GATEWAY DEPOSIT ACCOUNTS & ACCESS FACILITIES

General Conditions of Use

Effective from 1 March 2018

Gateway Deposit Accounts and Access Facilities are issued by:
Gateway Bank Ltd
ABN 47 087 650 093
AFSL 238293

TABLE OF CONTENTS

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

If in Australia

- During business hours call Gateway Member Services on 1300 302 474 or
- After business hours call the Visa Hotline on 1800 139 241, 24 hours a day, everyday.

Please also contact us to report the loss, theft or unauthorised use.

If overseas

- Go to www.visa.com.au to find Visa's toll-free number for the country you are visiting; or
- Call Gateway Member Services on +61 2 9307 4200 or email us at Member Services www.gatewaybank.com.au

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

To report the loss of any other access facility, or any other unauthorised transaction, contact us as set out in How to Contact Us.

CUSTOMER OWNED BANKING CODE OF PRACTICE

We warrant that we will comply with the Mutual Banking Code of Practice. Please see the section ***'About the Mutual Banking Code of Practice'*** at the end of these Conditions of Use for more detail.

ePAYMENTS CODE

We warrant that we will comply with the ePayments Code.

PRIVACY

We have a Privacy Policy that sets out:

- Our obligations regarding the confidentiality of your personal information; and
- How we manage your personal information.

We will give you the *'Your Privacy'* brochure detailing Gateway's Privacy Policy whenever we request personal information from you. It is always available on request and you can download it from our website at www.gatewaybank.com.au

HOW OUR CONDITIONS OF USE BECOME BINDING ON YOU

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

ACCESSING COPIES OF THE CONDITIONS OF USE

Please keep these General Conditions of Use in a safe place so you can refer to it when needed. Alternatively, you can view and download our current Conditions of Use from our website at **www.gatewaybank.com.au**

FINANCIAL CLAIMS SCHEME

The Financial Claims Scheme established under the Banking Act protects you, as a depositor, by providing you timely access to your deposits, up to a defined amount, in the unlikely event that the bank becomes insolvent and is placed into liquidation. You may be entitled to payment under the Financial Claims Scheme. Payments under the scheme are subject to a limit for each depositor.

For further information about the Financial Claims Scheme:

- Visit the APRA website at www.apra.gov.au
- Phone the APRA hotline 1300 55 88 49.

Account Operations

What is included in the Gateway Deposit Accounts and Access Facilities?

The ***Gateway Deposit Accounts and Access Facilities General Conditions of Use*** gives you the terms and conditions you need to have to open transaction, savings and term deposit accounts and the following access facilities:

- Visa Debit Card
- BPAY® (registered to BPAY Pty Ltd ABN 69 079 137 518)
- Telephone Banking and Online Banking
- EFTPOS and ATM access
- Direct debit requests.

Please refer to the ***Summary of Deposit Accounts & Availability of Access Facilities*** brochure for available account types, the conditions applying to each account type and the access methods attaching to each account type.

How do I open an account?

You will need to become a Member of Gateway Bank before we can issue the Gateway Deposit Accounts and Access Facilities to you. To become a Member, you will need to:

- complete a Membership application form; and
- subscribe for a Member share in Gateway Bank.

Proof of identity required

The law requires us to verify your identity when you open an account or the identity of any person you appoint as a signatory to your account.

In most cases we can prove your identity through an electronic verification service using the identification documentation we request that you provide us.

If you want to appoint a signatory to your account, the signatory will also have to provide proof of identity.

What accounts can I open?

When we issue you with the Gateway Deposit Accounts and Access Facilities, you can open any transaction, savings or term deposit account and set up access facilities that are relevant to your needs. Please first check the ***Summary of Deposit Accounts & Availability of Access Facilities*** brochure for the different account types and access facilities available, any special

conditions for opening, and the features and benefits of each account type.

Joint accounts

A joint account is an account held by two or more persons. The important legal consequences of holding a joint account are:

- the right of survivorship – when one joint account holder dies, the surviving account holder(s) automatically take the deceased joint account holder's interest in the account (for business accounts different rules may apply - see Note below)
- joint and several liability – if the account is overdrawn, each joint account holder is individually liable for the full amount owing.

You can operate a joint account on an 'all to sign' or 'any to sign' basis:

- 'all to sign' means all joint holders must sign withdrawal forms, cheques, etc
- 'any to sign' means any one joint account holder can sign withdrawal slips, cheques, etc.

All joint account holders must consent to the joint account being operated on an 'any to sign' basis. However, any one joint account holder can cancel this arrangement, making it 'all to sign'.

If you do not nominate one method of operation on the account, it will be deemed 'all to sign' and will remain in force until we receive a written request from all account holders to change the method of operation.

If there is a dispute notified to us between joint account holders, we may change the method of operation to 'all must sign' until we receive a written request signed by all account holders to vary the method of operation to 'any to sign'.

Note: ***The right of survivorship does not automatically apply to joint business accounts, such as partnerships. A partner's interest in a business joint account would normally pass to beneficiaries nominated in the partner's will or next-of-kin if there is no will.***

If you are operating a business partnership joint account, you should obtain your own legal advice to ensure your wishes are carried out.

Trust accounts

You can open an account as a trust account. However:

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

You agree to indemnify us against any claim made upon us in relation to, or arising out of that trust.

What fees and charges are there?

Please refer to the ***Fees & Charges and Transaction Limits*** brochure for current fees and charges.

We may vary fees or charges from time to time.
We will debit your account for all applicable government taxes and charges.

What interest can I earn on my Account?

Our Interest Rate Schedule provides information about our current savings and investments interest rates. Our website also has information about our current savings and investments interest rates. We may vary our savings and investments interest rates from time to time on all savings accounts except our term deposit accounts.

Our ***Summary of Deposit Accounts & Availability of Access Facilities*** brochure discloses how we calculate and credit interest to your account.

What are the taxation consequences?

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

Disclosing your Tax File Number (TFN)

When you apply for the Gateway Deposit Accounts and Access Facilities we will ask you whether you want to disclose your Tax File Number (TFN) or exemption. If you disclose it, we will note your TFN against any account you activate.

You do not have to disclose your TFN to us. If you do not, we will deduct withholding tax from interest paid on the account at the highest marginal rate.

For a joint account, each account holder must quote their TFN and/or exemptions, otherwise withholding tax applies to all interest earned on the joint account.

Businesses need only quote their ABN instead of a TFN.

Third party access

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

You can specify which of your accounts under the Gateway Deposit Accounts and Access Facilities you give the authorised person authority to operate on. You are responsible for all transactions your authorised person carries out on your account. **You should ensure that the person you authorise to operate on your account is a person you trust fully.**

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

Making deposits to the account

You can make deposits to the account:

- by cash or cheque at our head office/branch

- by direct credit e.g. from your employer for wages or salary – please note that we can reverse a direct credit if we do not receive full value for the direct credit
- by transfer from another account with us
- by transfer from another financial institution
- by cash or cheque at a Commonwealth Bank of Australia branch using a specially encoded deposit book
- by cash or cheque at selected ATMs, if your account is linked to a Visa Debit Card
- via Australia Post Bank@Post™, (trademark of Australia Post ABN 28 864 970 579)

unless otherwise indicated in the ***Summary of Deposit Accounts & Availability of Access Facilities*** brochure.

Deposits using electronic equipment

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

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

You may not receive value for your electronic deposit on the same day.

Depositing cheques drawn on Australian banks

You can only access the proceeds of a cheque when it has cleared. This usually takes 3 business days (or if the cheque deposit is via Bank@Post - 5 business days).

Withdrawing or transferring from the account

You can make withdrawals from the account:

- over the counter at our head office/branch (by corporate cheque only)
- by direct debit
- via Telephone Banking or Online Banking
- via BPAY® to make a payment to a biller
- via a wide range of ATMs, if your account is linked to a Visa Debit Card
- via selected EFTPOS terminals, if your account is linked to a Visa Debit Card (note that merchants may impose restrictions on withdrawing cash)
- via Australia Post Bank@Post.

unless otherwise indicated in the ***Summary of Deposit Accounts & Availability of Access Facilities*** brochure.

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

Debiting transactions generally

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

We have the right to decline your authorisation for any transaction if we are uncertain for any reason of the authenticity or validity of the authorisation or your legal capacity to give the authorisation. We will not be liable to you or any other person for any loss or damage which you or such other person may suffer as a result of our action.

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

Over the counter corporate cheque withdrawals

Gateway does not permit over the counter cash withdrawals. We will only permit over the counter withdrawals via Bank corporate cheque.

Withdrawals using our corporate cheques

This is a cheque Gateway draws payable to the person you nominate. You can purchase a corporate cheque from us for a fee: see the ***Fees & Charges and Transaction Limits*** brochure.

If a corporate cheque is lost or stolen, you can ask us to stop payment on it. You will need to complete a form of request, giving us evidence of the loss or theft of the cheque. You will also have to give us an indemnity – the indemnity protects us if someone else claims that you wrongfully authorised us to stop the cheque.

We cannot stop payment on our corporate cheque if you used the cheque to buy goods or services and you are not happy with them. You must seek compensation or a refund directly from the provider of the goods or services. You should contact a Government Consumer Agency if you need help.

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.

Overdrawing an account

You must keep sufficient cleared funds in your account to cover your cheque, direct debit and electronic transactions. If you do not, we can dishonour the transaction and charge dishonour fees: see the ***Fees & Charges and Transaction Limits*** brochure. Alternatively, we can honour the

transaction and overdraw your account. We may charge you a fee for each day (or part of a day) your account is overdrawn: see the ***Fees & Charges and Transaction Limits*** brochure.

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

Account statements

We will send you account statements at least every 3 months. More frequent or duplicate statements can be requested at any time. We may charge a fee for providing additional statements or copies: see the ***Fees & Charges and Transaction Limits*** brochure.

We recommend that you check your account statement as soon as you receive it. Immediately notify us of any unauthorised transactions or errors. Please refer to ***How to Contact Us*** on the back page for our contact details.

e-Statements

If you agree, we can provide your statements electronically. By registering for e-Statements, you authorise Gateway to provide your statements of account electronically in a PDF format via Gateway's Online Banking facility. Registration to receive e-Statements takes effect at Membership level so statements for all accounts under your Membership number will be available electronically. You have the option at any time to revert to receiving paper statements by calling Member Services on 1300 302 474.

You will be notified of the availability of statements by email to the nominated email address provided at the time of registration for this service. You should check your email regularly for notices that e-Statements are available. For more information on e-Statements refer to our website.

What happens if I change my name or address?

We recommend that if you change your name or address, you let us know immediately.

Dormant accounts

If no transactions are carried out on your accounts within your Membership for at least 24 months (other than transactions initiated by Gateway, such as crediting interest or debiting fees and charges) we may write to you asking if you want to keep your Membership open. If you do not reply we will treat your Membership as dormant.

Once your Membership becomes dormant, we may:

- charge a dormancy fee
- stop paying interest.

Under unclaimed monies legislation, we have a legal obligation to remit balances $500 and over to the Australian Securities and Investment Commission as unclaimed money.

Account combination

If you have more than one account with us, we may apply a deposit balance in any account to any other savings account in the same name which is overdrawn.

On termination of your Membership, we may combine all your accounts (whether savings or loan accounts) you have with us provided the accounts are all in the same name.

We will not combine accounts if to do so would breach the Code of Operation for Centrelink Direct Credit Payments.

We will give you written notice promptly after exercising any right to combine your accounts.

Closing accounts and cancelling access facilities

You can close the Gateway Deposit Accounts and Access Facilities at any time. However, you will have to surrender any Visa Debit Card at the time. We may defer closure and withhold sufficient funds to cover payment of outstanding electronic transactions and fees, if applicable.

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

- close the Gateway Deposit Accounts and Access Facilities in our absolute discretion by giving you at least 14 days notice and paying you the balance of your account; or
- cancel any access facility for security reasons or if you breach these General Conditions of Use.

Notifying changes

We may change fees, charges, interest rates and other conditions at any time. The following table sets out how we will notify you of any change.

Type of change	Notice
Increasing any fee or charge	20 days
Adding a new fee or charge	20 days
Changing the method by which interest is calculated	20 days
Changing the circumstances when interest is credited to your	20 days
Changing deposit interest rates	on the day of change
Increasing your liability for losses relating to ePayments (see the ePayments	20 days
Imposing, removing or changing any periodic transaction limit	20 days
Changing any other term or condition	when we next communicate with you

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

- notification by letter
- notification on or with your next statement of account
- notification on or with the next newsletter
- advertisements in the local or national media

- notification on our website.

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.

How we send notices and statements

We may send you notices and statements:

- by post, to your nominated mailing address
- by fax
- by email
- by advertisement in the media, for some notices only.

Complaints

We have an internal dispute resolution procedure to deal with any complaints you may have and if we cannot resolve your complaint we offer an external dispute resolution service.
If you want to make a complaint:

- Contact Gateway's Member Services on **1300 302 474**, or
- Email us at memberservices@gatewaybank.com.au or
- Complete the Member Comment Form available on our website or in branch and mail it together with any supporting documents to:

  The Complaints Officer
  Gateway Bank
  GPO Box 3176
  SYDNEY NSW 2001

Please refer to our ***Dispute Resolution Scheme*** brochure for details available at **www.gatewaybank.com.au** or by calling us.

Direct debit

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

To cancel the DDR Service Agreement, you can contact either the biller or us. If you contact us we will promptly stop the facility. We suggest that you also contact the biller.

If you believe a direct debit initiated by a biller is wrong you should contact the biller to resolve the issue. Alternatively, you may contact us. If you give us the information we require we will forward your claim to the biller. However, we are not liable to compensate you for your biller's error.

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

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

PayPal

When you use PayPal you are authorising PayPal to debit amounts from your account as a biller under direct debit. Please note that:

- you are responsible for all PayPal debits to your account
- if you dispute a PayPal debit, you can contact PayPal directly or ask us to do so
- we are not responsible for compensating you for any disputed PayPal debit, or for reversing any disputed PayPal debit to your account
- if you want to cancel your direct debit arrangement with PayPal, you can contact PayPal directly or ask us to do so
- when you ask us to pass on a disputed transaction to PayPal, or your request to cancel your direct debit arrangement with PayPal, we will do so as soon as practicable but we are not responsible if PayPal fails to respond as soon as possible or at all.

Other third party payment services may operate in a similar way to PayPal.

Electronic access facilities and ePayments conditions of use

Section 1: Information about our ePayment facilities

You should follow the guidelines in the box below to protect against unauthorised use of your Visa Debit Card and pass code. These guidelines provide examples of security measures only and will not determine your liability for any losses resulting from unauthorised ePayments. Liability for such transactions will be determined in accordance with the ePayments Conditions of Use and the ePayments Code.

Important Information You Need to Know Before Using a Device to Make Electronic Payments

- Sign the Visa Debit Card as soon as you receive it.
- Familiarise yourself with your obligations to keep your Visa Debit Card and pass codes secure.
- Familiarise yourself with the steps you have to take to report loss or theft of your Visa Debit Card or to report unauthorised use of your Visa Debit Card, BPAY, Telephone Banking or Online Banking.
- If you change a pass code, do not select a pass code which represents your birth date or a recognisable part of your name.
- Never write the PIN on the Visa Debit Card.
- Never write the pass code PIN on anything which is kept with or near the Visa Debit Card.
- Never lend the Visa Debit Card to anybody.
- Never tell or show the Visa Debit Card PIN or the Online Banking pass code to another person.
- Use care to prevent anyone seeing the pass code being entered on a device.
- Keep a record of the VISA Debit Card number and the VISA Card Hotline telephone number for your area with your usual list of emergency telephone numbers.
- Check your statements regularly for any unauthorised use.
- Immediately notify us when you change your address.
- ALWAYS access Telephone Banking or Online Banking service only using the OFFICIAL phone numbers and URL addresses.
- If accessing Online Banking on someone else's PC, laptop, tablet or mobile phone, ALWAYS DELETE your browsing history.
- ALWAYS REJECT any request to provide or to confirm details of your pass code. We will NEVER ask you to provide us with these details.

If you fail to ensure the security of your Visa Debit Card, access facility and pass codes you may increase your liability for unauthorised transaction.

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

- Visa Debit Card
- BPAY
- Online Banking
- Telephone Banking

You can use any of these electronic access facilities to access an account, as listed in the ***Summary of Deposit Accounts & Availability of Access Facilities.***

Visa Debit Card

Visa Debit Cards allow you to make payments at any retailer displaying the Visa logo, anywhere in the world. You can also withdraw cash from your account, anywhere in the world, using an ATM displaying the ***Visa logo***. We will provide you with a PIN to use with your Visa Debit Card. Visa Debit Cards also allow you to:

- check your account balances
- withdraw cash from your account
- transfer money between accounts
- deposit cash or cheques into your account at selected ATMs and at Bank@Post.

We may choose not to give you a Visa Debit Card if your banking history with Gateway is not satisfactory or if you are under 18 years of age.

Important Information about Chargebacks for VISA Debit Card

If you believe a Visa Debit Card transaction was:

- unauthorised;
- for goods or services and the merchant did not deliver them; or
- for goods and services which did not match the description provided by the merchant,

then you can ask us to 'chargeback' the transaction, by reversing the payment to the merchant's financial institution. However, we can only do a chargeback if you inform us of the disputed transaction within the timeframe determined by Visa. Currently the shortest cut-off time for notifying of chargeback circumstances is 45 days after the transaction, although longer periods may apply in particular circumstances.

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

You should inform us as soon as possible if you become aware of circumstances which might entitle you to a chargeback and let us have the cardholder's copy of the Visa transaction receipt in question.

Section 2: Definitions

(a) **ATM** means automatic teller machine

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

(c) **device** means a device we give to a user that is used to perform a transaction. Examples include:

  (i) ATM card

  (ii) debit card

(d) **EFTPOS** means electronic funds transfer at the point of sale — a network for facilitating transactions at point of sale

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

(f) **identifier** means information that a user:

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

  (ii) must provide to perform a transaction

  Examples include an account number or Member number

(g) **manual signature** means a handwritten signature, including a signature written on paper and a signature written on an electronic tablet

(h) **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

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

(i) **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

(j) **transaction** means a transaction to which these ePayments Conditions of Use apply, as set out in Section 3

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

(l) **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

(m) **we**, **us**, or **our** means Gateway Bank Ltd

(n) **you** means the person or persons in whose name this Account and Access Facility is held

Section 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.

Section 4:
When you are not liable for loss

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

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

(b) a device, identifier or 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.

Section 5: When you are liable for loss

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

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

(a) you are liable in full for the actual losses that occur before the loss, theft or misuse of a device or breach of 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 5.2 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:
    (i) incurred on any one day that exceeds any applicable daily transaction limit
    (ii) incurred in any period that exceeds any applicable periodic transaction limit
    (iii) that exceeds the balance on the facility, including any pre-arranged credit
    (iv) incurred on any facility that we and you had not agreed could be accessed using the device and/or 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). This clause does not require us to exercise any rights we may have under the rules of the card scheme. However, we cannot hold you liable under this clause for a greater

amount than would apply if we had exercised those rights.

Section 6: Pass code security requirements

6.1. Section 6 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

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

(c) 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.

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

6.5. 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.

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

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

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

Section 7: Liability for loss caused by system or equipment malfunction

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

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

(a) correcting any errors

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

Section 8: Network arrangements

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

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

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

8.2. We must not require you to:

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

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

Section 9: Mistaken internet payments

9.1. In this Section 9:

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

(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 payments made using BPAY.

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

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

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

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

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

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

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

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

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

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

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

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

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

(a) deal with the complaint under our internal dispute resolution procedures

(b) not require you to complain to the receiving ADI.

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

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

Information About a Receiving ADI's Obligations After We Request Return of Funds

The information set out in this box is to explain the process for retrieving mistaken payments under the ePayments Code, setting out what the processes are, and what you are entitled to do.

This information does not give you any contractual entitlement to recover the mistaken payment from us or to recover the mistaken payment from the receiving ADI.

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

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

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

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

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

- If the receiving ADI is satisfied that a mistaken internet payment has occurred, it must

seek the consent of the unintended recipient to return the funds to the user.

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

Process where funds are not available

- Where the sending ADI and the receiving ADI are satisfied that a mistaken internet payment has occurred, but there are not sufficient credit funds available in the account of the unintended recipient to the full value of the mistaken internet payment, the receiving ADI must use reasonable endeavours to retrieve the funds from the unintended recipient for return to the holder (for example, by facilitating repayment of the funds by the unintended recipient by instalments).

Section 10: Using Telephone Banking and Online Banking

10.1. We do not warrant that:

(a) the information available to you about your accounts through Telephone Banking and Online Banking is always up to date

(b) you will have 24 hours a day, 7 days per week, access to Telephone Banking or Online Banking

(c) data you transmit via Telephone Banking or Online Banking is totally secure.

Section 11: How to report loss, theft or unauthorised use of your Visa Debit card or pass code

11.1. If you believe your Visa Debit Card has been misused, lost or stolen or the pass code has become known to someone else, you must immediately contact us during business hours or the Visa Card HOTLINE at any time.

Please refer to How to Contact Us on the back page for our contact details.

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

11.3. The Visa Card HOTLINE is available 24 hours a day, 7 days a week.

11.4. If the Visa Card HOTLINE is not operating when you attempt notification, nevertheless, you must report the loss, theft or unauthorised use to us as soon as possible during business hours. We will be liable for any losses arising because the Visa Card

HOTLINE is not operating at the time of attempted notification, provided you report the loss, theft or unauthorised use to us as soon as possible during business hours.

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

(a) with us by calling Gateway Member Services on 1300 302 474 or priority paid mail as soon as possible; or

(b) by calling the VISA Card Hotline number for the country you are in.

VISA CARD HOTLINE

AUSTRALIA WIDE TOLL FREE

1800 224 004

SYDNEY METROPOLITAN AREA

(02) 9959 7480

Section 12: How to report unauthorised use of Telephone Banking or Online Banking

12.1. If you believe that your pass codes for Telephone Banking or 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.

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.

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

Section 13: Using the Visa Debit Card

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

13.2. We will advise you from time to time:

(a) what transactions may be performed using a Visa Debit Card
(b) what ATMs of other financial institutions may be used; and
(c) what the daily cash withdrawal limits are.

Please refer to the ***Fees & Charges and Transaction Limits*** brochure for details of current transaction limits.

13.3. You may only use your Visa Debit Card to perform transactions on those accounts we permit. We will advise you of the accounts which you may use your Visa Debit Card to access.

13.4. The Visa Debit Card always remains our property.

Section 14: Using Visa outside Australia

14.1. Visa Worldwide converts your overseas transactions to Australian currency at their applicable wholesale rate.

14.2. Gateway receives a commission on all foreign currency transactions using your Visa Debit Card. Please refer to the ***Fees & Charges and Transaction Limits*** brochure for the current commission.

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

Section 15: Additional Visa Debit Card

15.1. You may authorise us, if we agree, to issue an additional Visa Debit Card to an additional cardholder

15.2. You will be liable for all transactions carried out by this cardholder.

15.3. We will give each additional cardholder a separate pass code.

15.4. You must ensure that any additional cardholders protect their Visa Debit Card and pass code in the same way as these ePayments Conditions of Use require you to protect the Visa Debit Card and pass code.

15.5. To cancel the additional Visa Debit Card you must notify us. However, this cancellation may not be effective until the additional Visa Debit Card is returned to us or you have taken all reasonable steps to have the additional Visa Debit Card returned to us.

15.6. You will not be liable for the continued use of the additional Visa Debit Card from the date that you have:
(a) notified us that you want it cancelled; and
(b) taken all reasonable steps to have the additional Visa Debit Card returned to us.

Please note that if you are unable to return the additional Visa Debit Card to us, we may require you to make a written statement describing the steps you have taken to return the card.

Section 16: Use after cancellation or expiry of Visa Debit Card

16.1. You must not use your Visa Debit Card:
(a) before the valid date or after the expiration date shown on the face of Visa Debit Card; or
(b) after the Visa Debit Card has been cancelled.

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

Section 17: Exclusions of Visa Debit Card warranties and representations

17.1. We do not warrant that merchants or ATMs displaying Visa card signs or promotional material will accept Visa Debit Cards.

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

Section 18: Cancellation of Visa Debit Card or of access to Online Banking and Telephone Banking

18.1. You may cancel your Visa Debit Card, your access to Telephone Banking or Online Banking at any time by giving us notice.

18.2. We may immediately cancel or suspend your Visa Debit Card or your access to Telephone Banking or Online Banking at any time for security reasons or if you breach these
Conditions of Use. In the case of Visa Debit Card, we may cancel the Visa Debit Card by capture of the Visa Debit Card at any ATM.

18.3. We may cancel your Visa Debit Card or your access to Telephone Banking or Online Banking
for any reason by giving you 30 days notice. The notice does not have to specify the reasons for cancellation.

18.4. In the case of your Visa Debit Card, you will be liable for any transactions you make using your Visa Debit Card before the Visa Debit Card is cancelled but which are not posted to your account until after cancellation of your Visa Debit Card.

18.5. In the case of Telephone Banking, Online Banking, if, despite the cancellation of your access to
Telephone Banking or Online Banking, you carry out a transaction using the relevant access method, you will remain liable for that transaction.

18.6. Your Visa Debit Card or your access to Telephone Banking or Online Banking will be terminated when:

(a) we notify you that we have cancelled your Visa Debit Card or your access method to the account with us;
(b) you close the last of your accounts with us to which the Visa Debit Card applies or which has Telephone Banking or 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 the Visa Debit Card applies or which has Telephone Banking or Online Banking (unless we agree otherwise).

18.7. In the case of a Visa Debit Card, we may demand the return or destruction of any cancelled Visa Debit Card.

Section 19: Using BPAY

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

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

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

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

Section 20:
Processing BPAY payments

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

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

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

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

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

20.2. A BPAY payment instruction is irrevocable.

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

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

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

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.

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

(a) on the date you direct us to make it, if we receive your direction by the cut off time on a banking business day, 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.

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

(a) there is a public or bank holiday on the day after you 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.

20.8. 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.

20.9. 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.

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

Section 21: Future-dated BPAY payments

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

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

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

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

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

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

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

Section 22: Consequential damage for BPAY payments

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

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

Section 23:
Regular payment arrangements

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

23.2. 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.

23.3. 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.

23.4. 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.

About the Customer Owned Code of Practice

Mutual banking delivers Member-focused, competitive services. Mutual banks and mutual building societies are customer-owned financial institutions committed to putting their Members first.

The Customer Owned Banking Code of Practice, the code of practice for mutual 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 10 Key Promises to you are:

1. We will be fair and ethical in our dealings with you
2. We will focus on our Members
3. We will give you clear information about our products and services
4. We will be responsible lenders
5. We will deliver high customer service and standards
6. We will deal fairly with any complaints
7. We will recognise Member rights as owners
8. We will comply with our legal and industry obligations
9. We will recognise our impact on the wider community

10. We will support and promote this Code of Practice.

You can download a copy of the **Customer Owned Banking Code of Practice** here www.gatewaybank.com.au/about/Member-commitment
If you have a complaint about our compliance with the Mutual Banking Code of Practice you can contact:

Code Compliance Committee Mutuals
Mail: PO Box 14240
Melbourne VIC 8001
Phone: 1300 78 08 08
Fax: 03 9613 7481
Email: info@codecompliance.org.au
Web: www.cccmutuals.org.au/resolving-complaints/how-the-ccc-can-help/

The Code Compliance Committee Mutuals (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 Credit Ombudsman Service Limited, 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 Credit Ombudsman Service Limited:

by calling **1800 138 422**
by visiting **http://www.cosl.com.au**

How to contact us

Web
www.gatewaybank.com.au

Email
memberservices@gatewaybank.com.au

Call
1300 302 474

Fax
02 9307 4299

Registered Office
Level 16, 2 Market Street
SYDNEY NSW 2000

Postal Address
GPO Box 3176
SYDNEY NSW 2001

Gateway Bank Ltd
ABN 47 087 650 093
AFSL 238293
Australian Credit Licence Number 238293
GCUDAAFTC1302

bank gateway