Merchant Agreement
How to use your merchant facility

Dated 1 April 2020

Terms and conditions

These products are issued by the Commonwealth Bank of Australia
ABN 48 123 123 124 AFSL 234945

CommonwealthBank

Contents

Welcome

Who should read this booklet?

This booklet contains the terms and conditions which apply to your Facility and forms part of your contract with us and applies to all facilities, including terminal-based facilities and online solutions.

Having a clear picture of how to use your Facility, and the terms and conditions that apply, can help both you and us avoid misunderstandings.

It's important that you read this booklet so that you understand:

- what you need to do to use your Facility properly; and
- your obligations to us and our obligations to you.

We recommend you keep this booklet in a safe place for future reference. If you do lose it, you can call us and we will give you another copy or you can download a copy from our website.

How to use the booklet:

Part 1 - Where to get help

Numbers to call and websites to visit to get more information.

Part 2 - How to use your Facility

Explains how you must operate your Facility, e.g. getting started, accepting Payments, handling refunds, minimising disputes and chargebacks.

Part 3 - Terms and conditions

Sets out certain obligations that define the legal relationship between you and us. This includes what each of us is responsible for.

Part 4 - Optional products and features

Explains the rules that govern certain third party applications and optional products and services available through your Facility. Some of these optional products may be provided by or through the assistance of third party providers who may have separate terms and conditions which apply to the optional product.

Part 5 - Meaning of words

This part lists some key terms used in this document and what they mean. To assist you in understanding which terms are defined, we have capitalised them throughout this booklet.

Part 1: Where to get help

Here are the contact details to use:

Help or advice on operating your Facility	
Online	**commbank.com.au/merchantsupport**
General enquiries	Freecall **1800 230 177** 24 hours, 7 days
Stationery ordering	**commbank.com.au/eftposstationery**
Suspected Card fraud	Freecall **1800 023 919** and press 1 24 hours, 7 days
Obtaining authorisation	
eftpos	Freecall **1800 813 700** 24 hours, 7 days
Visa and Mastercard	Call **13 26 36** 24 hours, 7 days
AMEX/JCB	Call **1300 363 614** 24 hours, 7 days
Diners Club	Call **1300 360 500** 24 hours, 7 days

If you have a complaint, contact us in the first instance, we will make a record and give you the name of a contact person who is handling your complaint and a way to contact them. Within 21 days, we will provide a response to the complaint or advise you of the need for more time to complete our investigation. If we are unable to provide a final response to your complaint within 45 days, we will:

- inform you of the reasons for the delay and when we reasonably expect a decision;
- thereafter give you monthly progress updates;
- advise of your right to complain to the Australian Financial Complaints Authority (AFCA); and
- provide you with AFCA contact details.

Part 2: How to use your Facility

2.1 About this part

In this part we explain how to:

- operate your Facility; and
- manage risks relating to customer disputes and chargebacks.

For other useful information about your Facility, please refer to our Merchant services website at: **commbank.com.au/merchantservices**.

2.2 Getting started – eCommerce Facilities

2.2.1 Activating your eCommerce merchant facility

To access and use your eCommerce Facility, you will be allocated a user name and after first logging in using a password we send you, you must choose a password (which meets our security requirements).

You must use your user name and your password each time you wish to access and use this service.

To make, change or delete a Payment to us, you must input your user name and password.

You must ensure that your password is kept secure at all times and is not disclosed to any other person. If another person knows your user name and password they can access your information and conduct Transactions as if they are you. You must tell us promptly if you are aware or suspect that your password is known to another person and must also promptly change your password.

Access to your information and Transactions made by inputting your user name and password are deemed to be authorised by you unless they occur after you have told us that you are aware or suspect that your password is known to another person.

- You are responsible for ensuring the security of your computer and internet access when accessing the service, including using up to date anti-virus and internet security software.
- If you utilise a Single Sign On (SSO) service you must implement controls to ensure only intended users have access to your Facility and that the passwords of these users comply with the security obligations in this booklet.
- All information on the service is believed to be accurate and has been provided in good faith to the Bank, but the Bank makes no representation or warranty as to the accuracy or completeness of the information available through this service.

2.2.2 Your website obligations

Any business accepting Payments via a website must comply with the Website Requirements Policy on our website.

In addition to complying with the Website Requirements Policy, you must ensure that all content you place on your website, and our hosted page services is materially accurate and not misleading or deceptive, does not violate or infringe on the rights of any third party, is not libellous, threatening or obscene and complies with all applicable Australian and international laws and regulations.

You indemnify us and our suppliers, and shall keep us and our suppliers indemnified, against any claim by a third party that any uploaded material breaches a third party's intellectual property.

2.2.3 If you are a Direct Debit User

If we agree to you receiving Payments through the bulk electronic clearing system administered by the Australian Payments Network you agree to be bound by our Receivables Terms and Conditions which can be found here: **commbank.com.au/receivablesterms**.

2.2.4 Your customer terms and conditions

You must publish terms and conditions that have been approved by us, for your customers, if you are processing debits from their bank accounts. Any change to the terms and conditions must be approved by us and must be notified to your customers 14 days in advance.

2.3 Getting started - Terminals

Here are the steps you need to follow to get started:

2.3.1 Step 1 - Planning ahead

You should identify a safe location for the installation of terminals and any other equipment which is unobstructed, free of clutter and any other hazards. For your safety, terminals should be treated with the same care as any other electronic equipment.

You should think about which staff you will allow to use your Facility, and ways to restrict their access. You should also explain this booklet to your staff and how it affects them.

2.3.2 Step 2 - Establishment of Facility and installation of terminals and equipment

Our installers will contact you to arrange access to your premises. On the appointed day, they will install the terminal and any other equipment that we've agreed to provide you.

If you use your own equipment or software, then it must comply with our security and other requirements.

2.3.3 Step 3 - Setting your password

Our terminals come with a password which must be used when conducting certain Transactions, e.g. when processing refunds.

You must change the default password when you first use the terminal. You should also change your password on a regular basis and limit access to trusted staff.

2.3.4 Step 4 - Stationery

To ensure your terminal works properly, you must use our stationery. We give you an initial supply of stationery to get you started.

2.3.5 Step 5 - Initial training

During terminal installation, our installers will provide start-up training on how to operate the equipment.

You should then in turn train any other staff who will use the Facility.

2.4 Looking after our terminals and other equipment

2.4.1 Safety and maintenance

It is important you care for any terminal or other equipment we provide you and to keep them in good condition and unobstructed.

Liquids and dust may damage terminal components and like other electronic devices may create a safety hazard or otherwise prevent optimal performance. It's important you regularly clean and inspect our terminals for potential hazards.

Do not allow the power cables to become frayed, snagged or entangled. If these are damaged or distressed, or if you are concerned for any other reason, then you should contact us immediately.

Tell us immediately if our terminal is either not working or defective and we'll repair or replace it as soon as we can. Please use the downtime procedures until it is fixed or replaced.

Do not tamper with, remove terminal housing or attempt to repair any terminals or other equipment yourself. Please call us if you have equipment that requires replacement or repair. If you are in any doubt, please ensure you call us.

For further tips on maintaining our equipment, please refer to our FAQs on our website.

Note: Any terminals or other equipment we provide you remain our property and you must look after them. We are not liable, and you will be responsible for all costs, loss, liability, expense, and damages if any terminal or accessory:

- is altered, installed not in accordance with our instructions, repaired or maintained by parties not authorised by us;
- is opened, or the seals contained thereon are broken, tampered with or missing, or we otherwise reasonably believe that the terminal has been opened;
- is connected to any peripheral with cables or accessories not certified by us;
- is operated outside of the product specifications;
- suffers from abuse, negligence, accident, liquid spillage, pest infestation, floods or lightning damage;
- has a serial number that has been removed, tampered with or altered;
- is operated with operating supplies, including paper, accessories, chargeable batteries not certified by us; and/or
- has defects resulted from software not provided by our approved providers.

2.4.2 Terminal security

Keeping your terminal secure is important.

If your terminal is tampered with, this could lead to events such as Card or PIN details being copied or stolen by fraudsters.

If this happens you will be liable for any losses you or we suffer due to the fraudster's subsequent actions.

To protect your terminal:

- keep the terminal in a secure location;
- never leave your terminal unattended (or put it away if you need to leave the area);
- check the terminal regularly for any skimming devices and check the surrounding areas for any cameras;
- don't disclose your terminal password to anyone, or only tell staff you trust to process refunds. They must keep the password secret;
- there may be times when our installer needs to work on the terminal, e.g. to inspect or replace it. Make sure they have an appointment and provide ID, and if you're suspicious or have any questions call us on **1800 230 177**; and
- call us immediately on **1800 230 177** if the terminal, card imprinter, or stationery or any other equipment associated with your Facility is stolen or tampered with.

2.4.3 Software

Some facilities require separate operating software to be installed. If this applies you must only use software that we provide or agree that you can use. All software may only be used in accordance with the licence conditions.

2.4.4 Using equipment and software not provided by us

If you use your own equipment or software, you must ensure it complies with our security and other requirements. You may be required to make upgrades when our standards change.

2.5 Ordering additional stationery

To order stationery, visit **commbank.com.au/eftposstationery**. If you don't have access to the internet, call us on **1800 230 177**. At the time you place your order we will tell you the costs, including postage. Please allow five Banking Days for delivery.

2.6 Transactions above floor limit

You must obtain our authorisation before accepting a Transaction above your floor limit. If you are unsure of your floor limit, please contact us.

2.6.1 What is an authorisation?

An authorisation is when we confirm through the Cardholder's bank that:

- the Card number exists and the expiry date is valid;
- the Card number has not been reported lost or stolen as at that time; and
- enough funds are available to allow the Transaction to proceed.

If you process a Transaction electronically, we automatically obtain the authorisation for you. If the merchant services system is down, you will need to obtain authorisation by calling us to process an offline transaction. Please note offline authorisation is not available on UnionPay International.

2.6.2 Floor limits

A 'floor limit' is the highest Transaction amount you can process during system downtime without contacting us to obtain authorisation.

Please note:

- you have two floor limits - one for credit card Transactions and another for debit card Transactions;
- some cards have a pre-set offline Transaction limit which may prevent Transactions being processed up to your floor limit;
- for all Transactions where the Cardholder is not present the floor limit is $0 (i.e. all these Transactions must be authorised);
- you must never disclose your floor limit to Cardholders;
- your floor limit is provided in the welcome letter we send you when your Facility is approved. If you are unaware of your floor limit, please contact our Merchant support team for assistance.

2.7 If the system is down

If the merchant services system is down, depending on whether you have Store and Forward, you may not be able to obtain electronic authorisation and will need to call us.

2.7.1 If you have Store and Forward

Most terminals come with a Store and Forward function. If you're not sure whether you have this, call us on **1800 230 177**. Store and Forward allows you to continue to process Transactions under your floor limit in the usual way even when the terminal cannot connect to the Bank. The terminal prints a receipt which the Cardholder must sign.

Note: The customer's PIN will not work during system downtime. Please ask them to sign the Transaction receipt and verify their signature.

When the merchant services system is restored, the terminal automatically sends these Transactions to us.

If a Transaction is over your floor limit, the screen on your terminal will display a message 'input authorisation number', In this case you should call the authorisation centre:

1. Enter the last 7 digits of your merchant number and the Transaction details when prompted for authorisation;
2. Key in the authorisation number you are provided into the terminal;
3. The terminal then prints a receipt for the customer to sign and asks you whether you've obtained a valid signature;
4. If you are satisfied the customer's signature is valid, press 'Yes'. The system will then automatically send the Transaction for processing once the system is restored.

2.7.2 If you don't have Store and Forward

If you have a terminal that doesn't have Store and Forward, you can use offline paper vouchers to process the Transaction manually.

Remember, if a Transaction is above your floor limit you must obtain a 6 digit authorisation number which must be documented on the offline paper voucher or entered into the terminal as prompted.

Note: Inputting an invalid or incorrect authorisation number may impact the assistance we can offer you in disputing a chargeback.

Time limit

If we give you authorisation, the amount is reserved against the Cardholder's account until the Transaction is processed.

You must process or submit the Transaction to us within five Banking Days of authorisation or it will expire and you will lose the benefit of the authorisation.

2.8 Refunds

Refunds on Card Transactions must be returned to the same account used for the original sale where that account can be identified. If you give a refund to an account which is different to the account used in the original Transaction you may be breaching Card Scheme rules and will be wholly liable for any chargeback claim or dispute in respect of the original Transaction, regardless of whether we allowed you to process the refund. Never give cash refunds for Card Transactions.

When calculating refunds, you are responsible for the calculation and should rely on your own records, not solely on our reporting.

2.8.1 Refunds using a terminal

If you use a terminal, you can process refunds by selecting 'Refund' as the Transaction type on your terminal. The terminal will ask for a password.

Refunds during downtime

If your terminal is offline, use offline paper voucher to process this Transaction manually.

Include the refund amount on the Merchant Summary voucher under 'offline refund/ credit vouchers'.

If the value of the refund/credit vouchers exceeds that of the sales vouchers on any Merchant Summary, you must have the difference available in Your Account from the time you have posted the envelope to enable us to debit Your Account for the amount.

2.9 Securing customer information

When you accept Cards, you will be handling or transmitting Card and Cardholder details that are highly confidential.

Here are some of the things you must do to keep that information safe.

2.9.1 Always:

- ensure that any Card information that you transmit across the internet or other networks or that you store is encrypted in accordance with the Payment Card Industry Data Security Standard or any other prevailing card data security standard we advise you of from time to time;
- ensure that information you store is only accessible to people who are authorised to manage or view that data;
- store any records containing information such as copies of offline paper vouchers in a secure place only accessible by authorised people;
- after the period you need to keep the records has ended, destroy the records and any information in a way that ensures any information is unreadable.

2.9.2 Never:

- disclose or share any Card information with staff or any third party;
- request, use or store a Card number for any purpose that is not related to a Transaction;
- process a Card through any card reading device not authorised by us;
- ask for a Cardholder's PIN;
- store a Cardholder's Card, PIN or CVV;
- require the Cardholder to complete postcards or other forms that would result in account data being in plain view when mailed;
- require the Cardholder to provide their CVV or PIN on any written form.

2.10 Minimising fraud

By accepting Cards you provide convenience for both you and your customers, but there are risks.

One of the key risks is that third parties may use Cards or Card details fraudulently. You need to be concerned about this because fraud could lead to chargebacks and other losses to your business.

2.10.1 Examples of fraudulent use

Here are some common examples of fraudulent use of a Card:

- someone uses a stolen Card or account number to purchase goods or services fraudulently;
- a person known to the Cardholder uses a Card to order goods or services but has not been authorised to do so by the Cardholder;
- the customer falsely claims that he or she did not receive the goods or services;
- fraudsters run consecutive numbers on an internet site or Interactive Voice Response (IVR) in an attempt to find a valid Card number that they then use to purchase goods or services fraudulently;
- customer uses a stolen Card or account number to make a purchase and returns later requesting a refund to their own Card;
- customer makes a large order over the phone or online using a stolen Card or account number and requests part of the funds to be transferred to another account;
- manually entering stolen Card or account number details on the terminal or online merchant facility.

2.10.2 Some basic precautions

Make sure that you have policies and procedures for handling irregular or suspicious Transactions. Remind your staff that they must take steps to verify that the Cardholder is who they say they are.

Also, keep records of all Transactions and proof of delivery of goods or services for at least six months after the event.

Remember: Transaction authorisation doesn't guarantee that the purchaser is the true Cardholder.

2.10.3 Tricks of the fraudster

Fraudulent orders usually share a number of characteristics, especially for Card-not-present Transactions e.g. made over the internet, or by mail order or telephone order (often referred to as 'MOTO').

If you suspect the Transaction may be fraudulent, contact us immediately on 1800 230 177.

Here are some warning signs of possible fraud. One warning sign on its own may not necessarily be cause for alarm, but pay special attention if more than one factor is present:

Rush orders	Urgent requests for quick or overnight delivery.
Random orders	Customers who don't seem to care if a particular item is out of stock or isn't available in the style/colour originally requested.
Out of character orders	Transaction amount is inconsistent with the average transaction size of a typical order received.
Suspicious delivery address	Use of a post office box or an office address. If your business doesn't typically export goods, use caution when shipping to international addresses, particularly if you are dealing with a new customer or a very large order.
Multiple cards	If a customer wants to pay with multiple Cards.

Multiple purchases on one Card in a short period of time	Multiple Transactions charged to one Card over a very short period.
Terminal misuse	If a customer is taking a long time to enter their PIN, or is suspiciously handling the device.
Manual Card number entry	Customer requesting to manually enter their Card number on the terminal.
Hesitation (telephone orders or where the Card is presented)	Customers that hesitate or seem uncertain when giving personal information, such as a postcode or the spelling of a street or family name.

2.10.4 Card-present Transactions (where the customer is present)

Never accept a Card if:

- the terminal doesn't recognise the Card;
- the Card expiry date has passed;
- the Card or the signature has been visibly altered or tampered with;
- the signature doesn't match that on the back of the Card;
- the Card is damaged.

If any of these occur, ask the customer for another form of Payment. This applies to all Card types.

Other things to look for

Although having the Card available at the time of the Transaction gives some protection from fraud, there are still things you can look out for to reduce the risk even further:

- does the number on the Card match the number on the receipt?
- does the name match the customer?
- is the embossing on the Card clear and even, and does the printing look professional?
- does the signature on the Card match the signature on the sales slip?

Cardholder ID must be requested for certain Transactions only, such as manual cash disbursement or if you suspect fraud. If an ID has expired, does not match the name on the Card or the Cardholder does not provide identification, the merchant can choose not to accept the Card.

You should also:

- not hand-key in Transactions unless you have been approved to use MOTO functionality;
- arrange an alternative form of Payment, if the terminal response is 'declined';
- be wary if a customer presents a Card that rejects and then switches to another Card;
- make sure you don't process Transactions for someone else. Not only will you be liable for any chargebacks, we may also terminate your Facility if you do.

2.10.5 Card-not-present Transactions (where the customer is not present)

Card-not-present Transactions will require prior approval before enabling on any terminal.

Transactions of this nature carry a higher risk of fraud as Transactions are processed without the Card being swiped, inserted or manually imprinted by the merchant (e.g. Mail Order, Telephone Order, Internet based or manually keyed Transactions). As a result, you can't check whether the person you are dealing with actually has their Card with them or whether their signature matches that on their Card.

By carrying out some of the following checks (where appropriate, depending on the Transaction method) you can significantly reduce the incidence of fraudulent activity.

Check 1	**For online solutions, use additional security features such as fraud scrubbing or two-factor authentication tools such as 3D Secure**
Check 2	**For online solutions, use 'Card Verification Value' (CVV)** Ask the customer to input the CVV located on the Card signature panel or on the front of their Card. Verifying the CVV doesn't guarantee that the Card is not stolen or being used by someone who is not authorised to use the Card. It increases the likelihood that the person making the Transaction has the Card in their possession.
Check 3	**Ask for comprehensive customer details and do validity checks** Take reasonable steps to satisfy yourself of your customer's identity.
Check 4	**Follow up with an order confirmation** Call the customer some time later to confirm order details before delivering.
Check 5	**Ask for identification on delivery and don't leave goods at unattended addresses**
Check 6	**Use minimum and maximum Transaction amount controls** The size of the amounts will vary depending on your business. Minimum and maximum amount controls allow you to control risk.
Check 7	**Contact our call centre staff to verify suspicious activity on 1800 230 177**

2.10.6 Excessive fraud rates

We periodically measure merchant fraud rates and compare them against thresholds set by Card Schemes or industry bodies such as the Australian Payments Network.

If we consider that you have an unacceptable level of fraud, we may request that you implement measures to reduce your fraud rate.

Should your fraud rate not reduce to a level which is acceptable, the Cards Schemes or an industry body may issue a fine for which you will be liable.

2.11 Disputes and chargebacks

2.11.1 Card Scheme Disputes and Chargebacks

The rules of the Card Schemes, AMEX/JCB and Diners allow a Cardholder and the Cardholder's bank to dispute a Transaction in certain situations.

For example, if the Cardholder doesn't believe they authorised the Transaction, or says the goods were not delivered, that person can dispute the Transaction which may result in a chargeback.

Please note that you must not resubmit a previously charged back Transaction.

2.11.2 Examples of customer disputes

Some examples of customer disputes that can result in chargebacks are:

- the customer complains that goods or services are not as described on a website or in a mail order catalogue;
- the customer is billed twice for the same order or billed for an incorrect amount;
- the customer doesn't recognise the Transaction on their statement because the business name on the statement is different to the business name used on the website or mail/telephone order marketing materials;
- the customer argues that they never received the goods or services;
- there is confusion or disagreement between the customer and merchant over a return or refund amount;
- fraud (the customer claims they did not authorise the Transaction).

2.11.3 How the dispute process works

1. The Cardholder disputes a Transaction by advising their Card issuer. A Transaction can be disputed up to 120 days from the date of the Transaction or agreed goods/service delivery date, whichever is later. To be safe, keep clear and easy-to-read vouchers or records of Transactions and proof of delivery for at least 6 months after the date of delivery of goods or services.
2. The card issuer may send us a request for copies of documents and other supporting evidence to determine the validity of the Transaction or may raise the dispute with the relevant scheme.
3. Depending on the relevant Card Scheme's rules (whether it is Visa, Mastercard, UnionPay International or eftpos), we may contact you to ask for documentation or information to support or reject the dispute. Once a Transaction is disputed, it's your responsibility to prove that a valid Transaction occurred. You will have a limited timeframe to respond to any request by us, as set out in our request letter. For disputed AMEX/JCB or Diners Transactions, please refer to the relevant scheme.
4. Both banks, or the relevant scheme, evaluate the information and make a decision as to the validity of the dispute.
5. Where the fraud and authorisation related disputes reason code is provided by the issuer we do not generally have any ability to challenge the charge back and the Transaction will be 'charged back' (debited) to your bank account.
6. If the Cardholder dispute is not satisfactorily resolved or if we request supporting evidence and you don't provide this within the required timeframe or the relevant scheme decides in favour of the Cardholder, the disputed amount will be 'charged back' (debited) to your bank account.
7. If the Cardholder dispute is resolved in your favour the chargeback request is returned to the Card issuer and the Cardholder must pay their credit card bill as normal.

2.11.4 Minimising disputes

Keep good records

You can reduce the risk of chargebacks caused by customer disputes by keeping good records.

This will help you to find specific Transactions quickly and easily.

Inform the customer

Include all of the following information in your invoices, contract and promotional materials:

- your name as it will appear on the Cardholder's statement;
- your business address;
- customer service contact numbers;
- a complete description of goods and services provided;
- a specific delivery time;
- details of your return and cancellation policy;
- details of debit dates for regular instalments such as memberships or subscriptions.

2.12 Illegal Transactions

Some Transactions are illegal and if your Facility is used to process them you can find yourself in breach of Australian and international laws or the requirements of a Card Scheme.

For example you must not process any of the following:

Online Transactions

- relating to child pornography and other extreme sexual content;
- involving non-consensual and violent sexual content;
- involving the sale of tobacco or prescription pharmaceuticals;
- illegal gambling Transactions.

All Transactions

- that breach Australian or international laws, e.g. the sale of tobacco or liquor to minors;
- other types we tell you are prohibited by the Card Schemes, e.g. by Mastercard under their Business Risk and Mitigation (BRAM) programme and VISA under their Global Brand Protection Program (GBPP).

2.12.1 Non-compliance

If you have been found to have processed Illegal Transactions, the Card Schemes may impose a fine on us. You indemnify us against any loss resulting from any such fine and must reimburse us on demand.

In addition, we could terminate your Facility and list you on a Card Scheme database that could prevent you from operating a merchant facility in the future.

If you have any questions regarding Mastercard, Visa, UnionPay International or eftpos Transactions, please call us on **1800 230 177** or visit our Merchant Services website: **commbank.com.au/merchantservices**.

If you have any questions regarding AMEX/JCB or Diners Transactions, please contact the relevant scheme.

Part 3: Terms & conditions

3.1 About this part

This part sets out the terms and conditions that apply between you and us when you use your Facility. These terms are in addition to all other provisions of this booklet.

You must also comply with:

- Part 2: How to use your Facility;
- Part 4: Optional products and features (where applicable);
- the user guides or any other operating instructions for your Facility;
- any requirements that a Card Scheme or industry body impose on us that relate to your Facility (known as Card Scheme rules) that we tell you about;
- any other communication about your Facility, e.g. bulletins advising of changes to security or processing requirements.

Each of these forms your contract with us. You are bound by this contract and this booklet once we process and accept your application for a Facility and set up your merchant profile.

3.2 Equipment and software

3.2.1 Installation

You can use either our equipment and software, or your own. If you use your own equipment or software, then it must comply with our security and other requirements.

3.2.2 Upgrades

If you use our equipment and software you must allow us to upgrade it from time to time.

If you use your own equipment and software you must upgrade them whenever we tell you, e.g. when industry standards or our security standards change.

3.2.3 Maintaining your equipment

You must follow the security and other requirements set out in this booklet.

3.2.4 If your Facility is not working

We try to maintain your Facility, including all merchant services systems, in good working order and with as little downtime as possible.

We are not liable for any loss you incur if your Facility is not working, you can't process Transactions for any reason or because of any delay in processing.

3.3 Processing Transactions

3.3.1 Use of the Facility

Transactions processed through your Facility using unapproved channels or products is prohibited i.e. you process Card-not-present or eCommerce Transactions without our prior written approval.

3.3.2 Transaction records

You must:

- give us your records relating to any Transactions when we ask you for them;
- only process Transactions if the Cardholder has received the goods or services from you, unless the Cardholder has agreed to receive them later. Where the Cardholder has agreed to receive them later, the goods or services must be delivered within 12 months of the Transaction date;
- not split a single sale into more than one Transaction using the same card;
- not process purchase or refund Transactions through your merchant facility using either your own Card or a Card of an associated person. Using your Facility in this manner could result in your Facility being terminated.

3.3.3 Surcharging

If you charge a fee for Card Transactions:

- You must clearly and prominently display any surcharge before processing the Transaction;
- When refunding a Transaction you must refund any surcharge charged on the Transaction amount;
- For partial refunds, the surcharge must be pro-rated.

The surcharge must not exceed your cost of acceptance for the relevant Card Scheme. You should calculate your cost of acceptance at least once a year using the information we provide in your statements. You will receive an annual statement in July each year. There are regulatory consequences if you surcharge above your cost of acceptance. For more information visit the Payments System Regulation page at **www.rba.gov.au**.

3.3.4 No minimum Transaction amount

You must not impose any minimum transaction amount for Card Transactions.

3.3.5 No third-party processing

You must not process Transactions for someone else, unless we approve. Not only will you be liable for any chargebacks, we may also terminate your Facility if you do.

3.3.6 eCommerce Transactions

3.3.6.1 Authorisation limits

We may impose limits on the value of Transactions processed by you over periods of time. If proposed Transactions would result in the applicable limit being exceeded, we may reject the Transactions.

We will use reasonable endeavours to promptly notify you of any changes to those limits.

You are responsible and liable for all Transactions processed on your eCommerce facility. We may temporarily suspend your Facility if we believe it is under malicious attack, and use reasonable endeavours to notify you to resolve prior to re-enabling your Facility.

3.3.6.2 Your obligations

You must ensure that you:

- have and maintain adequate procedures and systems for processing Payments;
- correctly and promptly credit or debit, as the case may be, the amounts of each Payment to the applicable customer;
- store in a manner approved by us, the original records of each Payment received from a customer for a minimum period of seven years after the last Payment was made;
- have a fair policy for correction of errors and exchange and return of goods and services where a customer makes a complaint, or Customer Claim, or where we or a financial institution becomes involved in the correction of errors;
- promptly notify us if you are unable to apply Payments received by you from customers to accounts you maintain for your customers for any reason;
- notify us as soon as possible if you receive an erroneous Payment that may require a Correction and do all things reasonably necessary to ensure the error is corrected;
- take all reasonably necessary measures to resolve Customer Claims directly with the customers or other persons affected; and
- provide to us all information or documents as we may reasonably require relating to a Correction or customer.

3.3.7 Offering cash out and charge cards

3.3.7.1 Cash out

Cash out is only available on selected Cards. If you choose to provide Cardholders with cash out or cash with a purchase, the Cardholder must choose the 'Cheque' or 'Savings' option on a terminal rather than 'Credit'. Cash must only be provided directly to the Cardholder in the form of Australian legal tender (notes and coins).

You must not give cash out on credit cards, for contactless Payments or where the 'Credit' option is selected.

3.3.7.2 Credit/Charge cards (AMEX/JCB and Diners)

We may set your Facility to accept AMEX/JCB Cards if you have an existing relationship with the issuer or have been offered AMEX/JCB service by us.

To be able to accept Diners on your Facility you will first need to sign a separate agreement with them.

Once you have an agreement with Diners, contact us so we can set your Facility to accept Diners Cards.

Our only obligation to you in relation to any AMEX/JCB and Diners Transaction is to send the Transaction details to the scheme that issued the Card.

3.3.8 UnionPay International

We may make available to you acceptance of UnionPay International branded Cards. If we do, processing of those cards may be subject to additional terms and conditions available at: **commbank.com.au/unionpay**.

3.3.9 No book up arrangements

You must not hold a Cardholder's PIN or CVV as part of a book up arrangement.

3.4 Securing customer information

3.4.1 Data security standards

The Card Schemes have requirements relating to securing customer data known as the 'Payment Card Industry Data Security Standard'. They may in future have other data security requirements.

You must fully comply with the prevailing card data security standard as advised from time to time. If there is a data security breach, the Card Schemes, AMEX/JCB and Diners, may require an external investigation of your premises and systems. You agree to cooperate fully with the investigation and to pay the reasonable costs of the investigation.

3.5 Settlement & Payment

3.5.1 Maintaining an account

You must nominate and maintain an account for the duration of this Agreement.

Your nominated account must be in the same name as your Facility unless we agree otherwise.

We will credit Payments to your nominated account and debit fees and charges and other amounts payable under this Agreement from it.

Separate fee account

It you request and we agree, we may allow you to use two accounts, one for settling Transactions you process and one for paying your fees and other amounts you owe us (e.g. chargebacks).

Changes to Your Account

If you intend to change Your Account or payment channel, you must tell us before making any change. If we are not informed of a change and a settlement delay eventuates we will not be liable for any losses (including interest). If Your Account is with another financial institution and you change it, you will need to give us a new Direct Debit Authority.

3.5.2 How we pay you

We credit Your Account with the value of all valid sales and cash out Transactions, less any refund Transactions.

3.5.3 Statements

We send merchant statements and notices to your nominated postal address. It is your responsibility to advise us of any changes to your postal address. If you prefer to receive your merchant statements and notices electronically, please contact us to arrange this.

Electronic Transactions

You may select an automatic settlement time for your Facility or settle manually on certain devices. Where you do not select a settlement time, we will settle for you towards the end of the day.

Everyday Settlement

We settle all your electronic Mastercard, Visa, UnionPay International and eftpos Transactions up to settlement time, same day, 365 days a year. We call this Everyday Settlement.

This applies if you settle to one of our eligible business transaction accounts and you have been notified that Everyday Settlement applies.

If Your Account is with us but Everyday Settlement does not apply

We settle all your electronic Transactions up to settlement time, each weekday other than Public Holidays.

Transactions completed after settlement time, or on a weekend or Public Holiday, are processed on the next Banking Day.

If Your Account is with another financial institution

We credit or debit your Transactions as soon as practical, depending on your financial institution's process.

eCommerce multi-currency settlement

eCommerce multi-currency Transactions are settled daily net of all fees, including: interchange fees, other scheme fees, CBA margin, GST, and any other chargebacks or refunds processed against your Facility. Where debit transactions exceed your credit transactions processed on any given day, your settlement account will be debited for the difference in the settlement amount.

Manual Transactions

You must deposit the merchant copy of all offline paper vouchers with a Merchant Summary within three Banking Days.

If Your Account is with us, we credit Your Account when we receive the deposit, but you may not be able to withdraw the money for three Banking Days to allow for clearing time.

If Your Account is with another financial institution, it will be credited as soon as possible after deposit.

All vouchers must be legible, complete and correspond with the Merchant Summary. You will not get paid for any unclear, missing or unreadable vouchers.

3.5.4 What you must pay us

You must pay us (and we can debit Your Account with):

- any funds credited to Your Account in error;
- any chargeback amounts;
- fees;
- any other amounts you owe us under this Agreement;
- any negative net settlement at the end of the day. This includes settlements for which refund turnover exceeds purchase and cash out turnover.

Covering fees and chargebacks

Your Account must always have enough money in it to enable us to debit Your Account for the amounts you owe us.

If Your Account doesn't cover the amounts owed, we can:

- use our right of set-off (see *3.5.5 Set-off*);
- demand that you pay the amount from some other source;
- suspend your Facility; and/or

- if you fail to place enough money in Your Account within three Banking Days, terminate your Facility.

We will not be liable to you for any loss suffered or cost incurred, whether directly or indirectly, as a result of you not having sufficient funds in Your Account when we process a debit.

When you must compensate us

In some situations we may incur a loss or cost specifically relating to your Facility. You indemnify us against any such loss or cost and must compensate us on demand (except to the extent the loss or cost is proven to have been caused by our negligence).

These situations include:

- if you don't comply with this booklet in a material respect or any reasonable instructions we give you;
- where you damage our terminals or equipment, or damage is caused by fire, theft, flood or any other act in or around your premises (you will not be responsible for reasonable wear and tear resulting from the proper use of any terminals or equipment);
- any error, fraud or negligence by you;
- any dispute over goods or services between you and a customer;
- use of your Facility by anyone in a manner not authorised by you;
- if you process an Illegal Transaction;
- if there are excessive chargebacks, excessive levels of fraud or inappropriate use of your Facility (as determined by the Card Schemes or an industry body such as the Australian Payments Network);
- if a security breach occurs relating to your Facility leading to disclosure of Cardholder data.

Examples of compensation

Things you may need to reimburse us for include:

- any fines or costs we have to pay under Card Scheme rules or to an industry body such as the Australian Payments Network;
- losses we suffer due to Cardholder details being disclosed and us having to reimburse for unauthorised Transactions;
- any costs we incur to satisfy Card Scheme requirements, e.g. if we need to investigate security breaches or issues;
- repairs to our devices or other equipment.

At any time, if you receive Payment for goods or services prior to the delivery or provision of those goods or services, this raises additional business risks. We may require additional security to be held based on these additional risks.

3.5.5 Set-off

If we can't debit Your Account for an amount you owe us, we can deduct the amount from any other account you have with us. We can do this without demanding payment in advance.

We can also place a hold on Your Account and refuse to let you withdraw funds if we reasonably believe Transactions may be charged back, or Transactions you have processed may incur any other liabilities, fees or costs.

3.5.6 Forward Delivery Risk (FDR)

Forward Delivery Risk is the risk that:

- a Cardholder pays for a good or service to be delivered at a later date; and
- because that good or service is not later delivered, a chargeback is claimed and we need to reimburse the Cardholder.

If your business involves Card Transactions for goods or services which are to be delivered at a later date, and therefore we have an exposure to you for forward delivery risk, we may require you to do one or more of the following:

- provide information on your transaction profile;
- provide information for our credit assessment purposes;
- provide security to us to cover forward delivery risk (i.e. the increased risk of chargebacks) and other amounts owing by you;
- if Transaction values increase, provide additional security to us.

You must provide information on your Transaction profile on reasonable request and notify us if there is any change to your business that could increase the amount of sales that are not fulfilled at the time of the Payment transaction.

3.6 Fees

You must pay us the fees specified in the Fee Schedule or as we otherwise advise you. The Fee Schedule will be provided upon application and may be amended from time to time. In return we enable you to use the Facility under the terms and conditions of this Agreement.

3.6.1 When we deduct fees

Once a month we deduct fees for the Transactions you made in the previous month.

We also deduct some other fees, such as those for establishing and maintaining a Facility for You, at different times, as defined in the Fee Schedule, or otherwise on demand.

3.6.2 Publishing fees

Fees which are payable by you must not be disclosed to third parties.

3.7 Chargebacks*

Chargeback means you must reimburse us (and we can debit Your Account) for a Transaction amount that we previously gave you credit for.

We can chargeback a Transaction if:

- it is illegal;
- the Card was not valid at the time of the Transaction;
- the sales receipt has been altered without the Cardholder's authority;
- the Cardholder did not authorise the Transaction;
- it was made using your own Card;
- the Transaction amount is greater than your floor limit and you did not get an authorisation;
- you breached a relevant term of this Agreement;
- authorisation for the Transaction was declined for any reason;
- the Cardholder disputes liability for the Transaction for any reason;

- it represents the refinance of an existing debt or the collection of a dishonoured cheque.

*Only applicable for Mastercard, Visa, UnionPay International and eftpos. For AMEX/JCB and Diners, please refer to the relevant agreement.

3.8 Changing or terminating this Agreement

3.8.1 Changes

We can change any of the terms of this Agreement (including your fees and the Facility you use) at any time by giving notice.

If the change:

- introduces a fee or charge, we will give you notice of at least 30 calendar days;
- increases a fee or charge, we will give you notice of at least 30 calendar days.

If we believe a change is unfavourable to you, then we will give you prior notice of at least 30 days, subject to the following paragraph:

We may give you a shorter notice period, or no notice, of an unfavourable change if:

- we believe urgent action is necessary for us to avoid a material increase in our credit risk or our loss; or
- there is a change to, or introduction of a government charge that you pay directly, or indirectly, as part of your banking service. In that case, we will tell you about the introduction or change reasonably promptly after the government notifies us (however, we do not have to tell you about if the government publicises the introduction or change).

If the change relates to anything else, it will start on the date you receive the notice or any later date that we state in the notice. If you do not accept these changes you may terminate this Agreement, subject to any continuing obligations in this booklet. In this clause, a change does not include changes to interchange and other scheme fees, changes of which are set externally. For current interchange fees, contact the relevant scheme website. For current scheme fees, contact us.

Note: Written notices are taken to be received on the sixth Banking Day after posting.

3.8.2 Suspending your Facility

In any circumstance where we can terminate this Agreement, we may choose first to suspend your Facility.

If we can't agree with you on a way to address our reasonable concerns, we can terminate this Agreement immediately.

We can also terminate or suspend part of your Facility (e.g. an online solution or an optional product or feature) in the same way.

We may suspend your Facility without notice if we reasonably consider it necessary to protect our or your interests.

We will not be liable for any cost or loss (whether direct or indirect) that arises where we need to suspend your Facility.

3.8.3 Either of us may terminate this Agreement with notice

Either we or you may terminate this Agreement, by giving the other 30 days' written notice, specifying a termination date (written notices are taken to be received on the sixth Banking Day after posting).

3.8.4 When we can terminate this Agreement without notice

We can terminate this Agreement immediately if:

- in your application (or at a later time), you give us information which is materially incorrect, misleading, or not fully disclosed;
- we have reason to suspect (acting reasonably) that you have fraudulently processed Transactions (e.g. refunds), or allowed fraudulent Transactions to be processed through your Facility. This includes processing fraudulent Transactions on your own cards or cards of friends or associates;
- we reasonably consider that the risk of chargebacks, fraud or other losses relating to your Facility is too high;
- you cease business, become bankrupt or insolvent, have a receiver appointed, go into liquidation or enter into an arrangement with your creditors;
- you close Your Account without first letting us know;
- you breach any material terms of this Agreement, or you repeatedly breach any term of this Agreement;
- you have breached, or we reasonably suspect you of breaching or being complicit in the breach of any laws in a material respect, including those relating to anti-money laundering, counter-terrorism financing, sanctions, anti-bribery and corruption or privacy;
- it is identified that you have used your Facility through any unapproved channels or products.

We will try to give you verbal or written notice before we terminate this Agreement. If we can't contact you we can terminate immediately.

3.8.5 What happens when this Agreement terminates

Us

When this Agreement terminates, we:

- are no longer obliged to acquire Payments on your behalf;
- may enter your premises to repossess any unreturned equipment. We will try to give you reasonable notice. If we can't contact you we can enter your premises without notice;
- may debit any outstanding fees to Your Account, including termination fees.

If we terminate this Agreement, we will give the Card Schemes your details and the reasons why we terminated.

The Card Schemes may give this information to other financial institutions if you apply for a new facility through them. This information may then affect your ability to get that facility.

You

When this Agreement terminates you must:

- not process any further Transactions;
- maintain an account for 180 days so that we can continue to charge fees and process chargebacks to Your Account;
- continue to reimburse us for any chargebacks or other losses we reasonably incur;
- return to us within 14 days all equipment and any other material we reasonably specify;
- if applicable, contact AMEX/JCB and/or Diners to terminate any agreement you have with them.

3.9 Miscellaneous

3.9.1 Information

We may share your information with others as set out in our application form and our Privacy Policy available on our website. New technologies let us combine information we have about you and our other customers, for example Transaction information, with data from other sources, such as third party websites or the Australian Bureau of Statistics. We analyse this data to learn more about you and other customers, and how to improve our products and services. We sometimes use this combined data to help other businesses better understand their customers. When we do, we don't pass on any personal information about you.

We may also get from or give to any person involved in any Card Scheme, information about you for any purpose to do with the operation of that scheme.

You must tell us of any important changes in your business, such as your contact details, change of ownership, or a change in types of goods or services being sold.

You must provide us with any information we reasonably request and allow us to enter your premises to conduct any audits on giving you reasonable notice.

3.9.2 Notices

We can give you a notice in one of the following ways:

- in-person - give it personally to you, or to one of your staff at your place of business;
- by post - leave it at or send it by prepaid post to your last address notified (written notices are taken to be received on the sixth Banking Day after posting);
- by fax - send it by facsimile to the facsimile number last notified (faxes are taken to be received when the transmitting machine reports that the whole fax was sent);
- online - so long as you have not opted out, we can provide notices to you electronically by your last email address notified or by posting the notice on our website and sending you an email that the notice is ready for viewing;
- newspaper publication - publishing it in local or national media (in which case we will also post the notice on our website).

3.9.3 Governing law

This Agreement is governed by the law in force in New South Wales. Each party irrevocably and unconditionally submits to the non-exclusive jurisdiction of the courts of the jurisdiction specified in New South Wales and courts of appeal from them for determining any dispute concerning this Agreement or the Transactions contemplated by this Agreement.

3.9.4 Code of Banking Practice

The Code of Banking Practice or the Banking Code of Practice, applies where relevant to your Facility if you are a small business as defined in the Code of Banking Practice or the Banking Code of Practice (as the case may be) or an individual.

Anything that we are required to give to you under this Code may be given to you:

a. in writing, electronically or by telephone;

b. by telling you that the information is available on a website or other electronic forum; or

c. as otherwise agreed with you.

However, if the Code specifies the method of communication, then we will comply with that method.

3.9.5 Sale of business

If you sell your business, the new owner will need to apply for a new Facility with us if they wish to continue using our merchant services. You can't transfer a Facility without our consent.

3.9.6 Commissions

We may pay a commission to anyone that introduces your business to us. This may be a flat fee, or based on your Transaction volume.

3.9.7 Severance

If any part of this Agreement is found to be void or unenforceable for any reason, the rest of this Agreement will continue to apply.

3.9.8 Use of BPOINT logos and trademarks

You are authorised (subject to any directions which we may give) to use the BPOINT logos, trademarks or names on bills and any other related material approved by us for the sole purposes of advertising your participation in and promotion of BPOINT to customers.

You undertake to use only literature or promotional materials provided or approved in advance by us for the above purposes.

If you use the BPOINT logo or word BPOINT you must:

- always use the complete BPOINT logo Mark design and not use any variations to the word Mark "BPOINT" (the word Mark "BPOINT" may be used without the BPOINT logo Mark design; and the BPOINT logo Mark design may be used without the word Mark "BPOINT");
- not use the term "BPOINT" in the possessive or as an adjective (e.g. not use the terms "BPOINT's customers" or "BPOINT billers").

3.9.9 Downloading material from our sites

Any material developed or provided by us, including logos, marketing material, file specifications and technical specifications, which you download from Bank websites (Bank Material) is owned by us and/or our licensors. You may only use the Bank Material for the purpose of receiving Payment through BPOINT.

You should access Biller reports each Banking Business Day in order to apply Payments received and monitor approved and declined Transactions for reconciliation purposes. Biller Reports are available from your electronic banking channel but may relate to Transactions on the prior Banking Business Day.

3.9.10 Trustee

If you are acting in a trustee capacity, this Agreement binds you in your own right and in your capacity as trustee.

Part 4: Optional products and features

4.1 About this part

In addition to our card processing facilities, we also offer:

- Pi and CommBank Small Business Applications - enables you to perform additional functions through our compatible terminals and apps which you can download;
- eCommerce value added services - enables you to conduct a range of additional functions from our suite of online merchant facilities;
- Merchant Choice Routing – enables you to select your preferred network for routing multi-network contactless debit card Transactions.

This part sets out the additional terms and conditions that apply to you if you use these optional products or features.

If there is any inconsistency between this Part 4 and any other section of this booklet, the provisions of this Part 4 prevails to the extent of the inconsistency.

4.2 Pi and CommBank Small Business Applications

Clause 4.2.1 applies only to users of an Albert Terminal.

Clause 4.2.2 applies only to users of the CommBank Small Business Application and a Mobile Terminal.

The remainder of this clause applies to all users who access any of these services.

4.2.1 Pi Platform

The Albert terminal is a custom-built multifunctional terminal that allows you to accept Payments, download apps from the Pi AppBank and create and upload your own apps (Albert Terminal). Our Pi AppBank hosts apps developed by us and by third party developers.

Apps

We are not responsible for the performance or availability of apps created by a third party developer.

If you download an app from the Pi AppBank, you will need to accept the terms and conditions for that app. We will debit Your Account for fees payable under the terms and conditions for each app you purchase through the Pi AppBank, including from third party developers. We may receive commissions or fees from developers or providers of apps as a result of your purchase or use of their apps.

If you have authorised us to debit third party developer's fees from Your Account, we may provide those developers with information concerning your download and usage of the developers' app in connection with the payment and calculation of those fees.

If you have any questions on the functionality of an app, or a dispute in connection with an app, you should contact the developer of that app as set out in the terms and conditions for that app.

We may remove or prevent access to an app if we consider it necessary, for example due to security concerns. If you wish to create and upload your own app, you will need to accept the developer terms and conditions.

4.2.2 CommBank Small Business Application

The CommBank Small Business Application is designed for small business and enables merchants to electronically create Billing Material using their Mobile Terminal linked to their compatible mobile smartphone or tablet device and to email them to themselves and their customers. It also enables acceptance of Payments through BPAY electronic payment services.

Merchants can process Transactions with a customised Mobile Terminal linked to their compatible mobile smartphone or tablet device.

Using a compatible Mobile Device

You can only use your compatible Mobile Device to connect to your Mobile Terminal. From time to time we may vary the types of compatible Mobile Devices which we list on our website. You are responsible for downloading from the website approved by us to your Mobile Device all software needed to connect to your Mobile Terminal and to use the CommBank Small Business Application.

Billing Material

You are responsible for the accuracy of the information in both the Billing Material and email addresses. You are also responsible for the security and storage of Billing Material and information and messages created by you.

Use of BPAY* to receive Payments

You acknowledge that, before we agree that you can receive Payments through the electronic payments service (BPAY) promoted by BPAY Pty Limited ABN 69 079 137 518, you must agree to the BPAY Sub-Biller Agreement and have received a copy of the Operations Manual. You must perform all your obligations as a participating biller as set out in the Operations Manual and otherwise comply with the terms of the BPAY Sub-Biller Agreement. On termination of this Agreement or the BPAY Sub-Biller Agreement, you must immediately advise your customers that they can no longer make Payments through BPAY.

*BPAY is a registered trademark of BPAY Pty Ltd

4.2.3 Instruction manual

We issue instructions or manuals, which you must follow, explaining how to:

- access the Pi Platform and use your Albert Terminal; and/or
- access the CommBank Small Business Application and use your Mobile Terminal.

We may change these instructions or manuals from time to time. We recommend checking the CommBank website for the most up-to-date instruction manuals.

4.2.4 Software

We may from time to time update the software needed to use your Albert Terminal, your Mobile Terminal, the Pi Platform or the CommBank Small Business Application (for example to enhance security or to provide additional features). We may require you to download updates to the software to continue to access these services. We may temporarily remove or prevent access to or use of the software if we reasonably consider it necessary, for example to install a security patch or upgrade. We are not liable if a third party prevents access to or removes the software from an apps store for any reason but we will endeavour to restore access to the software as soon as reasonably practical.

4.2.5 Telecommunication costs

You are responsible for any charges imposed by your telecommunications provider for accessing the Pi Platform or CommBank Small Business Application or to use your Albert Terminal or Mobile Terminal with your compatible mobile smartphone or tablet device, including call costs and data costs associated with downloading software.

4.2.6 Security and privacy

You must take steps reasonably necessary to stop unauthorised access to your apps and your terminal or compatible mobile smartphone or tablet device, including information relating to your customers. If you link a terminal to a WiFi network, the network must be secured with a password which is different to the factory default and which must not be disclosed to your customers or members of the public. You must comply with Australian privacy laws. You are responsible for the security of apps downloaded to your terminal or Mobile Device.

For CommBank Small Business Application users, you must not leave your compatible mobile smartphone or tablet device unattended and left connected to the CommBank Small Business Application or Mobile Terminal. When not in use, you must lock your compatible mobile smartphone or tablet device using a password known only to you.

4.2.7 Trademarks and copyright

You acknowledge and agree that the CommBank, BPAY, Albert, Pi, Leo and Emmy trademarks and logos and other product and service names (Trademarks) are our trademarks and that you will not display or use the Trademarks other than in marketing materials provided by us which you must not add to or alter in any manner. You must comply with any written direction received from us in respect of the use of the Trademarks. Any material developed or provided by us, including software, logos, marketing material, file specifications and technical specifications, which you download from our web sites (Bank Material) is owned by us and/or our licensors and may be subject to protection by copyright laws, or laws protecting trademarks and trade. Except as otherwise expressly stated in the Terms and Conditions, you may only use the Bank Material for the purpose of receiving Payment through your Albert Terminal or Mobile Terminal and, in respect of the CommBank Small Business Application, to send Billing Material to your customers and to yourself. You may only use any marketing material solely to promote your ability to accept Payments through your Albert Terminal or Mobile Terminal. You acknowledge and agree that we and/or our licensors retain all intellectual property rights of the Bank Material and you must not use the Bank Material in any manner that would infringe, violate, dilute or misappropriate any such rights. On termination of this Agreement, your right to use Bank Material ceases and, for CommBank Small Business Application users, you must remove it from your compatible mobile smartphone or tablet device.

4.2.8 Communication or service failure

We do not warrant that the Pi Platform, apps created by a third party developer or the CommBank Small Business Application we provide will be fault free or that any problem with the Pi Platform or the CommBank Small Business Application can be solved immediately or quickly. You acknowledge that those services may rely on factors outside our control. We will use reasonable endeavours to overcome any fault in the services we provide to you as quickly as possible, We are not liable to you for any direct or consequential losses which arise from disruptions to our systems or processes. We are not responsible for any applications provided by developers other

than ourselves (and whether or not downloaded from the Pi App bank) to your Albert Device or compatible mobile smartphone or tablet device. We can't control the operations and systems of other institutions or telecommunication providers, and we're not liable to you for any loss from disruptions to the operations or systems of those institutions or providers.

Billing Material means quotations, invoices, receipts and payment information.

Compatible mobile smartphone or tablet device means the compatible internet connected device (for example a compatible mobile phone or tablet device) you use to link to your Mobile Terminal.

Mobile Terminal means an Emmy or Leo terminal or any replacement terminal provided to you by us.

4.3 eCommerce value add services

4.3.1 Tokenisation

To store Card (excluding UnionPay International) or bank accounts in our Tokenisation service you must obtain our approval and if approved, provide us with the following information to be stored through our Tokenisation platform:

- scheme Card particulars;
- scheme debit card particulars;
- charge card particulars; and
- bank account particulars.

The record provided to us must be in the format approved by us.

On receipt of the records, we will allocate an identifying number (token) to the relevant Card, charge card or bank account particulars of each customer identified in such record and retain that record until advised by you or on termination of the merchant Facility.

We will make available to you the tokens allocated by us corresponding to each of your customers whose particulars you have supplied to us.

By providing us with the token of your customer and instruction to obtain a Payment, you are deemed to have provided us with that customer's relevant payment particulars.

4.3.2 Schedule Payments

To use the Schedule Payments service you or your customer must set up a schedule of Payments and provide us with details of the Card, charge card or bank account to be debited.

By providing us with a schedule and the Card, charge card, bank account or token, you authorise us and we undertake to schedule your customer's Payments and process the Transactions automatically without having to further instruct us.

You must advise us of any change to Scheduled Payments no later than 11:30pm Sydney time the day prior to the day the Payment is scheduled to be processed.

4.3.3 Delays

We will not be in breach of this Agreement merely because of a delay in the processing of Payments, including because our systems are not working and we will not be liable to you for any such delay.

4.3.4 Fraud Prevention Options

If you have a website, we recommend implementing the following security features:

Fraud Scrubbing

Fraud Scrubbing solutions can be used to identify, blacklist and stop potential fraudsters, and computer macro programs from accessing the payment page. It utilises checks on country of card origin, scripting where the online user must enter a current word/phrase on webpage, IP address checks, cross checking fraud databases, validation tests, etc.

Mandatory CVV capture

Enable mandatory capture of the Card Verification Value and check its validity during the Transaction. This ensures the Card is with the person making the Transaction, however it does not guarantee it is the Cardholder making the Transaction.

3D Secure (3DS)

3D Secure uses advanced authentication mechanisms to validate the payer's identity allowing users to make better risk based decisions to better protect you. 3D Secure helps ensure that the Cardholder is the person placing the order with their own Card.

Note: Please refer to the Visa and Mastercard websites for Cards excluded from this program.

4.4 Merchant Choice Routing

Merchant Choice Routing (MCR) is an optional feature available on select terminals and pricing plans.

Where your Cardholder uses a multi-network Card for a contactless Payment (i.e. branded by more than one Card Scheme), MCR allows you to select which network brand on the Card is used for processing the Transaction by allowing you to select a threshold for each network. MCR may not work on all Cards or Payments using digital wallets.

If you are approved for and enable MCR:

- you must follow our set-up directions;
- contactless Card Transactions on multi-network Cards will be routed to your nominated available network;
- it is your responsibility to understand interchange costs associated with processing Transactions through each network on an ongoing basis. We cannot advise you which network will be best for you. For current interchange fees, contact the relevant network or view their website;
- we will not be responsible for any delays in implementing or disabling MCR;
- you must ensure that refunds are processed through the same network (i.e. Card Scheme) as the original Transaction;
- you acknowledge that we may temporarily suspend or permanently deactivate your MCR capability and revert to the default network for processing where we reasonably consider it is necessary. Should this occur, we are not liable to you for any loss or higher interchange costs.

Part 5: Meaning of words

This part lists the key terms used in the document and what they mean.

When we refer to a document, including this Agreement, this includes any variation or replacement of that document.

Where we give examples of something this does not limit other situations that may also apply.

Agreement
The agreement between you and us regarding your Facility and any related services, as set out in this document.

Banking Day
A weekday other than a day that is a Public Holiday.

BPOINT
The service we offer for the processing of Payments by customers by debit entries to credit or debit accounts held with a financial institution or any other payment method made available from time to time under this Agreement to credit to Your Account.

Card
Any debit or credit card, but not a charge card, regardless of its form, whether traditional card, virtual, part of a digital wallet, wearable device or otherwise tokenised.

Cardholder
A person to whom a Card is issued at the accountholder's request.

Card-not-present
This includes online Transactions and Transactions by mail order or phone.

Card Scheme
The Mastercard, Visa, UnionPay International and eftpos card schemes. These schemes publish rules that apply to entities like us that process Card Transactions on behalf of merchants.

Correction
A Transaction to correct a processing error. It does not include the processing of Customer Claims.

Customer Claim
A claim by a customer for a refund of a Payment (made using BPOINT) for any reason.

CVV (Card Verification Value)
The last three digits printed on the signature panel on the back of a Card used in a Card-not-present situation to confirm that the customer is holding the actual card (also known as the "CVC2" or "CW2").

Facility
Means your merchant facility and includes using terminals, online solutions and optional products or features.

Fee Schedule
Any list or notice of fees we provide to you.

Illegal Transaction
A Transaction which is contrary to applicable laws or not permitted under Card Scheme rules as notified to you.

Payment
A payment made, or to be made, by or on behalf of a customer to you through your Facility which is credited, or to be credited, to an account of yours.

Public Holiday
A day which is a national public, bank or special holiday.

Transaction
Any sales, refund or cash out transaction completed by use of a Card or Card details (including a bill payment).

We
Commonwealth Bank of Australia ABN 48 123 123 124.

You
The person we approve as the "merchant" when we process your application form. If there is more than one, "you" means each person separately as well as every two or more of them jointly.

Where we refer to "you" doing something, this also includes anything your staff or anyone else acting on your behalf does.

Your Account
The bank account you must maintain under this Agreement, and where the context permits includes any separate account we permit under section 3.5.1 Maintaining an account.

ADB3864 090819