Us resolve your complaint. If You do not supply this additional information as requested, it may affect our ability to investigate and resolve your complaint in a timely manner.

**59.8.3** We will tell You either the outcome of our investigation or the fact that We need more time to complete our investigation. We will do this in writing within 30 days after We receive your complaint. In all but exceptional cases

(subject to IMB's discretion), We take less than 30 days to complete our investigation. (If it takes longer, We will tell You in writing).

**59.8.4** When We complete our investigation, We will advise You in writing of the outcome and our reasons for our decision, with reference to any relevant provisions of these Terms and Conditions and, where relevant, to sections of the ePayments Code.

**59.8.5** If We decide that your Account has been incorrectly debited or credited, We will promptly adjust the Account (including any fees and charges) and tell You in writing of the amount which has been debited or credited to your Account as a result. If We decide that your Account has not been incorrectly debited or credited, or in the case of Unauthorised Transactions that You contributed to part of the loss, We will provide You with copies of any document or other evidence on which We based our decision.

**59.8.6** If You are not satisfied with our decision, You may request a review of the decision by our senior management. We will also advise You of other avenues of dispute resolution that are available to You if We fail to observe the requirements of this PDS when We allocate liability.

**59.8.7** If, when conducting our investigation and dispute resolution procedures, there is an unreasonable delay or the outcome of our investigation is prejudiced, or We fail to comply with the provisions of the ePayments Code, We may accept full liability for the amount that is the subject of your complaint.

**59.8.8** If You are not satisfied with our decision, please talk to Us first. At any time, however, You can seek an external review of our decision. IMB is a member of the Australian Financial Complaints Authority (AFCA), which is a self-regulatory service providing an external and impartial dispute resolution process for retail members and customers of participating building societies, credit unions, banks and other financial service providers.

AFCA's determinations are binding upon IMB if You accept the decision.

**You can contact AFCA by:**

| | |
|---|---|
| Telephone | 1800 931 678 (Local call rate within Australia) |
| Facsimile | (03) 9613 6399 |
| Mail | AFCA, GPO Box 3, Melbourne VIC 3001 (Australia) |
| Website | afca.org.au |
| Email | info@afca.org.au |

This service is provided free of charge.

**59.8.9** We may choose to resolve certain complaints that relate to Cards under the relevant card scheme rules rather than in accordance with clauses 59.8.3 to 59.8.7. In the case that We choose to resolve a complaint in this way:

a) the timeframes set down by the relevant card scheme apply, instead of the timeframes set out above;
b) We will advise You of the relevant timeframes that apply to our investigation and when You can reasonably expect a decision;
c) if We are not able to resolve the complaint within 60 days We will give You:
    i) written notice of the reason for the delay;
    ii) updates on the progress of the complaint every two months;
    iii) a date when You can reasonably expect a decision (unless We are waiting on a response from You and We have advised You that We require your response);
d) We will advise You that We have suspended your obligation to pay any amount which is the subject of the complaint (and any credit or other charges related to that amount) until the complaint is resolved.

### 59.9. Notice of changes

If We change this clause 59, We will give You notice in accordance with clause 2.

**Guidance note**

- Where We have expressly authorised particular conduct, engaging in that conduct is not a contravention of the requirements of this clause 59.
- Where We have expressly or impliedly promoted, endorsed or authorised the use of an account access service then no disclosure, recording or storage of an Access Code by You that is required or recommended for the purposes of using that account access service is a contravention of the requirements of this clause 59.

## 60. Mistaken Internet Payments

**NOTE:** This clause 60 does not apply to BPAY or PayTo.

### 60.1. Mistaken Internet Payments Warning

ADIs rely solely on the PayID or BSB and account number (not the Payee Name or similar) to process payment instructions into and out of accounts. The 'Payee Name' (or similar) is for information purposes only and is not taken into account by ADIs when processing a payment instruction.

You must ensure that the PayID or BSB and account number You provide in relation to a payment instruction into or out of an account are correct. If the PayID or BSB and/or the account number are incorrect, the payment may be made to the wrong recipient. We will not be liable for any losses if the funds cannot be retrieved from the Unintended Recipient.

### 60.2. Reporting a Mistaken Internet Payment

You may report to Us that You believe a payment You have made to a Payee using Internet Banking or the Mobile Banking App is a Mistaken Internet Payment. We will acknowledge and investigate any report You make to Us under this clause 60.2.

The applicable processes and timeframes for investigating and responding to a report of a Mistaken Internet Payment are set out in this clause 60 and depend on how quickly You report the payment to Us. We encourage You to report any payment You believe to be a Mistaken Internet Payment to Us as soon as possible – how quickly You report the payment to Us may, in some circumstances, affect the proportion of the payment that can be recovered from the Unintended Recipient.

The processes outlined in this clause assume that the payment You are reporting to Us was initiated via the IMB Internet Banking system or the Mobile Banking App – that is that We are the Sending Institution. If You believe that a payment You have made from another ADI's internet banking system is a Mistaken Internet Payment, You should report the payment as such to the institution whose internet banking system You used to make the payment.

### 60.3. Process where the report is made within 10 Business Days after the payment

If We are satisfied that a Mistaken Internet Payment has occurred, We will request that the Receiving Institution return the funds. If the Receiving Institution is satisfied that a Mistaken Internet Payment has occurred and confirms that there are sufficient funds in the Unintended Recipient's Account, the Receiving Institution must return the funds to Us within 5 – 10 Business Days. Once We receive the funds from the Receiving Institution, We will return the funds to your Account as soon as practicable.

### 60.4. Process where the report is made between 10 Business Days and 7 months after the payment

If We are satisfied that a Mistaken Internet Payment has occurred, We will request that the Receiving Institution begin an investigation. The Receiving Institution may take up to 10 Business Days to complete their investigation. If the Receiving Institution is satisfied that a Mistaken Internet Payment has occurred, it must prevent the Unintended Recipient from withdrawing the funds for a further 10 Business Days. The Receiving Institution will notify the Unintended Recipient that the funds will be withdrawn from their Account at the expiration of the 10 Business Days unless the Unintended Recipient can establish that they are entitled to the funds. If the Unintended Recipient does not establish that they are entitled to the funds within this 10 Business Day period, the Receiving Institution will return the funds to Us within 2 Business Days of the expiry of the 10 Business Day period. Once We receive the funds from the Receiving Institution, We will return the funds to your Account as soon as practicable.

### 60.5. Process where the report is made more than 7 months after the payment

If We are satisfied that a Mistaken Internet Payment has occurred, We will request that the Receiving Institution return the funds. If the Receiving Institution is satisfied that a Mistaken Internet Payment has occurred, it will seek the consent of the Unintended Recipient to return the funds. If the Unintended Recipient consents, the Receiving Institution will return the funds to Us. Once We receive the funds from the Receiving Institution, We will return the funds to your Account as soon as practicable.

### 60.6. Process where a report is made but We are not satisfied that a Mistaken Internet Payment has occurred

If We are not satisfied that a payment You have reported to Us is a Mistaken Internet Payment We are not required to take any further action. In this case, You will be liable for any loss You may have sustained by making the payment.

### 60.7. Process where a report is made but the Receiving Institution is not satisfied that a Mistaken Internet Payment has occurred

If We are satisfied that a Mistaken Internet Payment has occurred but the Receiving Institution is not and there are sufficient funds in the Unintended Recipient's Account, the Receiving Institution may choose to seek the consent of the Unintended Recipient to return the funds. If We receive the funds from the Receiving Institution, We will return the funds to your Account as soon as practicable.

### 60.8. Process where a Mistaken Internet Payment has occurred but the funds are not available

If both We and the Receiving Institution are satisfied that a Mistaken Internet Payment has occurred but there are insufficient credit funds available in the Account of the Unintended Recipient to cover the full value of payment, the Receiving Institution will consider whether to pursue the return of funds (in part or in total) or not pursue return of any funds. The Receiving Institution must use reasonable endeavours to retrieve the funds from the Unintended Recipient if they choose to pursue the return of funds.

### 60.9. Process where the Unintended Recipient is in receipt of income support payments from Services Australia and Department of Veterans' Affairs

Where the Unintended Recipient is in receipt of income support payments from Services Australia or Department of Veterans' Affairs, the Receiving Institution must recover the funds in accordance with the Code of Operation.

### 60.10. Notification of outcome of report

Regardless of whether We are satisfied that a Mistaken Internet Payment has occurred and/or whether the payment has been successfully returned to You, We will notify You in writing of the outcome of your report within 30 Business Days of You making the report.

### 60.11. Complaints about Mistaken Internet Payments

**60.11.1** You may complain to Us about how We have dealt with your report of a Mistaken Internet Payment, including in regards to either We or the Receiving Institution:

a) not being satisfied that a Mistaken Internet Payment has occurred; or
b) not having complied with the processes or the timeframes set out in this clause 60 (which reflect ePayments Code requirements).

**60.11.2** Any complaints We receive under this clause 60.11 will be dealt with under our internal dispute resolution scheme (see Part H: Our Commitment to You), which may include referral to our external dispute resolution scheme provider if You are not satisfied with our internal response to your complaint.

**60.11.3** We will never require You to lodge a complaint with the Receiving Institution in the case of a Mistaken Internet Payment made using IMB Internet Banking or the Mobile Banking App.

## 60A. Confirmation of Payee

Effective from the date We enable CoP functionality. See our website for details.

### 60A.1 Confirmation of Payee Functionality

**60A.1.1** It is your responsibility to ensure the BSB and Account number You have entered are correct. If the CoP response indicates that the details do not match, You should check the Account Details with the intended recipient before proceeding with the payment. Your liability for payments will not be affected by any CoP match results shared with You.

**60A.1.2** You must not misuse CoP. We may limit or suspend your use for any reason without notice to You if We believe it is reasonably necessary to protect You or Us from possible fraudulent activity, scams or any other activity that may result in loss to You or Us.

**60A.1.3** We will use the Account Details as most recently provided by You and verified, as required by Us for the purposes of CoP. You must notify Us where there are changes to your personal details and provide Us with supporting evidence where We require.

**60A.1.4** We are not responsible for any information You or another party use in a CoP lookup or where a party refuses or delays a payment following a CoP lookup.

**60A.1.5** You acknowledge and authorise:

- Us to use and disclose your Account Details in the Confirmation of Payee service; and
- payers' financial institutions to use your Account Details for the purposes of the CoP service and prior to making payments to You.

### 60A.2 Privacy and Opt Out

**60A.2.1** 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 Act 1988 (Cth) and any regulations made under that Act, You acknowledge and agree that You consent to that disclosure, storage and use.

**60A.2.2** You may opt out of CoP in limited circumstances where the Account is eligible. Please contact Us on 133 462 or +61 2 4298 0111 (if overseas) for further information. We are not liable for any loss You may incur in connection with opting out of CoP.

**60A.2.3** Notwithstanding opting out of CoP, You acknowledge and authorise Us to:

- confirm, disclose, store and use your Account Details through CoP to government agencies for the purposes of making a payment to You by government agencies.
- acting reasonably, We may opt You back in to the CoP service without notice, where We consider it necessary to manage a risk such as for the purposes of protecting You or others from scams and frauds. We may disclose your Account details to other financial institutions through CoP to facilitate fraud processes.
- contact You to discuss a request to opt out or to remain opted out of CoP.

**60A.2.4** For joint Accounts, if at least one Account Holder has opted out, the Account will be opted out of CoP.

The Account may only be opted back in once every Account Holder that opted out of CoP for that Account elects to opt back in (except where We consider it necessary to opt the Account back in to CoP to manage a risk as previously described).

## Part F: Terms and Conditions for BPAY

### 61. BPAY Terms and Conditions

These BPAY Terms and Conditions apply if You ask Us to make a BPAY Payment on your behalf through the BPAY Scheme.

We are a member of the BPAY Scheme. The BPAY Scheme is an electronic payment scheme through which You can ask Us to make payments on your behalf to Billers who tell You that You can make BPAY Payments to them. We will tell You if We are no longer a member of the BPAY Scheme.

When You ask Us to make a BPAY Payment, You must give Us the information specified below under the heading "Information You must give Us". We will then debit your Account with the amount of that BPAY Payment. We may decide not to make a BPAY Payment if there are insufficient cleared funds in your Account at that time and clause 7.1 will apply. We are not acting as your agent or the agent of the Biller when We make a BPAY Payment on your behalf.

Further information on BPAY can be found at bpay.com.au

#### 61.1. How to use the BPAY Scheme to make a BPAY Payment

We will treat any instruction to make a BPAY Payment as authorised by You if, when it is given to Us (in the case of a BPAY Payment made using Internet Banking, the Mobile Banking App or Telephone Banking) your PIN is entered or (in the case of a BPAY Payment made using a Card), your Card and PIN are used at an ATM or other IMB Interface or via Internet Banking or the Mobile Banking App. We do not guarantee that any of our ATMs will be equipped to conduct BPAY Payments.

If there is any inconsistency in relation to the use of the BPAY Scheme between the terms and conditions set out in this Part F and the remainder of this PDS, the latter will apply to the extent of any inconsistency.

Information You must give Us.

You must give Us the following information when You make a BPAY Payment:

a) the Account from which You want Us to debit the BPAY Payment;
b) the amount of the BPAY Payment;
c) the Biller's Code of the Biller You wish to pay; and
d) the Biller customer reference number.

We do not have to effect a BPAY Payment if You do not give Us all of the above information or if any of that information is inaccurate.

#### 61.2. Payments

We may impose restrictions on the Accounts from which a BPAY Payment may be made or impose limits on the amount of BPAY Payments.

We will not accept an instruction to stop a BPAY Payment once You have instructed Us to make that BPAY Payment. You must notify Us immediately if You become aware that You may have made a mistake when instructing Us to make a BPAY Payment, or if You did not authorise a BPAY Payment that has been made from your Account (this does not apply to a mistake You make as to the amount You mean to pay - see below).

#### 61.3. Processing payments

We can decide the order in which payment services will be processed.

### 61.4. Valid Payment Direction

Billers who participate in the BPAY Scheme have agreed that a BPAY Payment You make will be treated as received by the Biller to whom it is directed:

a) on the date that You make that BPAY Payment, if You tell Us to make the BPAY Payment before our payment cut-off time on a banking Business Day; or
b) on the next Business Day, if You tell Us to make a BPAY Payment after our payment cut-off time on a Business Day or on a non Business Day; or
c) on the day or next Business Day that You have nominated for a Scheduled payment to take place.

A delay may occur in the processing of a BPAY Payment where:

a) there is a public or bank holiday on the day You tell Us to make a BPAY Payment;
b) You tell Us to make a BPAY Payment either on a day which is not a Business Day or after our payment cut-off time on a banking Business Day;
c) another financial institution participating in the BPAY Scheme does not comply with its obligations under the BPAY Scheme; or
d) a Biller fails to comply with its obligations under the BPAY Scheme.

### 61.5. When a Biller cannot process a payment

If We are notified that a Biller cannot process a BPAY Payment, We will:

a) advise You of this;
b) credit your Account with the amount of the BPAY Payment;
c) if You ask Us to do so, take all reasonable steps to assist You in making a BPAY Payment to that Biller as soon as possible.

### 61.6. Accuracy of information

You are responsible for ensuring:

a) the customer information provided to Us by You at the time of registration is accurate and that You inform Us promptly of any change to this information;
b) the accuracy of information provided to Us through Internet Banking, the Mobile Banking App or Telephone Banking.

If You discover that You instructed Us to make a payment to a Biller for an incorrect amount:

- if the amount You instructed Us to pay is greater than the required amount, contact the Biller for a refund; or
- if the amount is less than the required amount, You should make a further payment (using BPAY or another method) for the difference.

You may contact IMB to request a payment trace investigation with the Biller. This may result in You being referred back to the Biller and fees will apply for this service.

### 61.7. Changes to terms affecting BPAY

We reserve the right to vary these BPAY Terms and Conditions and will inform You of the changes in accordance with clause 2 of this PDS.

### 61.8. Suspension

We may suspend your right to participate in the BPAY Scheme at any time if You are suspected of acting in a fraudulent manner.

### 61.9. Cut-off times

If You instruct Us to make a payment before the times specified below it will in most cases be treated as having been made on the same day.

Cut-off times:

a) Monday - Friday: 4:00pm New South Wales time
b) Saturday, Sunday and Public Holidays: Processed next Business Day.

Where You make a payment authorisation outside of these times or on a non-Business Day, We will hold the amount You have requested for payment in a payment file, but will not process the payment until the next Business Day.

NB. You will not earn interest on the funds the subject of your payment authorisation where it is made outside business hours, while it awaits processing on the next Business Day.

BPAY Payments may take longer to be credited to a Biller if You tell Us to make a BPAY Payment on a Saturday, Sunday or public holiday or if the Biller does not process a payment as soon as they receive its details.

### 61.10. Account records

You must check your Account records carefully and immediately report to Us as soon as You become aware of any BPAY Payment that You think is erroneous, or made by someone else without your permission.

### 61.11. Liability for mistaken payments, Unauthorised Transactions and fraud

You must tell Us immediately if:

a) You become aware of any delays or mistakes in processing your BPAY Payments; or

b) 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 Payment in the way described in this clause. If the ePayments Code applies to your Account and a BPAY Payment is made on your Account without your knowledge or consent, liability for that unauthorised BPAY Payment will be determined in accordance with clause 59.

Otherwise, to the extent permitted by any applicable law or code, We are not liable for any consequential loss or damage You suffer as a result of using the BPAY Scheme other than any loss or damage which is due to our negligence or breach of any condition or warranty implied by law which cannot be excluded restricted or modified at all or only to a limited extent.

If a BPAY Payment is made to a person or for an amount which is not in accordance with your instructions (if any), and your Account has been debited with the amount of that payment, We will credit that amount to your Account. However, if You were responsible for a mistake resulting in that payment and We cannot recover within 20 banking Business Days of Us attempting to do so from the person who received the amount of that payment, You must pay Us that amount.

If a BPAY Payment is made in accordance with a payment direction which appeared to Us to be from You or on your behalf but for which You did not give authority, We will credit your Account with the amount of that unauthorised payment.

However, You must pay Us the amount of that unauthorised payment if:

a) We cannot recover that amount within 20 banking Business Days of Us attempting to do so from the person who received it; and

b) the payment was made as a result of the payment direction which did not comply with any requirements We may have for such payment direction;

except in respect of any loss or liability arising from our fraud, negligence or wilful misconduct (or of our employees, contractors or agents).

If a BPAY Payment is induced by the fraud of a person involved in the BPAY Scheme, then that person should refund You the amount of the fraud induced payment.

However, if that person does not refund You the amount of the fraud induced payment, You must bear that 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 We will attempt to obtain a refund for You of the fraud induced payment.

You indemnify Us against any loss or damage We may suffer due to any claims, suits, demands or action of any kind brought against Us arising directly or indirectly because You:

a) did not observe any of your obligations under the BPAY Scheme terms and conditions; or

b) acted negligently or fraudulently in connection with the other terms and conditions of your Account.

If You tell Us that a BPAY Payment made from your Account is unauthorised, You must first give Us your written consent addressed to the Biller who received that BPAY Payment, consenting to Us obtaining from the Biller information about your account with that Biller or the BPAY Payment, including your customer reference number and such information as We reasonably require to investigate the BPAY Payment.

We are not obliged to investigate or rectify any BPAY Payment if You do not give Us this consent. If You do not give Us that consent, the Biller may not be permitted under law to disclose to Us information We need to investigate or rectify that BPAY Payment.

### 61.12. Disputes

If You have a complaint which relates to the BPAY Scheme and You are not an individual, or your complaint or dispute is in relation to transactions using a facility designed primarily for business purposes, then We will resolve your dispute in accordance with dispute resolution procedures established under the BPAY Scheme. Otherwise We will resolve your dispute in accordance with the procedures in clause 59.8.

### 61.13. Registration & cancellation of BPAY View

**61.13.1** You are required to register to use BPAY View for each Biller from whom You wish to receive your bill electronically.

**61.13.2** You can cancel your registration for each Biller at anytime through Internet Banking.

**61.13.3** If You register for BPAY View, You:

a) agree to IMB disclosing to Billers nominated by You:

   i) such Personal Information (for example your name, Email address and the fact that You are our member) as is necessary to enable the Billers to verify that You can receive bills and statements electronically using BPAY View (or telling them if You cease to do so); and

   ii) that an event in clause 61.14 b), c), d), e) or f) has occurred.

b) agree to Us or a Biller (as appropriate) collecting data about whether You access your Emails, Internet Banking and any link to a bill or statement;

c) agree where You register to receive a bill or statement electronically through BPAY View, You are entitled to receive that bill or statement from the applicable Biller;

d) agree to receive bills and statements electronically and that this satisfies the legal obligations (if any) of the Biller to give You bills and statements. For the purposes of this clause We are the agent for each Biller nominated by You under a) above; and

e) agree to direct any enquiries relating to a bill or statement You receive to that Biller.

## 61.14. Receiving paper bills

You may receive paper bills and statements from a Biller instead of electronic bills and statements:

a) at your request to a Biller (a fee may be charged by the applicable Biller for supplying the paper bill or statement to You if You ask for this in addition to an electronic form);

b) if You deregister a Biller from BPAY View;

c) if We receive notification that your internet Email mailbox is full, so that You cannot receive any Email notification of a bill or statement;

d) if your internet Email address is incorrect or cannot be found and your Email is returned to Us undelivered;

e) if We are aware that You are unable to access your Email or our service or a link to a bill or statement for any reason;

f) if any function necessary to facilitate BPAY View malfunctions or is not available for an extended period.

We accept no liability to provide You with a paper bill or statement in any of these circumstances unless We are the Biller.

## 61.15. Notice of electronic bills or statements

**61.15.1** You will receive notification to your Nominated Email Address that an electronic bill or statement has been received in your Internet Banking.

**61.15.2** You agree that when using BPAY View:

a) if You receive an Email to your Nominated Email Address notifying You that You have a bill or statement in your Internet Banking site, then the bill or statement is received by You:

   i) when We receive confirmation that your server has received the Email notification, whether or not You choose to access your Email; and

   ii) at the Email address nominated by You;

b) if You receive notification on Internet Banking without an Email then the bill or statement is received by You:

   i) when a notification is posted on our Internet Banking site, whether or not You choose to access Internet Banking; and

   ii) on our Internet Banking site;

c) bills and statement delivered to You, unless deleted by You, remain accessible through Internet Banking for the period determined by the Biller up to a maximum of 18 months after which they will be deleted, whether paid or not; and

d) You will contact the Biller direct if You have any queries in relation to bills or statements.

**61.15.3** You must:

a) check your Emails or Internet Banking weekly;

b) tell Us if your contact details (including your Nominated Email Address) change;

c) tell Us if You are unable to access your Email or Internet Banking or a link to a bill or statement for any reason; and

d) ensure your mailbox can receive notifications (eg. has sufficient storage space available).

**61.15.4** Unless expressly provided for in this clause 61, We are not responsible for arranging or ensuring that any Biller You nominate will make bills and statements available to You. If You fail to receive bills and statements from a Biller or the bill or statement is not available to be viewed using BPAY View You should contact the applicable Biller to obtain a paper bill or statement.

### 61.16. BPAY View billing errors

**61.16.1** A BPAY View billing error means any of the following:

a) if You successfully registered with BPAY View:

   i) failure to give You a bill (other than because You failed to view an available bill);
   ii) failure to give You a bill on time (other than because You failed to view an available bill on time);
   iii) giving a bill to the wrong person; or
   iv) giving a bill with incorrect details;

b) if your BPAY View deregistration has failed for any reason, giving You a bill if You have unsuccessfully attempted to deregister.

**61.16.2** You agree that if a billing error occurs:

a) You must, immediately upon becoming aware of the billing error, take all reasonable steps to minimise any loss or damage caused by the billing error, including contacting the applicable Biller and obtaining a correct copy of the bill; and

b) the party who caused the error is responsible for correcting it and paying any charges or interest which would ordinarily be payable to the applicable Biller due to any consequential late payment and as a result of the billing error.

**61.16.3** You agree that for the purposes of clause 61.16.1 and 61.16.2, You are responsible for a billing error if the billing error occurs as a result of an act or omission by You or the malfunction, failure or incompatibility of computer equipment the User is using at any time to participate in BPAY View.

## Part G: Terms and Conditions for Osko, PayID and other NPP Payments

This Part G of the PDS applies to the use of Osko, PayID and other NPP Payments.

### 62. Osko

#### 62.1. Osko

Osko is an NPP Payments service that allows customers to make and receive payments in near real-time. We subscribe to Osko under the BPAY Scheme.

#### 62.2. Availability

You can make Osko Payments in Internet Banking or the Mobile Banking App.

Osko Payments can be made from most IMB deposit Accounts, but not from Term Deposit Accounts.

You can only make an Osko Payment to a Payee with an account at another financial institution if that other financial institution supports Osko Payments. The Payee's account must also be able to receive the Osko Payment. For example, if the Payee's account type is one that is not permitted by the Payee's financial institution to receive Osko Payments, You will not be able to make an Osko Payment to that account.

Osko Payments can also be received by You into most IMB deposit Accounts, but not Term Deposit Accounts. Osko Payments can also be received into IMB loan Accounts.

Please refer to the descriptions of deposit Accounts in Section 5, Part B of this PDS for details of those deposit Accounts from which Osko Payments can be made and which can receive Osko Payments.

You must comply with the terms and conditions applying to the Account to which You request Us to credit or debit an Osko Payment and the service You use to participate in Osko. If there is any inconsistency between the terms and conditions applying to the relevant Account or service and this Section 5 Part G, this Section 5 Part G will apply to the extent of that inconsistency.

We will tell You if We are no longer able to offer You Osko. If We are no longer able to offer You Osko, You will not be able to send or receive Osko Payments through Us.

Where We are able to do so We will tell You if there are any delays in processing Osko Transactions and when your Osko Transaction is likely to be completed.

#### 62.3. Osko Transaction limits

We may impose restrictions on the Accounts from which Osko Payments may be made or which can receive Osko Payments, and impose limits on the amount of Osko Payments that may be made or received. Any restrictions are set out in the **PDS – Fees, Charges and Limits**.

### 62.4. How to make an Osko Payment

You must give Us the following information when You make an Osko Payment:
a) the Account from which You want Us to debit the Osko Payment;
b) the amount of the Osko Payment; and
c) the PayID or bank account details of the account You wish to pay.

Please refer to clause 63 of this PDS for terms and conditions for PayID.

When initiating an Osko Transaction, You might direct the Osko Transaction to an incorrect account if You get the BSB and account number, or the PayID wrong. To try to avoid making a payment to an incorrect PayID, We will ask You to verify that You have the right PayID. We will do this by presenting You with the associated PayID Name as an additional confirmation of the intended recipient before You submit an Osko Transaction. You will need to confirm this information before the Osko Transaction is processed by Us.

When You have provided all the information required to make an Osko Payment and confirmed the PayID if applicable, We will then debit the Account You specify with the amount of that Osko Payment.

You should ensure that all information You provide in relation to an Osko Payment is correct as We will not be able to cancel an Osko Payment once it has been submitted.

We do not have to effect an Osko Payment if You do not give Us all of the above information or if any of the information You give Us is inaccurate.

We will treat any Osko Payment direction made using Internet Banking or the Mobile Banking App as authorised by You if when it is given to Us, your login details including PIN have been used to access Internet Banking or the Mobile Banking App.

We may require You to authenticate Osko Transactions in our complete discretion. Where We require You to authenticate an Osko Transaction We will send an OTP via SMS. You will be required to enter this OTP in to the current Internet Banking session You are logged into before You can make a payment to a PayID Payee the first time You send a payment to that PayID Payee.

### 62.5. Receiving an Osko Payment

You can receive an Osko Payment into an eligible IMB Account. For details of eligible IMB Accounts, refer to clause 62.2.

To receive an Osko Payment You must provide the Osko Payer with:
a) the amount of the Osko Payment; and
b) your PayID or IMB bank Account details.

If You use PayID You must have a PayID linked to your Account to be credited with the Osko Payment.

If You provide the wrong details to the Osko Payer, the payment will not be credited to your Account.

### 62.6. Osko Adjustments

**62.6.1** An Osko Adjustment is an Osko Transaction initiated by Us or You to adjust or reverse an Osko Payment which has already been settled and cleared. An Osko Adjustment may arise as a result of:
a) an Osko Payment Return;
b) a Mistaken Osko Payment;
c) an Error Osko Payment;
d) a Misdirected Osko Payment;
e) an Osko Overpayment;
f) a Duplicate Osko Payment;
g) a payment processing error made by an NPP participating financial institution;
h) an Osko Payment that has been made without your authorisation; or
i) a fraudulent Osko Payment (including fraud arising in connection with the use of a PayID).

**62.6.2** You can request an Osko Adjustment if You believe that an Osko Payment from or to your IMB Account is one of the transactions described in clause 62.6.1. However, just because You made a request does not mean that an Osko Adjustment will be made. Whether an Osko Adjustment will be made, and your liability, is dealt with in clauses 62.7 to 62.11.

**62.6.3** We may make an Osko Adjustment if We agree to your request for an Osko Adjustment or when We decide to do so, but only when We are required to make the adjustment or have the right to make the adjustment under the rules that apply to participants in Osko and the NPP. We will follow those rules in relation to Osko Adjustments.

**62.6.4** If You receive an Osko Payment to your Account, the Osko Payer may also seek an Osko Adjustment for that payment. Whether an adjustment will be made, and your liability, is dealt with in clauses 62.7 to 62.11.

### 62.7. Mistaken Osko Payments

A Mistaken Osko Payment will be dealt with as a Mistaken Internet Payment, refer to clause 60.

### 62.8. Misdirected Osko Payments

If We determine that a settled Osko Payment from your Account is a Misdirected Osko Payment, We may request a return of the payment from the Osko Payee's financial institution. That financial institution must use reasonable endeavours to assess and determine whether it is a Misdirected Osko Payment, and if it is satisfied that the payment is a Misdirected Osko Payment, it must make the payment return within the timeframes specified in clause 62.10.7.

Where We and the sending financial institution determine that an Osko Payment made to your Account is a Misdirected Osko 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 Misdirected Osko Payment. We will notify You if this occurs.

### 62.9. Duplicate and Error Osko Payments, and Osko Overpayments

If We determine that a settled Osko Payment from your Account is:

a) a Duplicate Osko Payment;
b) an Error Osko Payment; or
c) has been sent as a result of our own error,

or if You request a return of all of an Osko Overpayment (or the amount overpaid), We may request a return of the payment from the Osko Payee's financial institution. That financial institution must use reasonable endeavours to assess and determine whether the payment is one of the payments described above, and if it is satisfied that it is one of these payments, it may make a payment return (or return the amount overpaid) within the timeframes specified in clause 62.10.7.

### 62.10. Payment disputes and investigations

**62.10.1** You may ask Us to investigate an Osko Transaction.

**62.10.2** You must tell Us immediately if:

a) You become aware of any delays or mistakes in processing your Osko Payments; or
b) You think that You have been fraudulently induced to make an Osko Payment.

**62.10.3** We will attempt to rectify any such matters in relation to your Osko Payment in the way described in this clause 62 (and clause 60 where relevant).

**62.10.4** If You have a complaint which relates to Osko and You are not an individual, or your complaint or dispute is in relation to transactions using a facility designed primarily for use by a business, and established primarily for business purposes, then We will resolve your dispute in accordance with dispute resolution procedures established for Osko by BPAY. Otherwise We will resolve your dispute in accordance with the procedures in clause 59.8.

**62.10.5** We will keep You informed of the progress of all disputes and investigations. However We may not notify You or keep You informed of certain investigations and disputes where We reasonably determine that doing so will, or is likely to, compromise the integrity of the investigation or Osko more broadly.

**62.10.6** If You tell Us that an Osko Payment made from your Account is unauthorised, You must first give Us your written consent addressed to the Osko Payee who received that Osko Payment, consenting to Us obtaining from the Osko Payee information about your Osko Payment, including such information as We reasonably require in order to investigate the Osko Payment. We are not obliged to investigate or rectify any Osko Payment if You do not give Us this consent. If You do not give Us that consent, the Osko Payee may not be permitted under law to disclose to Us information We need to investigate or rectify that Osko Payment.

**62.10.7** If We request an Osko Payment Return for an Osko Payment, the payee financial institution should resolve a request for payment return within 10 Business Days if the request is initiated because of a complaint or request made by You to Us. If the payee financial institution cannot resolve the request for payment returned within 10 Business Days, for example because your request is some time after the original Osko Payment, the payee financial institution must send Us a pending status message indicating that the case is still being investigated. Where the request for payment return is initiated by Us due to a Duplicate Osko Payment or due to a processing error made by Us, the payee financial institution should respond to the request within 24 hours, on a best endeavours basis.

### 62.11. Liability

**62.11.1** You will not be liable for a Misdirected Osko Payment from your IMB Account except to the extent that You cause, or contribute to, the addressing error in the Misdirected Osko Payment.

**62.11.2** If a financial institution participating in the NPP that services accounts with PayID (including IMB) fails to comply with its obligations under the NPP in relation to registration and maintenance of the PayID, You will not be liable for fraud resulting from or caused by that failure, except to the extent that You cause or contribute to the relevant addressing error.

**62.11.3** You will not be liable for any loss or damage to Us or another financial institution participating in NPP from a claim brought against Us or the other financial institution as a result of relying on the PayID information from the NPP addressing lookup service, except to the extent that You cause, or contribute to, the addressing error. This does not apply to loss or damage from fraud (see clause 62.11.2 which applies in the case of fraud).

**62.11.4** If an Osko Payment from your IMB Account is an Unauthorised Transaction (see clause 59), liability for an Unauthorised Transaction will be determined in accordance with clause 59.

**62.11.5** Except as set out in clauses 62.11.1 to 62.11.4, to the extent permitted by any applicable law or code:

a) We are not liable to You for any funds that You did not recover from an Osko Payment from your IMB Account where You have requested (or have the right to request) an Osko Adjustment, or any other loss or damage arising from your failure to recover those funds, provided that We have followed the procedures in this clause 62 if You requested an Osko Adjustment;
b) We are not liable for any consequential loss or damage You suffer as a result of using Osko, other than any loss or damage which is due to our negligence or breach of any condition or warranty implied by law which cannot be excluded restricted or modified at all or only to a limited extent; and
c) You are liable for any loss or damage to You or Us from fraudulent Osko Payments where the responsibility for the fraud is attributable to your conduct.

**62.11.6** To the full extent permitted by law, You indemnify Us against any loss or damage We may suffer due to any claims, suits, demands or action of any kind brought against Us arising directly or indirectly because You:

a) did not observe any of your obligations under the Osko or PayID Terms and Conditions in this PDS; or
b) acted negligently or fraudulently in connection with the other terms and conditions of your Account.

### 62.12. Notifications

Subject to clause 62.10.5, We will inform You via Internet Banking or the Mobile Banking App when:

a) We confirm and validate each Osko Payment direction You give Us;
b) an Osko Transaction You have initiated is successfully completed or fails for any reason; and
c) an Osko Payment has been deposited into your Account.

In Internet Banking and the Mobile Banking App You can also set up Email and SMS alerts for when You receive an Osko Payment to your Account. You may enable Push Notifications to receive alerts about Osko Payments (effective from date functionality is available in Mobile Banking App).

You may also, at any time, access a record of all Osko Transactions which You have been involved with via Internet Banking or the Mobile Banking App.

### 62.13. Suspension and termination

We may suspend or terminate your participation in Osko as provided in clause 3, or if We cease to offer Osko.

### 62.14. Changes to terms affecting Osko

We reserve the right to vary these Osko Terms and Conditions and will inform You of the changes in accordance with clause 2.

## 63. PayID

### 63.1. Making and receiving NPP Payments using PayID

The PayID Service is the NPP Payment addressing service that enables payers to make NPP Payments (including Osko Payments) to Payees using an alternative identifier instead of Account details.

You can create a PayID for your eligible IMB Account. For details of eligible Accounts, see clause 62.2.

You are not required to have a PayID for your Account, and You do not have to use a PayID when You are making an Osko Payment. However if You do not have a PayID for your Account, You will not be able to receive Osko Payments to your Account using a PayID. Instead, You will need to provide your BSB and Account number to the Osko Payer.

Whether You choose to create a PayID for your Account or not, You and each ATO may use a Payee's PayID to make Osko Payments to the Payee from your Account if:

a) We and the Payee's financial institution support Osko payment service;
b) the Payee's account is able to receive the particular Osko Payment; and
c) the PayID is not locked.

### 63.2. Choosing a PayID

We currently support the following PayID Types:
a) mobile phone number; and
b) Email address.

We will publish a list of supported PayID Types from time to time.

You may create a PayID as long as it is a supported PayID Type. Some PayID Types may be restricted to business customers and Organisations. Only eligible customers will be able to create a PayID that is a restricted PayID Type.

You must satisfy Us that You own or are authorised to use your chosen PayID before You can use it to receive Osko 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.

Depending on the policy of a payer's financial institution, your PayID Name may be displayed to payers who send Osko Payments to You.

At the same time as You create your PayID, We will provide You with a PayID Name.

### 63.3. Creating your PayID

Before You can create your PayID to receive Osko 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 which can receive Osko Payments. For details of eligible Accounts see clause 62.2.

You can create a PayID for receiving NPP Payments in Internet Banking or in the Mobile Banking App. When You create your PayID in Internet Banking or the Mobile Banking App, We will send You an OTP via SMS if You are registering your mobile phone number as your PayID, or via Email where You are registering your Email address as your PayID. You will be required to enter this OTP in the Internet Banking session You are logged into to complete registration of the PayID.

We will not create a PayID for You without your prior consent.

You may choose to create more than one PayID for your Account.

If your Account is a joint Account, You and each other joint Account Holder can create a unique PayID for the Account.

If You have an ATO on your Account, each ATO may create a unique PayID for the Account.

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 63.5 for details on transferring PayIDs.

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 receive a message advising that the service is unable to register the PayID. We cannot disclose details of any Personal Information in connection with duplicate PayIDs.

### 63.4. Recording your PayID

We will ensure that your PayID and Account details are accurately recorded in the PayID Service.

### 63.5. Transferring your PayID

You can request transfer of your PayID at any time.

You can transfer your PayID to another Account with Us, or to an account with another financial institution by submitting a request to Us in Internet Banking.

A transfer of your PayID to another Account with Us will generally be effective immediately, unless We notify You otherwise.

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, Osko 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.

A locked PayID cannot be transferred.

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.

### 63.6. Closing a PayID

To close your PayID, follow the instructions in Internet Banking or the Mobile Banking App. Once a PayID is closed, it is removed from the PayID Service and cannot be used for Osko Payments.

You must notify Us immediately if You no longer own or have authority to use your PayID.

### 63.7. Locking and unlocking a PayID

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 Osko Payments fraudulently.

You can request that We unlock a PayID that We have locked. We do not have to agree to your request. In Internet Banking You can lock your own PayID and unlock a PayID that You have locked.

### 63.8. Joint Accounts

When You direct an Osko Payment to a PayID connected to a joint account, other account holders may be able to see the messages and notifications associated with the Osko Payment. Similarly other Account Holders on your Account may be able to see messages and notifications associated with Osko Payments addressed to your PayID.

### 63.9. Privacy

By creating your PayID You acknowledge that You authorise:

a) Us to record your PayID, PayID Name and Account details (including full legal Account name) (PayID record) in the PayID Service; and

b) Osko payers' financial institutions to use your PayID information for the purposes of constructing Osko Payment messages, enabling Osko Payers to make Osko Payments to You, and to disclose your PayID Name to Osko Payers for Osko Payment validation.

To the extent that the creation and use of the PayID record constitutes a disclosure, storage and use of your Personal Information, You acknowledge and agree that You consent to that disclosure, storage and use.

## 63A. PayTo

Effective from the date We enable PayTo functionality.

### 63A.1 Creating a Payment Agreement

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

b) If You elect to establish a Payment Agreement with a Merchant or Payment Initiator that offers PayTo, You may be required to provide that Merchant or Payment Initiator with your personal information including your Account number/BSB 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 provided to the Merchant or Payment Initiator will be subject to the privacy policy and terms and conditions of the relevant Merchant or Payment Initiator.

c) Payment Agreements must be recorded in the Mandate Management Service in order for NPP Payments to be processed in accordance with them. The Merchant or Payment Initiator is responsible for creating and submitting a record of each Payment Agreement to their financial institution or payments processor for inclusion in the Mandate Management Service. The Mandate Management Service will notify Us of the creation of any Payment Agreement established using your Account or PayID details. We will deliver a notification of the creation of the Payment Agreement to You and provide details of the Merchant or Payment Initiator named in the Payment Agreement, the payment amount and payment frequency (if these are provided to seek your confirmation of the Payment Agreement). You may authorise or decline any Payment Agreement presented for your approval. If You authorise, We will record your authorisation against the record of the Payment Agreement in the Mandate Management Service and the Payment Agreement will then be deemed to be effective. If You decline, We will note that against the record of the Payment Agreement in the Mandate Management Service.

d) We will process payment instructions in connection with a Payment Agreement, received from the Merchant's or Payment Initiator's financial institution, only if You have authorised the associated Payment Agreement. Payment instructions may be submitted to Us for processing immediately after You have authorised the associated Payment Agreement so You must ensure the details of the Payment Agreement are correct before You authorise 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 authorised.

e) If a Payment Agreement requires your authorisation within a timeframe stipulated by the Merchant or Payment Initiator, and You do not provide authorisation within that timeframe, the Payment Agreement may be withdrawn by the Merchant or Payment Initiator.

f) If You believe the payment amount or frequency or other detail presented is incorrect, You should decline the Payment Agreement and contact the Merchant or Payment Initiator and have them resubmit the Payment Agreement creation request.

### 63A.2 Amending a Payment Agreement

a) Your Payment Agreement may be amended by the Merchant or Payment Initiator from time to time, or by Us on your instruction.

b) We will send You notification/s of proposed amendments to the payment terms of the Payment Agreement as 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. We will deliver a notification of the proposed amendment to You for authorisation. You may authorise or decline any amendment request presented for your authorisation. If You authorise, We will record the authorisation against the record of the Payment Agreement in the Mandate Management Service and the amendment will then be deemed to be effective. If You decline, the amendment will not be made. A declined amendment will not otherwise affect the Payment Agreement.

c) Amendment requests which are not confirmed or declined within 6 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.

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

e) Once an amendment request has been authorised by You, We will promptly update the Mandate Management Service with this information.

f) Once a Payment Agreement has been established, You may instruct Us to amend your 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. You may not request Us to amend the details of the Merchant or Payment Initiator, or another party.

**63A.3 Pausing or resuming a Payment Agreement**

a) You may instruct Us to pause and resume your Payment Agreement via Internet Banking. 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.

b) Merchant 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.

**63A.4 Cancelling a Payment Agreement**

a) You may instruct Us to cancel a Payment Agreement via Internet Banking. We will act on your instruction promptly by updating the record of the Payment Agreement in the Mandate Management Service. The Mandate Management Service will notify the Merchant's or Payment Initiator's financial institution or payment processor of the cancellation.

b) You will be liable for any loss that You suffer because of the cancellation of a Payment Agreement that is in breach of the terms of an agreement between You and the relevant Merchant or Payment Initiator.

c) Merchants and Payment Initiators may cancel Payment Agreements. If the Merchant or Payment Initiator cancels a Payment Agreement to which You are a party, We will notify You of the cancellation. We will not be liable to You or any other person for loss incurred as a result of cancellation of your Payment Agreement by the Merchant or Payment Initiator.

**63A.5 Migrating Direct Debit arrangements**

a) Merchants and Payment Initiators who have existing Direct Debit arrangements with their customers, may establish Payment Agreements for these, as Migrated DDR Mandates, in order to process payments under those arrangements via the NPP rather than the Bulk Electronic Clearing System ("BECS"). We are not able to migrate your existing Direct Debits unless actioned by the Merchant or Payment Initiator.

b) If You have an existing Direct Debit arrangement with a Merchant or Payment Initiator, You may be notified by them that future payments will be processed from your Account under PayTo. You are entitled to prior written notice of variation to your Direct Debit arrangement and changed processing arrangements, as specified in your Direct Debit Service Agreement, from the Merchant or Payment Initiator. If You do not consent to the variation, You must advise the Merchant or Payment Initiator. We are not obliged to provide notice of a Migrated DDR Mandate to You for You to confirm or decline. We will process instructions received from a Merchant or Payment Initiator on the basis of a Migrated DDR Mandate.

c) You may amend, pause (and resume), cancel your Migrated DDR Mandates, or receive notice of amendment, pause or resumption, or cancellation initiated by the Merchant or Payment Initiator, in the manner described above.

**63A.6 Your responsibilities**

a) You must ensure that You carefully consider any Payment Agreement creation request or amendment request made in respect of your Payment Agreement or Migrated DDR Mandates and promptly respond to such requests. We will not be liable for any loss that You suffer because of any payment processed by Us in accordance with the terms of a Payment Agreement or Migrated DDR Mandate.

b) You must notify Us immediately if You no longer hold or have authority to operate the account (for example, by way of an ATO or POA) from which payments under a Payment Agreement or Migrated DDR Mandate have been/will be made.
c) You must promptly respond to any notification that You receive from Us regarding the pausing or cancellation of a Payment Agreement or Migrated DDR Mandate for misuse, fraud or for any other reason. We will not be responsible for any loss that You suffer as a result of You not promptly responding to such a notification.
d) You are responsible for ensuring that You comply with the terms of any agreement that You have with a Merchant or Payment Initiator, including any termination notice periods.
e) You acknowledge that You are responsible for any loss that You suffer in connection with the cancellation or pausing of a Payment Agreement or Migrated DDR Mandate by You which is in breach of any agreement that You have with the Merchant or Payment Initiator.
f) You are responsible for ensuring that You have sufficient funds in your Account to meet the requirements of your Payment Agreements and Migrated DDR Mandates. Where there are insufficient funds, the payment will be rejected.
g) 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 by calling 133 462 or +61 2 4298 0111 (if overseas).
h) From time to time, You may receive a notification from Us requiring You to confirm that all of your Payment Agreements and Migrated DDR 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 DDR Mandate/s.
i) Use of the facilities that We provide to You in connection with establishing and managing your Payment Agreements and Migrated DDR Mandates is required to meet the terms and conditions set out in this PDS. 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 Access Codes (such as a PIN or password) needed to access the facilities We provide are kept confidential and are not disclosed to any other person.
j) 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 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 consistent with the terms of this PDS.
k) Where an intellectual property infringement claim is made against You, We will have no liability to You under this PDS to the extent that any intellectual property infringement claim is based upon:
    i) modifications to Our Intellectual Property by or on behalf of You in a manner that causes the infringement; or
    ii) You fail to use Our Intellectual Property in accordance with this PDS.
l) You must comply with all applicable laws in connection with the use of PayTo.

### 63A.7 Our responsibilities

a) We will accurately reflect all information You provide to Us in connection with a Payment Agreement or a Migrated DDR Mandate in the Mandate Management Service.
b) We may monitor your Payment Agreements or Migrated DDR Mandates for misuse, fraud and security reasons. You acknowledge and consent to Us pausing or cancelling all or some of your Payment Agreements or Migrated DDR Mandates if We reasonably suspect misuse, fraud or security issues. We will notify You of any such action to pause or cancel your Payment Agreement.
c) 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 DDR Mandate or that was not authorised by You, please contact Us as soon as possible via 133 462 or +61 2 4298 0111 (if overseas).
d) We will not be liable for any payment made that was authorised by the terms of your Payment Agreement or Migrated DDR Mandate.

### 63A.8 Privacy

By confirming a Payment Agreement and/or permitting the creation of a Migrated DDR Mandate against your Account with Us, You acknowledge that You authorise Us to collect, use and store your personal information including your name, account details and other relevant information and the details of your Payment Agreement/s and Migrated DDR Mandate/s 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 enable Us to make payments from your account.