Gateway Bank

# Online Banking Terms and Conditions

Valid from 1 July 2024

# ONLINE BANKING TERMS AND CONDITIONS

Your first use of Online Banking is subject to the following Terms and Conditions that set out the use of Online Banking between yourself and Gateway Bank ("Gateway") and your use of Online Banking signifies that you have read, understood and accepted these Conditions of Use.

These Conditions of Use should be read in conjunction with the Gateway Deposit Accounts and Access Facilities General Conditions of Use which incorporates the General Fees, Charges and Transaction

Limits and the Summary of Deposit Accounts & Availability of Access Facilities available by accessing them at www.gatewaybank.com.au

Gateway warrants that it will comply with the Customer Owned Banking Code of Practice (COBCoP) and the ePayments Code and any liability for losses resulting from unauthorised transactions will be determined in accordance with the ePayments Code.

If you have any questions relating to these Terms and Conditions please call Gateway on 1300 302 474, Monday to Friday from 8am to 6pm AEST.

## EPAYMENTS CONDITIONS OF USE

These ePayments Conditions of Use govern all electronic transactions made using Online Banking.

## 1. IMPORTANT INFORMATION YOU NEED TO KNOW BEFORE USING ONLINE BANKING TO MAKE ELECTRONIC PAYMENTS

i. Familiarise yourself with your obligations to keep your pass code secure, see 'Pass code Security Requirements' below for more information;

ii. Familiarise yourself with the steps you have to take to report unauthorised use of your Online Banking and immediately report any unauthorised use or compromise of your pass code to Gateway;

iii. Use care to prevent anyone from seeing the pass code being entered on a device;

iv. Check your account transaction history regularly for any unauthorised use and report, as soon as possible, any instances of unauthorised use;

v. ALWAYS access Online Banking through Gateway's website;

vi. Do not leave electronic equipment unattended while connected to Online Banking;

vii. If accessing Online Banking on someone else's PC, laptop, tablet or mobile phone, ALWAYS DELETE your browsing history;

viii. ALWAYS REJECT any request (via email, SMS, phone etc) to provide or to confirm details of a pass code to anyone else. Gateway will NEVER ask you to provide us with these details;

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

x. You must be careful to ensure that you enter transaction details carefully as we do not check the BSB and account number against the recipient's account name. Once a payment or transfer has been made it will not be possible for us to stop or reverse the transaction, funds paid to the wrong account may not be recoverable;

xi. Immediately notify us when you change your address or other contact details; and

xii. An Australian mobile phone number is required for SMS, One Time Passwords (OTP) and full Online Banking access. You will be unable to transfer funds to another account holder, whether another Gateway Member or to an external account outside Gateway if an Australian mobile phone number is not provided.

## 2. DEFINITIONS

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

b. device means a device we give to a user that is used to perform a transaction. Examples include:
   (i) Personal Computer, laptop or tablet
   (ii) Mobile phone

c. facility means an arrangement through which you can perform transactions

d. identifier means information that a user:
   (i) knows but is not required to keep secret, and
   (ii) must provide to perform a transaction

e. Examples include an account number or Member number

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

g. pass code means a password or code that the user must keep secret, that may be required to authenticate a transaction or user. A pass code may consist of numbers, letters, a combination of both, or a phrase. Examples include:
   (i) personal identification number (PIN)
   (ii) Online Banking password
   (iii) Telephone Banking password
   (iv) One Time Password (OTP) required to authenticate a transaction

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

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

i. transaction means a transaction to which these ePayments Conditions of Use apply, as set out under Transactions below

j. unauthorised transaction means a transaction that is not authorised by a user

k. user means you or an individual you have authorised to perform transactions on your account, including:
   (i) a third party signatory to your account
   (ii) a person you authorise us to issue an additional card to

l. we, us, or our means Gateway Bank Ltd

m. you means the person or persons in whose name the account and access facility is held

## 3. TRANSACTIONS

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

(a) initiated using electronic equipment, and

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

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

(a) electronic card transactions, including ATM, EFTPOS and debit card transactions that are not intended to be authenticated by comparing a manual signature with a specimen signature

(b) Telephone Banking and bill payment transactions

(c) Online Banking transactions, including 'Pay Anyone'

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

(e) online bill payments (including BPAY)

(f) direct debits

(g) transactions using mobile devices.

## 4. WHEN YOU ARE NOT LIABLE FOR A LOSS

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

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

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

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

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

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

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

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

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

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

(b) we can prove that a user received a device or pass code by obtaining an acknowledgement of receipt from the user

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

## 5. WHEN YOU ARE LIABLE FOR A LOSS

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

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

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

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

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

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

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

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

5.3 Where:

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

(b) we prove that a user breached the pass code security requirements in Section 6 for one or more of the required pass codes, but not all of the required pass codes you are liable under clause 2 only if we also prove on the balance of probability that the breach of the pass code security requirements under Section 6 was more than 50% responsible for the losses, when assessed together with all the contributing causes.

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

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

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

(a) are liable for the actual losses that occur between:
  (i) when the user became aware of the security compromise, or should reasonably have become aware in the case of a lost or stolen device, and
  (ii) when the security compromise was reported to us
(b) are not liable for any portion of the losses:
  (iii) incurred on any one day that exceeds any applicable daily transaction limit
  (iv) incurred in any period that exceeds any applicable periodic transaction limit
  (v) that exceeds the balance on the facility, including any pre-arranged credit
  (vi) incurred on any facility that we and you had not agreed could be accessed using the device and/or pass code used to perform the transaction.

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

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

(a) $150, or a lower figure determined by us
(b) the balance of the facility or facilities which we and you have agreed can be accessed using the device and/or pass code, including any prearranged credit
(c) the actual loss at the time that the misuse, loss or theft of a device or breach of pass code security is reported to us, excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction or other periodic transaction limit.

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

(a) we must consider all reasonable evidence, including all reasonable explanations for the transaction occurring
(b) the fact that a facility has been accessed with the correct device and/or pass code, while significant, does not, of itself, constitute proof on the balance of probability that a user contributed to losses through fraud or a breach of the pass code security requirements in section 6.

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

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

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

## 6. PASS CODE SECURITY REQUIREMENTS

6.1 This section applies where one or more pass codes are needed to perform a transaction.

6.2 A user must not:

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

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

(i) carried with a device

(ii) liable to loss or theft simultaneously with a device

(c) unless the user makes a reasonable attempt to protect the security of the pass code

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

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

(a) hiding or disguising the pass code record among other records

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

(c) keeping a record of the pass code record in a securely locked container

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

This list is not exhaustive.

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

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

6.6 *Note 2: For the obligations applying to the selection of a pass code by a user, see clause 6.5.*

6.7 A user must not select a numeric pass code that represents their birth date, or an alphabetical pass code that is a recognisable part of their name, if we have:
(a) specifically instructed the user not to do so
(b) warned the user of the consequences of doing so.

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

6.9 Where we expressly authorise particular conduct by a user, either generally or subject to conditions, a user who engages in the conduct, complying with any conditions, does not breach the pass code security requirements in this section.

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

## 7. LIABILITY FOR LOSS CAUSED BY SYSTEM OR EQUIPMENT MALFUNCTION

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

7.2 Where a user should reasonably have been aware that a system or equipment provided by any party to a shared electronic network was unavailable or malfunctioning, our liability is limited to:
(a) correcting any errors
(b) refunding any fees or charges imposed on the user.

## 8. NETWORK ARRANGEMENTS

8.1 We must not avoid any obligation owed to you on the basis that:
(a) we are a party to a shared electronic payments network

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

8.2 We must not require you to

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

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

## 9. MISTAKEN INTERNET PAYMENTS

9.1 In this Section:

(a) direct entry means a direct debit or direct credit

(b) mistaken internet payment means a payment by a user through a 'Pay Anyone' Online Banking facility and processed by an ADI through direct entry where funds are paid into the account of an unintended recipient because the user enters or selects a Bank/State/Branch (BSB) number and/or identifier that does not belong to the named and/or intended recipient as a result of:

(i) the user's error, or

(ii) the user being advised of the wrong BSB number and/or identifier.

This does not include funds transferred to a recipient as a result of a scam.

(c) This does not include payments made using BPAY.

(d) receiving ADI means an ADI whose customer has received an internet payment

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

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

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

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

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

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

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

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

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

(a) are not satisfied that a mistaken internet payment has occurred

(b) have not complied with the processes and timeframes set out in clauses 9.2 - 9.5, or as described in the box below.

9.8 When we receive a complaint under clause 9.6 we must:
(a) deal with the complaint under our internal dispute resolution procedures
(b) not require you to complain to the receiving ADI.

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

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

## 10. USING ONLINE BANKING

10.1 We do not warrant that:
(a) the information available to you about your accounts through Online Banking is always up to date
(b) you will have 24 hours a day, 7 days per week, access to Online Banking
(c) data you transmit via Online Banking is totally secure

## 11. HOW TO REPORT UNAUTHORISED USE OF ONLINE BANKING

11.1 If you believe that your pass code for Online Banking transactions have been misused, lost or stolen, or, where relevant, your pass code has become known to someone else, you must contact us immediately.

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

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

## 12. CANCELLATION OF YOUR ACCESS TO ONLINE BANKING

12.1 You may cancel your access to Online Banking at any time by giving us notice.

12.2 We may immediately cancel or suspend your access to Online Banking at any time for security reasons or if you breach these Conditions of Use.

12.3 We may cancel your access to Online Banking for any reason by giving you 30 days notice. The notice does not have to specify the reasons for cancellation.

12.4 In the case of Online Banking, if, despite the cancellation of your access to Online

Banking, you carry out a transaction using the relevant access method, you will remain liable for that transaction.

12.5 Your access to Online Banking will be terminated when:

(a) we notify you that we have cancelled your access method to the account with us;
(b) you close the last of your accounts with us which has Online Banking;
(c) you cease to be our Member; or
(d) you alter the authorities governing the use of your account or accounts to which has Online Banking (unless we agree otherwise).

## 13. USING BPAY

13.1 You can use BPAY to pay bills bearing the BPAY logo from those accounts that have the BPAY facility.

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

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

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

## 14. PROCESSING BPAY PAYMENTS

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

(a) you become aware of any delays or mistakes in processing your BPAY payment;
(b) you did not authorise a BPAY payment that has been made from your account; or
(c) you think that you have been fraudulently induced to make a BPAY payment.
(d) *Please keep a record of the BPAY receipt numbers on the relevant bills.*

14.2 A BPAY payment instruction is irrevocable.

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

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

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

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

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

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

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

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

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

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

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

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

(a) advise you of this;

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

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

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

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

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

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

## 15. FUTURE DATED BPAY PAYMENTS

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

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

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

(b) If there are insufficient cleared funds or, as relevant, insufficient available credit, the BPAY payment will not be made and you may be charged a dishonour fee.

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

(d) You should contact us if there are any problems with your future-dated payment.

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

## 16. CONSEQUENTIAL DAMAGE FOR BPAY PAYMENTS

16.1 This clause does not apply to the extent that it is inconsistent with or contrary to any applicable law or code of practice to which we have subscribed. If those laws would make this clause illegal, void or unenforceable or impose an obligation or liability which is prohibited by those laws or that code, this clause is to be read as if it were varied to the extent necessary to comply with those laws or that code or, if necessary, omitted.

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

## 17. REGULAR PAYMENT ARRANGEMENTS

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

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

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

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

## 18. CUT OFF TIMES

18.1 All non-BPAY transactions through the Online Banking Service, will be effective:

(a) On the same day, if you asked us to make transfer/payment before our processing cut-off time on a business day (before 5.00pm Monday to Friday (AEST));

(b) On the next business day, if you asked us to make transfer/payment after our processing cut-off time or on a weekend, public holiday or non business day; or

(c) On the date requested if it is a future dated transaction.

18.2 All BPAY transactions through the Online Banking Service, will be effective:

(a) On the same day, if the BPAY transaction is authorised prior to our processing cut-off time on a business day (before 3 pm Monday to Friday (AEST)); and

(b) Any transactions conducted outside of the hours specified above will be processed on the next available business day within the times specified above.

(c) Final processing of the payment is up to the utility or organisation concerned and may not take place immediately. It may be a day or two before the transaction is processed and the bill is paid. Your account will be debited immediately, but the payment will not be made immediately.

(d) We advise you to check your transaction listing regularly through Online Banking to monitor the payment of your bills using this service, and to plan ahead so that the correct due dates are met using this service.

## 19. JOINT ACCOUNTS

19.1 If your account is a joint account each party to that account is jointly and severally liable for all transactions.

## 20. SECURITY

20.1 Gateway will take reasonable precautions to ensure that information concerning your accounts and transactions performed through Online Banking will remain confidential and protected from unauthorised access.

20.2 It is your sole obligation to maintain an electronic device with up to date security measures in place in order to access Online Banking. Refer to https://www.gatewaybank.com.au/about-us/member-commitment/online-security/ for more information.

20.3 If you travel outside of Australia you may still have access to Online Banking. Gateway does not advocate the use of a shared electronic device to access Online Banking as this may compromise your use of Online Banking.

## 21. WITHDRAWAL LIMITS

We limit the amount of daily withdrawals or payments you may make using electronic methods, either generally or in relation to a particular facility. These transaction limits are set out in the *Fees & Charges and Transaction Limits* brochure. Please note that merchants, billers or other financial institutions may impose additional restrictions on the amount of funds that you can withdraw, pay or transfer.

## 22. FEES AND CHARGES

22.1 Please refer to the General Fees, Charges and Transaction Limits brochure available on Gateway's website for current fees and charges. We may vary fees or charges from time to time.

22.2 No fees are payable to Gateway for using Online Banking. However, you may incur data charges from your network provider for using Online Banking. An Internet connection is required when using Online Banking and normal data charges apply. Gateway is not liable for any additional costs you incur.

## 23. CHANGES TO CONDITIONS OF USE

We reserve the right to change these Conditions of Use and to vary the fees and charges that apply to Online Banking.
We will notify you in writing at least 20 days before the effective date of a change if we:

(a) impose or increase any fee or charge;
(b) increase your liability for unauthorised use; or
(c) adjust daily withdrawal limits.

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

(a) notification by letter or email
(b) notification on or with your next statement of account
(c) notification on or with the next newsletter
(d) advertisements in the local or national media
(e) notification on our website.
(f) However, we will always select a method or methods appropriate to the nature and extent of the change, as well as the cost effectiveness of the method of notification.

## 24. ABOUT THE CUSTOMER OWNED BANKING CODE OF PRACTICE

Customer Owned banking delivers customer-focused, competitive services. The Customer Owned Banking Code of Practice, the code of practice for credit unions, customer owned banks and mutual building societies, is an important public expression of the value we place on improving the financial wellbeing of our individual Members and their communities.

Our 7 Key Promises to you are:

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

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

If you have a complaint about our compliance with the Customer Owned Banking Code of Practice you can contact us in the first instance. If you are unhappy with our response you can contact:

**Customer Owned Banking Code Compliance Committee**
Mail: PO Box 14240 Melbourne VIC 8001
Phone: 1800 931 678
Fax: 03 9613 7481
Email: info@codecompliance.org.au
Web: https://cobccc.org.au/

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

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

You can contact the **Australian Financial Complaints Authority (AFCA)**:
by calling 1800 931 678
by visiting www.afca.org.au
By post Australian Financial Complaints Authority
GPO BOX 3 Melbourne VIC 3001

# How to contact us


**Online**
www.gatewaybank.com.au

**Email**

memberservices@gatewaybank.com.au

**Call**

1300 302 474

**Registered Office**

Level 10, 68 York Street

SYDNEY NSW 2000

**Postal Address**

GPO Box 3176

SYDNEY NSW 2001



Gateway Bank Ltd
ABN 47 087 650 093
AFSL / Australian Credit Licence Number 238293
OLBTC181101