CommBank Smart Health

Terms and Conditions

Effective 5 November 2023

These products are issued by the Commonwealth Bank of Australia ABN 48 123 123 124 AFSL and Australian credit licence 234945.

008-054 051123

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, processing Claims, 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/smart-health
General enquiries	Freecall **1800 222 484** 8 am to 8 pm (Sydney time), Monday to Friday, excluding national public holidays.
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:

- set up and operate your Facility; and
- manage risks relating to patient disputes and chargebacks.

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

2.2 Getting started – CommBank Smart Health

CommBank Smart Health includes an online portal called the "CommBank Smart Health Hub".

You must log in to the Hub to complete your Facility set up. You will receive a welcome email when your Facility is registered which will include your login details. You will also receive a step-by-step user guide to use and operate CommBank Smart Health, including how to navigate the Hub which may also be accessed at any time via the 'Support' section in the Hub.

The Hub is used to:

- register Providers you wish to allow to process Claims;
- create user profiles for other people you may wish to access the Hub;
- link your terminal;
- complete integration to practice management software (if applicable);
- access reporting and reconciliation data.

2.3 Getting started – Terminals

Where your Facility includes a terminal, here are the steps you need to follow to get started:

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.

Step 2 – Establishment of Facility and installation of terminals and equipment

Depending on your merchant product, our installers may 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.

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.

Step 4 – Stationery
To ensure your terminal works properly, you must use our stationery. We give you an initial supply of free stationery to get you started.

Step 5 – Linking your terminal to the Hub
Prior to your terminal being installed, you will need to have logged into the Hub and should be aware of the "terminal" section within the Hub, as your terminal installer will require you have this open or available. User guides for CommBank Smart Health are also available within the Hub.

Step 6 – Initial training
Depending on your merchant product, either our installers will provide start-up training on how to operate the equipment or you will be provided a training video.

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

Step 7 – Practice management software integration
Where you are using practice management software approved by us, you will be required to follow the instructions within the Hub to complete your integration to CommBank Smart Health.

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.

Further, you must ensure that any terminals or other equipment we provide you:

- are not altered, repaired or maintained by parties not authorised by us;
- are not connected to any peripheral with cables or accessories not certified by us;
- are not operated outside of the product specifications;
- do not suffer from abuse, negligence, accident, liquid spillage, pest infestation, floods or lightning damage;
- are not tampered with, opened or have a serial number that has been removed;
- are not operated with operating supplies, including paper, accessories, chargeable batteries, not certified by us; and
- do not have software installed by unapproved providers.

Any terminal or other equipment we provide you, remains our property. Do not tamper with, remove terminal housing or attempt to repair any terminals or other equipment provided by us, yourself. You will be responsible for any damage to the terminal or other equipment.

If you have any concerns about any terminals or other equipment we provide you, contact us on 1800 222 484 immediately. We will repair or replace any faulty terminals or equipment as soon as reasonably practicable. Please use the downtime procedures until it is fixed or replaced.

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

2.4.2 Terminal security

It is important that you keep your terminal secure and prevent unauthorised access.

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

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);
- you should think about how customers can access the terminal so that they can protect the entry of their PIN in the terminal by way of shielding with their hand or body;
- you need to ensure that security cameras will not be positioned or focused on the terminal so that PIN entry can be recorded;
- check the terminal regularly for any skimming devices and check the surrounding areas for any cameras;
- don't disclose your terminal password to anyone, other than 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 222 484**; and
- call us immediately on **1800 222 484** 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.

2.5 Ordering additional stationery

To order stationery, visit **commbank.com.au/eftposstationery**. If you don't have access to the internet, call us on **1800 222 484**. 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, for a Transaction above the floor limit, 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 mode that comprises of:

- a transaction floor limit for debit and credit cards below which transactions can be completed without an authorisation code;
- a transaction count for the number of transactions that may be stored when offline and forwarded to the Bank for processing when reconnected;
- a set of response codes that apply when the terminal goes into Store and Forward mode.

If you're not sure whether you have this, call us on **1800 222 484**. 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 Cardholder'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 into the terminal the authorisation number provided;
3. The terminal then prints a receipt for the Cardholder to sign and asks you whether you've obtained a valid signature;
4. If you are satisfied the Cardholder'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, depending on the type of merchant facility you have, you may be able to 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. In more serious instances it may lead to Card Scheme penalties or the termination of this Agreement.

2.7.3 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 the password which is set-up at the time of installation.

2.8.2 Refunds during downtime

If your terminal is offline, use offline paper voucher to process the Transaction manually and 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 Cardholder information

When you accept Cards or process Claims, 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 and processing Claims you provide convenience for both you and your patients, 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.

You must ensure that you only process genuine and accurate Claims and that they correspond with the patient and services provided. Claims may be rejected or reversed where insufficient or incorrect information is provided, or the Claim is not processed in accordance with our reasonable instructions or the rules of Medicare, DHA or a Health Scheme.

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;
- Someone uses another person's details to claim for health services from a Health Scheme;
- Someone known to the Cardholder uses a Card to order goods or services but has not been authorised to do so by the Cardholder;
- The Cardholder falsely claims that goods or services were not received;
- 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;
- Someone uses a stolen Card or account number to make a purchase and returns later requesting a refund to their own Card;
- Someone 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;
- Someone manually enters 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 222 484**

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.
Incorrect patient details	A patient tries to use a family member's or friend's Medicare or Health Scheme details to process a Claim.
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 are 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	A customer requesting to manually enter their Card number on the terminal.
Hesitation (telephone orders or where the Card is presented)	A customer hesitates or seems uncertain when giving personal information, such as a postcode or the spelling of a street or family name.

2.10.4 Card-present Transactions

Never accept a Card if:

- the terminal doesn't recognise the Card;
- 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.

You should also

- process all Transactions online using the terminal or seek a manual authorisation number;
- not hand-key in Transactions unless you have been approved to use MOTO functionality;

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

2.10.5 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?
- Does the individual reference number or Health Scheme details match the patient?
- 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, you can choose not to accept the Card.

You should also:

- arrange an alternative form of payment or use of another Card, if the terminal response is 'declined';
- be wary if a customer presents a Card that is rejected 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.

2.10.6 Card-not-present Transactions (e.g. mobile application transactions)

We may from time to time provide our technology to private health insurers or Health Schemes to integrate within their own mobile apps. Where your patient is registered within one of these apps, CommBank Smart Health allows you to submit an in-app Claim and Card Transaction for your patient to approve. Approved Claims and Card Transactions will be processed via CommBank Smart Health.

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:

- Ask for comprehensive patient details and do validity checks;
- Take reasonable steps to satisfy yourself of your patient's identity;
- Contact our call centre staff to verify suspicious activity on **1800 222 484**;
- Contact Medicare, the private health insurers and/or Health Scheme to verify suspicious activity.

2.10.7 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. Medicare, private health insurers and Health Schemes also periodically measure fraud rates.

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 are required under this Agreement to indemnify us and pay.
- Medicare, private health insurers and/or Health Schemes may issue us with a notice to deregister you from our systems, in which case you may no longer be able to process Claims.

2.11 Disputes and chargebacks

2.11.1 Card Scheme Disputes and Chargebacks

The rules of the Card Schemes, AMEX/JCB, UnionPay International 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 or services 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 Cardholder disputes

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

- the Cardholder complains that goods or services are not as described on a website or in a mail order catalogue;
- the Cardholder is billed twice for the same order or billed for an incorrect amount;
- the Cardholder 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 Cardholder argues that they never received the goods or services;
- there is confusion or disagreement between you and the Cardholder over a return or refund amount;
- fraud (the Cardholder 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 540 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 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 by keeping good records.

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

Inform the patient

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.

You must not process any Transactions:

- that breach Australian or international laws;
- other types, we will tell you from time to time, 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 224 484**.

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.

Sub-Part A deals with your use of your Facility for Card Transactions.

Sub-Part B deals with your use of your Facility for processing Claims.

Sub-Part C deals with your Facility generally.

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 requirements of Medicare, private health insurers, and/or Health Schemes that we tell you about in addition to any other obligations you may owe to them;
- any other communication about your Facility expressed to form part of this Agreement, 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.

Part 3A: Card Transactions

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.

Any power adapters or chargers you use must be in accordance with Australian safety standards.

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.

If you are experiencing any issues with your Facility, please let us know as soon as possible so we may work to resolve the issue promptly.

3.3 Processing Transactions

3.3.1 Use of the Facility

Transactions processed through your Facility using unapproved channels or products are prohibited i.e. you process Card-not-present 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 choose to surcharge for Transactions, it is your responsibility to ensure your surcharges are not excessive. You should review and as appropriate, adjust your rates of surcharge regularly, but at least every year. To assist you, we provide details of your average cost of acceptance for each Card Scheme in your merchant statements. You will also receive an annual merchant statement in July each year.

If you choose to surcharge, you must also:

- Clearly and prominently display the surcharge before processing a Transaction so as to allow a Cardholder to choose another payment method if they desire; and
- Refund any surcharge when refunding a Transaction (this may require pro-rating the refund of a surcharge for partially refunded Transactions).

There may be regulatory consequences for excessive surcharging. For more information visit the Payments Surcharges page at **accc.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 CommBank Smart Health Facilities

CommBank Smart Health enables Transactions to be processed in-app and on terminals. Facilities created as part of CommBank Smart Health cannot be used for any other purpose other than processing Card Transactions using CommBank Smart Health.

3.3.7 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.

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.

3.3.8 Offering cash out and charge cards

3.3.8.1 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 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, where the 'Credit' option is selected.

You must not give cash out on UnionPay International cards (even if they are debit cards).

3.3.8.2 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.

3.3.9 UnionPay International

We may make available to you acceptance of UnionPay International branded Cards. UnionPay International Card transactions must not be processed if your Facility is offline. If your Facility is offline, you must not:

- accept UnionPay International Cards;
- provide refunds on UnionPay International Cards; or
- use offline paper vouchers, Store and Forward does not apply and the authorisation centre is not able to approve the UnionPay International transactions.

Some UnionPay International Cards don't have cardholder names or expiry dates. You can still process a transaction if a UnionPay International Card doesn't include either or both of these.

We recommend you only process transactions where the Card is present. If you decide to process card-not-present transactions and are not able to verify the customer's full name, address and phone number (because the customer is an overseas resident) you will be liable for any chargebacks.

The period for UnionPay Cardholder disputes is up to 180 days.

3.3.10 No book up arrangements

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

3.3.11 Contactless Transactions and network selection

Contactless/eCommerce Transactions are routed for processing to the network which corresponds with the type of Card used by the Cardholder. For Multi Network Debit Cards, the Transaction is generally routed for processing through the primary network branded on the Card.

Unless you have opted to implement least cost routing, we may vary the networks through which contactless and/or eCommerce Transactions are routed at any time, without notice.

3.4 Card security standards

The Card Schemes have requirements relating to securing Cardholder 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 Card settlement and Payment

3.5.1 How we pay you

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

Settlement amounts will be net of any Chargeback received up to settlement cut-off times.

3.5.2 Daily settlement cut-off

All Transactions are automatically settled using a daily settlement cut-off time of 10pm (Sydney time). Any Transactions processed after this time will be processed for settlement on the following Banking Day. You may choose to manually settle your Facility, however doing so will impact the transaction reporting available through the Hub.

3.5.3 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.

In this case, 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.

3.5.4 Manual Transactions

For Transactions processed manually, 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.

3.5.5 Forward Delivery Risk (FDR)

If you receive Payments for goods or services prior to their delivery or provision, there is an increased risk that we will need to process a chargeback without Your Account having sufficient funds to cover that chargeback. Because of this increased risk we may (acting reasonably) require you to do one or more of the following at any time:

- Provide information about any Payments received where the goods or services are provided at a later time;
- Provide information on your Transaction profile;
- Provide information for our credit assessment purposes, including periodic credit reviews;
- Maintain Your Account for the settlement of Transactions with us;
- Provide security (including any additional security) to us to cover any chargebacks and amounts owed by you.

You must 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; or
- period between date of Payment transaction and delivery or provision of the related goods or services.

The requirements contained in this clause 3.6 are material terms of this Agreement.

3.6 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 material term of this Agreement;
- authorisation for the Transaction was declined for any reason;
- the rules of any Scheme require or permit us to do so in circumstances of a Cardholder dispute;
- 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.

Part 3B: Health Claims

3.7 Co-operation and accessing CommBank Smart Health services

Claims processed through CommBank Smart Health are provided under arrangements with the party who pays for or contributes towards the claim (for example Medicare or a Health Scheme). Private health insurance Claims are provided to you under arrangements with DHA. Where you or your Provider require an authorisation from Medicare, DHA or a Health Scheme to process Claims. You or your Provider must obtain that authorisation before using the relevant CommBank Smart Health claiming service. You must provide us with evidence of such authorisation if we request it.

You must co-operate with us, Medicare, DHA, Health Schemes and/or the Commonwealth Ombudsman (as applicable) in relation to the investigation of any complaint or issues relating to the use of your CommBank Smart Health facility.

3.8 Practice and Provider authority

You must procure, and you represent and warrant that you have obtained, the authority of each Provider and each other user for whom you establish a profile on the Hub, to have a profile established on the Hub and to have their details published on the Whitecoat directory.

You are responsible for any transactions initiated or performed by a Provider or other user for whom you have established a profile on the Hub and for any of their acts or omissions in relation to the Facility.

You indemnify us for any losses, claims, actions or demands arising from any use of the Facility by any Provider or other user for whom you have established a profile on the Hub except to the extent such losses, claims, actions or demands arise from our own negligence or wilful misconduct or that of our agents.

3.9 CommBank Smart Health Hub

You are responsible for securing your login details and for any users granted access to the Hub under your profile and must take precautions to prevent unauthorised access. This may include staff training or the use of software such as anti-'spamming', anti-'key logging' and anti-'virus' software.

Within the Hub you may also receive notices, access reporting and reconciliation information including any payments and Claims processed via CommBank Smart Health. You (or any user authorised by you) may also request access to other optional products or features.

You are responsible for, and authorise us to action, any request, communication or instruction given in the Hub using login details attributed to your Facility as being made by you, including electronically executed documents. We don't need to verify the authority of any user of your login details unless you have told us to cancel any login details. You are also deemed to have received a notice or other communication we send you through the Hub which may be viewed or accepted by your users. You must ensure that any users you permit to access the Hub are aware of and follow these terms.

3.10 Information accuracy

You must:

- follow any Claim processing instructions we reasonably provide you;
- ensure that you only submit genuine and accurate Claims and that they correspond with the patient and services provided;
- provide us with any documentation to support a Claim within 14 days if we request it;
- only initiate a Claim where the health service was provided by a Provider and delivered at an authorised operating location;
- ensure patients are provided with a receipt for all Claims processed.

Claims may be rejected or reversed where insufficient or incorrect information is provided, or the Claim is not processed in accordance with our reasonable instructions or the rules of Medicare, DHA or a Health Scheme.

3.11 Claim data

You must ensure that you have all necessary approvals and consents to submit a Claim and that you comply with your obligations under law (including the *Privacy Act 1988* (Cth), *Healthcare Identifiers Act 2010* (Cth), *My Health Records Act 2012* (Cth), *Health Records and Information Privacy Act 2002* (NSW) or other equivalent state-based legislation as applicable).

Any information provided whilst using CommBank Smart Health may be accessed and stored by Whitecoat and us in line with our Commbank Group Privacy Statement available on our website.

We will use and disclose Claim information where permitted or required by law. We will also use and disclose Claim information in connection with making CommBank Smart Health available to you or performing our obligations and exercising our rights under our agreements with Medicare, DHA or directly with a private health insurer (as applicable).

3.12 Whitecoat directory

CommBank Smart Health includes capability for patients to search for practices and Providers using the Whitecoat online directory. You acknowledge and agree that we may disclose your practice trading name and/or registered Provider names, trading address and phone numbers to Whitecoat to publish a business profile on the Whitecoat directory (**www.whitecoat.com.au**). We may licence the use of Whitecoat directory data to health care service providers (including government bodies) for providing their services to their patients. If you wish to have your practice and Provider details removed from the Whitecoat directory, please contact the CommBank Smart Health directory support team via email at **smarthealthsupport@cba.com.au**.

3.13 Claim settlement and payments

3.13.1 Claim payments

Medicare Easyclaim Claims are processed through our arrangements with Medicare. When using Easyclaim, you must follow the instructions set out in the user guide we provide you to process the Claim. Approved Medicare Easyclaim benefits are to be paid directly to your patient through their nominated debit card. For bulk billing Claims, Medicare are responsible for transferring any Medicare benefit payments to you. You must comply with all Medicare rules and regulations when processing Medicare Claims.

Health Scheme and private health insurance Claims and price estimates are processed in accordance with the rules set by the Health Scheme or DHA. When you lodge Health Scheme or private health insurance Claims through CommBank Smart Health, you direct and authorise us to collect your benefit payments on your behalf.

The Bank will pay the approved benefit to Your Account. Where a benefit is paid but then rejected or reversed by a private health insurer or Health Scheme, you authorise Whitecoat and the Bank to debit Your Account for the rejected or reversed amount.

3.13.2 How we pay you

We credit Your Account with the value of all valid Claims, less any refunded or reversed Claims.

If Your Account is with us

We settle all approved Claims on the day following Claim approval.

If Your Account is with another financial institution

We process your approved Claims the day following Claim approval. Crediting to your account will depend on your financial institution's process.

Part 3C: General

3.14 Information

We may share your information with others as set out in this Agreement, our application form and our Privacy Statement available on our website at **https://www.commbank.com.au/support/privacy.html**. 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 or your patients.

We may also get from or give to any person involved in Medicare, any Health Scheme or 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 to conduct any audits.

You acknowledge and agree that we may access your relevant practice and Provider data, such as Transaction and Claims information, for the purposes of providing and supporting the products and/or services. You must make your patients aware that this information may be stored for the purposes of delivering the service.

3.14.1 Sharing information

In addition to our rights under this Agreement, you agree that:

- we can use and disclose any transaction information you provide in connection with performing our obligations and exercising our rights under our agreements with DHA, Medicare, private health insurer, any Health Scheme or Card Scheme;
- we can use and disclose any information in connection with your Facility that we obtain from any third-party, such as transaction information, to provide you with access to the Hub and other services in relation to your Facility;
- we can share your information with third parties as may be required to provide you with the Hub and other services in relation to your Facility;
- we may collect and use technical data and related information, to facilitate the provision of the software updates and any services related to the Facility;
- you can only use or disclose transaction information for the purpose of processing a Transaction in accordance with this Agreement;
- to the extent you have any rights in the transaction information, you grant us a perpetual irrevocable licence to exercise those rights.

3.15 Your Account

You must nominate and maintain an Australian transaction account for the duration of this Agreement ("**Your Account**").

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.

3.16 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 Claim benefit that is paid but then rejected or reversed by a private health insurer or Health Scheme;
- 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.

3.16.1 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 *3.18 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.

3.16.2 When you must compensate us

In some situations we may incur a loss or cost specifically relating to your Facility. You agree to indemnify us against any such loss or cost and must reimburse us on demand.

By way of example, 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 patient;
- if you do not keep your Facility secure, or if your Facility is accessed or used in an unauthorised way;
- 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 Claim or Cardholder data.

However, you will not be required to indemnify us to the extent the loss or cost has been caused by our acts or omissions.

3.16.3 Examples of compensation

Losses and costs 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 terminals or other equipment that are required because the terminals or equipment are damaged as a result of your acts or omissions.

3.17 Our liability for your Facility

We are not liable for any loss you incur as a result of your use of your Facility, other than for our own fraud, negligence or wilful misconduct, including if your Facility is not working or is not available, if you can't process Transactions for any reason or because of any delay in processing, provided that nothing in these terms and conditions is intended to limit any rights you may have at law, where we are not permitted to do so.

If any guarantee, term, condition or warranty is implied or imposed in relation to these terms and conditions under the Australian Consumer Law or any other applicable legislation (a **Non-Excludable Provision**) and we are able to limit your remedy for a breach of the Non-Excludable Provision, then our liability for breach of the Non-Excludable Provision is limited to one or more of the following at our option:

- In the case of goods, the replacement of the goods or the supply of equivalent goods, the repair of the goods, the payment of the cost of replacing the goods or of acquiring equivalent goods, or the payment of the cost of having the goods repaired; or
- In the case of services, the supplying of the services again, or the payment of the cost of having the services supplied again.

3.18 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.

3.19 Statements

If you are a relationship-managed merchant, statements will be sent to you electronically via NetBank or CommBank App where a proprietor or director of your business is registered to use NetBank and/or the CommBank App. Where you are a relationship-managed merchant but don't have NetBank or CommBank App access or opt out of receiving statements via NetBank or the CommBank App and for non-relationship managed accounts, we will send statements and notices to your nominated postal address. It is your responsibility to advise us of any changes to your postal address and email address. If you prefer to receive your merchant statements and notices electronically, please contact us to arrange this.

If you choose to receive merchant statements electronically through CommBiz, merchant statements will be taken to have been issued by us when they are available to "Users" (as defined in the "CommBiz Terms and Conditions") in a manner consistent with those terms and conditions. This may mean that no email notification is provided when the merchant statement is available.

Payment and Claim history is also made available in the Hub.

3.20 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.

3.20.1 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.

3.20.2 Publishing fees

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

3.21 Changing or terminating this Agreement

3.21.1 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);
- a change is required to immediately restore or maintain the security of a system or the Facility, including the prevention of systemic or individual criminal activity, including fraud and scams or to otherwise manage a material and immediate risk.

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.

3.21.2 Suspending your Facility

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

We can also terminate or suspend any part of your Facility in the same way.

We may suspend your Facility without notice if we reasonably consider it necessary to protect our or your interests. If we do so, we will act fairly and reasonably towards you.

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

3.21.3 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).

3.21.4 When we can terminate this Agreement without notice

In some circumstances, we may terminate this Agreement (in full or in part) without providing you with prior notice. When we do so, we will act fairly and reasonably towards you and will try to contact you. Such circumstances are:

- 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 or Claims (e.g. refunds), or allowed fraudulent Transactions or Claims 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;
- your Facility has been operated, used or accessed in a manner that we reasonably consider is unsatisfactory or inconsistent with this Agreement;
- 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 (or any Provider or other person using your Facility) 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;
- we reasonably consider necessary, for example to comply with our financial crimes policies, any laws in Australia or overseas, Card Scheme rules, manage any risk, or for a Claim, if your instructions are not clear;
- we believe on reasonable grounds that you may be (or any Provider or other person using your Facility may be) a person, acting for or conducting business with a person with whom we are not permitted to deal with by law or a regulatory authority
- it is identified that you (or any Provider or other person using your Facility) have used your Facility through any channels or products not approved by us;
- the Medicare, Health Scheme or DHA systems (as applicable) are unavailable or have been suspended by Medicare, a Health Scheme or DHA;
- our agreement with Medicare, private health insurers, DHA, and/or a Health Scheme (as applicable) is terminated, suspended or otherwise not available;
- any of your (or any Provider or other person using your Facility) acts or omissions puts us in breach under our agreement with Medicare, private health insurers, DHA, and/or a Health Scheme (as applicable)
- you have not used your Facility for more than 12 months; or
- you do not provide us with any information we reasonably request from you.

3.21.5 What happens when this Agreement terminates

Us

When this Agreement terminates, we:

- are no longer obliged to acquire Payments on your behalf;
- are no longer obliged to process Claims on your behalf;
- may enter your premises to repossess any unreturned equipment. We will try to give you reasonable notice;
- may retain all or part of any security provided to us for as long as we reasonably require to secure any of your obligations under this Agreement. If you request, and we agree, we may substitute the security for another form of security deemed acceptable by us;
- may debit any chargebacks and 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;
- not process any further Claims through the Facility;
- 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.

3.22 Miscellaneous

3.22.1 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;
- the Hub – by making it available in the Hub or other application used for your Facility;
- newspaper publication – publishing it in local or national media (in which case we will also post the notice on our website).

3.22.2 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.

3.22.3 Banking Code of Practice

The Banking Code of Practice applies to your Facility if you are a small business (as defined in the Code) 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.

3.22.4 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.

3.22.5 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.

3.22.6 Severance

If any term of this Agreement is found to be wholly or partially void or unenforceable for any reason, that term will be severed to the extent that it is void or unenforceable and the rest of this Agreement will continue to apply.

3.22.7 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 using the Facility.

3.22.8 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 Card and Claim processing capabilities, we also offer:

- App Marketplace – enables you to perform additional functions through our compatible terminals and apps which you can download;
- Least cost routing (also referred to as merchant choice routing) – enables you to select your preferred network for routing Multi Network Contactless Debit Card Transactions where you have an eligible terminal and pricing plan;
- Practice management software integration – enables you to integrate you CommBank Smart Health terminal with your compatible practice management software.

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 prevail to the extent of the inconsistency. We may also make additional products and features available in the Hub. Separate or additional terms and conditions may apply to these additional products and features available in the Hub. You may view and apply for these products and services within the Hub.

4.2 App Marketplace

If you use the App Marketplace, these features form part of your Facility. Our liability for your Facility is limited in the manner set out in clause 3.18 of this Agreement.

4.2.1 Use of apps

Smart Health terminals are multifunctional terminals that allow you to accept Payments, download apps and create and upload your own apps. Our App Marketplace hosts apps developed by us and by third-party developers.

We are not responsible for, and will have no liability for, the performance or availability of apps created and provided by a third-party developer in the App Marketplace.

If you download an app from App Marketplace, you will need to accept the terms and conditions for that app before you use it. We will debit Your Account for fees payable under the terms and conditions for each app you purchase through App Marketplace, 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. We may need to provide those developers with information concerning your download and usage of the developers' app in connection with the payment and calculation of those fees and by using those apps, you authorise us to share such information.

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 Instruction manual

We issue instructions or manuals, which you must follow, explaining how to access the App Marketplace and use your Smart Health 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 which can be found at **www.commbank.com.au/smarthealth**.

4.2.3 Software

We may from time to time update the software needed to use your Smart Health terminal or the App Marketplace (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.

4.2.4 Telecommunication costs

You are responsible for any charges imposed by your telecommunications provider for accessing the App Marketplace to use your Smart Health terminal with your Compatible Mobile Smartphone or Tablet Device, including call costs and data costs associated with downloading software.

4.2.5 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 patients. 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 patients or members of the public. You must comply with Australian privacy laws. You are responsible for the security of apps downloaded to your terminal.

4.2.6 Trademarks and copyright

You acknowledge and agree that the CommBank, 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 or processing a Claim through your Smart Health terminal. You may only use any marketing material solely to promote your ability to accept Payments and process Claims through your Smart Health 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.

4.2.7 Communication or service failure

We do not warrant that the apps created by a third-party developer on the App Marketplace or the Hub will be fault free or that any problem with the App Marketplace or the Hub can be solved immediately or quickly. You acknowledge that those services may rely on factors outside our control. We do not warrant continuous, uninterrupted access to those services. 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 App Marketplace) to your 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.

4.3 Least cost routing (LCR)

Least cost routing (LCR) (also referred to as merchant choice routing or MCR) allows you to select which network brand to process a contactless, Multi Network Debit Card Transaction (i.e. a Transaction using a card branded by both eftpos and Mastercard or Visa), and/or eCommerce payments using a Multi Network Debit Card, giving you control to select the cheapest route.

eCommerce payments are processed through the debit payment network(s) enabled on your customer's card. Where the customer's card displays two debit payment networks, you may process the payment through either network.

You could select the cheapest network to process the Transactions for each of your eftpos, Mastercard and Visa debit card Transactions where they are contactless or processed in eCommerce and/or set up transaction thresholds where applicable. LCR is an optional feature only available on selected terminals and pricing plans and is being introduced on selected eCommerce Facilities.

Your LCR selection may not work on all Cards or Payments using digital wallets.

If you are approved for and enable LCR:

- you must follow our set-up directions;
- you must understand your pricing associated with Visa, Mastercard and eftpos Card Transactions and set your own eCommerce/contactless Multi Network Debit Card Transaction thresholds for routing where applicable. We cannot advise you which network will be best for you and we cannot guarantee cost savings. For current interchange fees, contact the relevant network or view their website;
- we will not be responsible for any delays in implementing or disabling your LCR selections;
- 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 LCR selection capability and revert to the default network for processing where we reasonably consider it is necessary. For example, in the event that the lowest cost network is unavailable, or where there is a breach of Card Scheme rules. Should this occur, we are not liable to you for any loss or higher interchange costs;
- you will need to factor in any surcharge which you wish to apply as it is not included in your nominated thresholds for routing.

4.4 Practice Management Software Integration

We work with third-party practice management software providers to enable integration with CommBank Smart Health. If you would like to integrate a practice management software with CommBank Smart Health, you must ensure your practice management software is compatible and follow the set up guide we provide. A list of compatible practice management software can be found in the Hub and at www.commbank.com.au/smart-health.

4.5 Claims submitted using Apple devices

We provide the capability to submit select Claims from patients who have their private health insurance credentials stored with Apple for use with the Apple Pay NFC Platform. Where you submit Claims presented by a patient using the Apple Pay NFC Platform, you are granted a personal, non-transferable and non-exclusive right to submit such Claims under our licence agreement with Apple.

Apple assumes no liability related to any changes in performance of the Smart Health terminal, or additional regulatory requirements arising, in whole or in part, from the use of the Apple Pay NFC Platform on the Smart Health terminal. Apple will not be liable for any loss or damages arising out of or relating to your use or inability to use the Apple Pay NFC Platform on the Smart Health terminal. All Apple intellectual property rights relating to or residing in the Apple Pay NFC Platform shall remain with Apple and you must not use the Apple Pay NFC Platform in connection with any product that is not an Apple-branded product.

You acknowledge and agree that your use of the Apple Pay NFC Platform does not give you the right to develop, market or distribute any software program or pass designed for use with an Apple-branded product unless you have a separate licence to secure such rights from Apple directly at **https://developer.apple.com/**.

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.

Apple
Apple Inc. and/or its affiliated companies.

Apple Pay NFC Platform
The portion of Apple Pay that enables end-users to use features and functionality, and to access other related services using Apple products designated by Apple.

AusPayNet
Self-regulatory body and industry association for payments.

Bank, we, us *and* our
Commonwealth Bank of Australia ABN 48 123 123 124.

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

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.

Card-not-present
This includes Transactions by mail order or phone or via a supported mobile application.

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

Claim
Any claim for benefit from Medicare, a private health insurer or a Health Scheme processed using CommBank Smart Health.

Compatible Mobile Smartphone or Tablet Device
The compatible internet connected device (for example a compatible mobile phone or tablet device) you use to link to your Smart Health terminal.

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").

DHA
Dedalus Health Australia Pty Limited (formerly DXC Technology Australia Pty Limited). DHA distribute the "Healthpoint" product, which enables you to submit private health insurance claims to insurers in the DHA network. A full list of supported health funds with CommBank Smart Health and Healthpoint is available at **www.commbank.com.au/smart-health**

Facility
Your CommBank Smart Health facility and includes using terminals, mobile solutions, online portals, online websites and optional products or features.

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

Health Scheme
An entity (other than Medicare or a private health insurer) which pays for or contributes a payment towards a Claim.

Hub
The CommBank Smart Health Hub referred to in clause 2.2 where you can view, set up, and manage your CommBank Smart Health facility and request additional products and features.

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

Medicare
Medicare Australia as established under the *Human Services (Medicare) Act. 1973*.

Multi Network Debit Card
A payment card displaying two debit payment networks – eftpos (eftpos Payments Australia Limited) and another card network (for example, Mastercard debit, Visa debit).

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

Provider
A provider of products or services approved by Medicare, private health insurers and/or Health Schemes for whom you have established a profile on the Hub to use your Facility for the purposes of having claims for benefits processed through your Facility.

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

Store and Forward
A mode on a terminal that allows you to continue to process Transactions under your floor limit, as per normal, even in instances where the terminal cannot connect to the Bank.

Transaction

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

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, Hub users or Providers 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 3.15 Your Account.