

Business Banking Online and Payment Services.

Terms and Conditions.

Effective date: 10 November 2023

These Business Banking Online and *Payment Services* Terms and Conditions ("Terms and Conditions") are part of a Product Disclosure Statement ("PDS") for BankSA Business Banking Online.

The Corporations Act does not require us to give customers a PDS for *Debit Direct Entry*.

However, for ease of reference, we use the term "Product Disclosure Statement" or "PDS" to refer to the terms and conditions that relate to *Debit Direct Entry*.

There are 2 parts to the PDS for Business Banking Online and the Payment Services. This document contains the terms and conditions for Business Banking Online and the Payment Services. It also summarises the features, benefits and risks of Business Banking Online and the Payment Services. The other document that makes up this PDS is our Business Banking Online fees and charges brochure.

Information in this Product Disclosure Statement.

The law requires that the information in this PDS is up-to-date at the time it is given to you, except for any changes which may occur from time to time that are not materially adverse, provided we give you a means of finding out about these changes. You can find out about any changes by calling 13 13 76, 7.30am to 7.30pm, Monday to Saturday. You can also obtain a paper copy of the updated information free of charge by contacting us at any of our branches.

These Terms and Conditions were prepared on 4 October 2023. However, they are intended to be used only for services provided after the effective date shown on the cover of this PDS.

The Terms and Conditions apply to the use of Business Banking Online and the Payment Services by you and any user. The features, benefits, risks and Terms and Conditions are in addition to the terms and conditions that apply to each *account*. Please refer to the PDS for your account for the terms and conditions of that *account*.

The meaning of words printed *like* this and other common key words is explained in Section I.

Please let us know if you did not receive both parts of the PDS at the same time.

The PDS is an important document. Please read the PDS carefully as it will help you to:

- decide whether Business Banking Online and
- the *Payment Services* will meet your needs; and
- compare Business Banking Online and the *Payment Services* to other banking services you may be considering.

The products to which this PDS applies are financial products issued by BankSA – A Division of Westpac Banking Corporation ABN 33 007 457 141 AFSL and Australian credit licence 233714.

You may contact us:

- by calling 13 13 76, 7.30am to 7.30pm, Monday to Saturday;
- by visiting our website: banksa.com.au;
- by calling any of our Branches;
- by writing to us at PO Box 399, Adelaide SA 5001.

Important.

Protect *passwords* and any *authentication device*.

If you or a *user* believe that a user's password or *authentication device* has been compromised, you or they must take immediate action to limit your liability.

Further information about:

- keeping your passwords and any *authentication devices* secure is set out in clauses 3 and 22.1; and
- your liability for unauthorised transactions is set out in clause 6.

Contents

Section A	Features and benefits and significant risks of Business Banking Online and the Payment Services.	5
Section B	Fees and Charges.	14
Section C	Terms and Conditions that apply to Business Banking Online and the Payment Services.	15
Section D	Terms and Conditions that apply to Business Banking Online.	38
Section E	Terms and Conditions that apply to BPAY.	53
Section F	Terms and Conditions that apply to <i>Credit Direct Entry</i>	62
Section G	Terms and Conditions that apply to <i>Debit Direct Entry</i>	64
Section H	Terms and Conditions that apply to RTGS and Overseas Telegraphic Transfer.	71
Section I	Definitions.	75

Section A – Features and benefits and significant risks of **BUSINESS BANKING ONLINE** and the **PAYMENT SERVICES**.

Business Banking Online offers you a fast, easy and convenient way to do banking transactions. The features and benefits of Business Banking Online and the *Payment Services* are:

Benefit	Feature	Description
Convenience	Easily accessible	Business Banking Online is an Internet based banking service that can be accessed through compatible devices with Internet access. Not all functionality may be available when accessing <i>Business Banking Online</i> through some devices or at some screen resolutions.
	You define transaction limits	To provide the greatest flexibility, there are no system established transaction limits. Transaction limits are established and maintained by the appointed <i>Company Administrator(s)</i> on a company/client or <i>Authorize</i> user basis or both.
	Real time account information	At a glance, you can view all your linked <i>account</i> balances and transactions. This information is up to the minute, and will include ATM, EFTPOS and real time transfers (including Osko® payments, Basic Single Credit Transfers) conducted on your <i>accounts</i> today.
	Transaction history	You are able to view transactions on your linked <i>accounts</i> .

Benefit	Feature	Description
Convenience	Export transaction history	You are able to export your transaction information into your financial management system. If you have exported your transactions throughout the year, you will be able to see the full year's transactions at a glance.
	Compatibility with financial packages	Business Banking Online allows for customised formatting of <i>account</i> transaction information to allow you to export information to many accounting systems.
	Scheduled payments	You are able to set up periodical transfers helping you to make your payments on time, every time.
	International payment services	You are able to transfer funds overseas via telegraphic transfer, through Business Banking Online. To use these services, you must have selected 'yes' to the telegraphic transfer option when applying for Business Banking Online. A fee is payable for telegraphic transfer payments. Please refer to the Business Banking Online fees and charges brochure.
	Real Time Gross Settlement (RTGS) payments	Allows you to transfer funds to any Australian bank account on a 'real time basis', i.e funds will arrive in the receiving account on the same day (depending on the recipient institution's capabilities). For example, you can transfer proceeds of property settlements on the day of settlement. A fee is payable for RTGS payments. Please refer to the Business Banking Online fees and charges brochure.
	Process Credit Direct Entry files	You can pay creditors, employees or other third parties by transferring funds to any bank account in Australia with a single file, resulting in a single debit to your <i>account</i> .

Benefit	Feature	Description
Convenience	Osko Payment	Allows you to receive funds from any Australian bank account (depending on the payer's Financial Institution) in near real time using the Osko Payment service.
	Process <i>Debit Direct Entry</i> files	Obtain direct payments from debtors, employees or other third parties in accordance with the authorities they provide to you, by transferring funds from any bank account in Australia with a single file, resulting in a single credit to your <i>account</i> . Note: strict conditions apply to the use of <i>Debit Direct Entry</i> and if you use <i>Debit Direct Entry</i> you may be liable for any loss arising from its misuse (refer to Section G in this PDS for details).
	<i>Direct Entry</i>	To create payrolls and other <i>Direct Entry</i> files you can create and save payroll or <i>Entry</i> files for later use. A fee is payable for <i>Direct Entry</i> payments. Please refer to the Business Banking Online fees and charges.
	Import <i>Direct Entry</i> files	You are able to import <i>Direct Entry</i> files created within your financial management package.
	Create <i>Direct Entry</i> files from payee accounts	You are able to register <i>payee accounts</i> that can easily be created into a <i>Direct Entry</i> file by clicking on the required payees.
<i>Direct Entry</i> files	You are able to create and import <i>Direct Entry</i> files.	

Benefit	Feature	Description
Convenience	Foreign exchange rates	You can view current foreign exchange rates.
	Sub-accounting	Allows you to divide an <i>account</i> into segments for your internal accounting purposes. See clause 24 for further details.
	Telegraphic transfer templates	Allows you to save telegraphic transfer templates.
	Foreign currency accounts	The functions available to foreign currency <i>accounts</i> include transaction history and <i>account</i> details. You can also complete overseas telegraphic transfers, transfers between foreign currency <i>accounts</i> with the same foreign currency as well as transfers between foreign currency accounts and certain Australian dollar <i>accounts</i> .
	View export/import transactions	You can view any outstanding export and import transactions.
	Corporate Solution	If you use Corporate Solution in connection with Business Banking Online, you will be able to receive electronic records of transactions on your linked <i>accounts</i> in the form of statement files.

Benefit	Feature	Description
Security	Password setting	You are able to change and reset all access <i>passwords</i> at anytime to preserve the security of Business Banking Online.
	Authentication Device	An <i>authentication device</i> is a personal authentication device issued to a user to assist in validating transactions or changes (including administrative) that require authority in Business Banking Online. Each <i>authentication device</i> will have its own operating requirements. This functionality allows another level of security for Business Banking Online, ensuring that only users who are authorised to do so can complete transactions or make changes on the system. Transactions cannot be submitted to us for processing without meeting our security requirements.
Control	Optional dual administration	To ensure a higher level of control, you can request administration functions requiring two company Administrators to authorise any variations to a user or company set up.
	Dual authorisation of transactions allowed	You are able to set the operating authority for your <i>accounts</i> as one or two to authorise a transaction.
	Maintain Accounts List	Allows you to choose which of your BBO registered <i>accounts</i> are displayed on your desktop. This facility is similar to a favourites function.

Benefit	Feature	Description
Control	Link personal accounts	You are able to view your personal account information within Business Banking Online if you are a <i>principal</i> .
Support	Working Hours support line	For support on any Business Banking Online issues, you can contact our support centre on 1300 554 004, or speak with your relationship manager. The support centre is available between 7.30am–7.30pm, Monday to Friday.
BPAY® payments	Make bill payments online	The <i>BPAY scheme</i> is a facility that allows you to make electronic payments by requesting us to debit an amount from your account to pay organisations who agree that you can make payments to them through the <i>BPAY scheme</i> .

The significant risk of Business Banking Online and the Payment Services are:

Functionality	Description of Tasks
Client systems	<p>A change in your system may make Business Banking Online inaccessible. Different firewall/proxy configurations may interfere with access. Assistance and support on all Business Banking Online issues is available by contacting our support centre. The contact details for the support centre are set out in the above table under "Support".</p>
Mistaken, unauthorised or fraudulent transaction	<p>It is possible for mistaken, unauthorised or fraudulent payments to be made. For example:</p> <ul style="list-style-type: none">(a) you should take care to ensure that you correctly identify accounts that you want users to be able to access. If not, there is a risk that confusion between accounts may lead to an error in which account is debited;(b) the same debt may be paid more than once; and(c) as Business Banking Online can be operated by more than one person, there is a risk that daily limits may not be enforced. <p>Unauthorised transactions can also occur on your account because of computer or human error or fraud.</p> <p>See clause 3 for information about security and clause 6 for information about liability for unauthorised transactions.</p>
Security	<p>Here is a risk that system failure may permit unauthorised logins. Please see clause 3 for information about security and clause 6 for information about loss caused by the failure of our electronic equipment.</p> <p>If your <i>password</i> and any <i>authentication devices</i> are lost, stolen or compromised, the security of Business Banking Online may be affected. Please see clause 2.2 for further information about your obligations to keep your <i>passwords</i> and <i>authentication devices</i> secure and clause 6 for information about your liability if <i>passwords</i> or <i>authentication devices</i> are lost, stolen or compromised.</p>

Functionality Description of Tasks

Data export formats/ Telegraphic transfer templates/ Direct entry templates

There is a risk that, if the information required for a data export format, telegraphic transfer template or *Direct Entry* template is not provided in the specific format required, the data export format, telegraphic transfer template or *Direct Entry* template might be rejected or produce a mistaken payment.

Third party access

There is a risk that an error by you, a user or by us will permit greater or lesser access to third parties than intended. See clause 28 for information about third party access.

Security

You should check whether your local PC and/or browser stores sensitive information. Again, if a person is able to retrieve the stored sensitive information then your *accounts* can be accessed.
A weak *password* can be easily guessed. Please see clause 3 for more information about protecting your password.
Authentication devices can be lost or stolen. Please see clause 6.6 for further information about your liability for unauthorised transactions if an *authentication device* is lost or stolen.

Functionality Description of Tasks

BPAY payments

There is a risk of mistaken, fraudulent or unauthorised transactions occurring on your *account* because of computer or human error or fraud. Please see clause 37 for information about when you will be liable for unauthorised transactions.

There is a risk that payments will not be received on time due to systems or telecommunications link unavailability, scheduled outage, equipment failure or other reasons. Please see clause 6 for information about loss caused by the failure of *electronic equipment*.

Credit Direct Entry

There is a risk that payments will not be received on time using *Credit Direct Entry* due to systems or telecommunications link unavailability, scheduled outage, equipment failure or other reasons. Please see clause 6 for information about loss caused by the failure of *electronic equipment*.

If your password and any *authentication device* is lost, stolen or compromised, the security of Business Banking Online may be compromised. Please see clause 22 for further information about your obligations to keep your passwords and *authentication devices* secure and clause 6 for information about your liability if passwords or *authentication devices* are lost, stolen or compromised.

Section B – Fees and Charges.

1. Important Note.

You must pay our fees and charges for using Business Banking Online and the *Payment Services* as set out in our Business Banking Online fees and charges brochure or as otherwise notified to you. Information on current standard fees and charges is also available on request. We may introduce new fees and charges, or change the existing fees and charges, from time to time. If we do so, we will give you notice in accordance with clause 2 of Section C.

You can obtain a copy of the Business Banking Online fees and charges brochure by contacting us or by calling the General Customer Enquiries phone number listed on the outside of the back cover of these terms and conditions, or by printing the brochure from our website when you access Business Banking Online.

We may debit fees and charges to the *account* that is nominated by you in your application for Business Banking Online to be the billing *account*, or the billing *account* you chose whilst processing a *chargeable financial transaction* using Business Banking Online.

Please be aware that if you have insufficient funds in your nominated billing *account*, it may become overdrawn when fees and charges are debited and further fees and charges relating to the overdraw may apply. If you do not nominate a billing *account*, we may contact you to arrange for the fees and charges to be paid in another manner.

If you close the billing *account* you must nominate another billing *account* to continue using Business Banking Online.

Section C – Terms and Conditions that apply to **BUSINESS BANKING ONLINE** and the **PAYMENT SERVICES**.

1 About the PDS.

- 1.1 The PDS sets out the terms and conditions that govern:
 - a. Business Banking Online;
 - b. BPAY;
 - c. *Credit Direct Entry*;
 - d. *Debit Direct Entry*; and
 - e. *RTGS* and overseas telegraphic transfers.
- 1.2 You should read carefully the PDS and any other terms and conditions we give you which we advise you apply to Business Banking Online, BPAY, *Credit Direct Entry*, *Debit Direct Entry*, *Osko*, *Basic Single Credit Transfer* or *RTGS* and overseas telegraphic transfers.
- 1.3 We have not taken into account labour standards or environmental, social or ethical considerations for the purpose of selecting or retaining the *Payment Services* in relation to *accounts*.
- 1.4 We will act fairly and reasonably in accordance with our legitimate business interests in exercising our rights and discretions under these terms and conditions.

2 Changes to the PDS.

- 2.1 We may vary the PDS at any time. In doing so we must comply with any applicable law.
- 2.2 We notify you of:
- changes to anything in the PDS; and
 - any event affecting any of the matters specified in the PDS, in the way set out in clause 2.3.
- 2.3 The following table sets out when and how we notify you about certain changes or events:

Type of change or event	Notification we will give you
A If we: (a) introduce a new fee or charge; or (b) increase any fee or charge; or (c) in relation to an <i>EFT transaction</i> : (i) impose or increase charges for the issue or replacement <i>Code</i> or <i>authentication device</i> or performing an <i>EFT transaction</i> ; or (ii) increase your liability for losses relating to <i>EFT transactions</i> ; or (iii) vary the daily or periodic transaction limits on <i>EFT transactions</i> , a <i>Payment Service</i> or <i>electronic equipment</i> .	We will give written or electronic notice to you at least 30 days before the change or event affects you.
B If we make any other change that affects the PDS.	We will notify you in the media, in writing or electronically as soon as reasonably possible (which may be before or after the change takes effect) or, if the change is unfavourable, by giving you at least 30 days notice.

- 2.4 We will notify you in one of the following ways:
- in writing. We may write to you directly or notify you in the media depending upon the change; or
 - electronically (where the *Banking Code* and *ePayments Code* permits and if you agree); or

- c. in any other way agreed to by you; or
- d. notifying your agent in any way agreed to by the agent.

2.5 If we give you written notice, you are taken to have received it 3 *banking business days* after we post it by ordinary mail to the mailing address we have last recorded. So that our record of your contact details remains accurate and up to date, you must notify us of any change to your contact details. You can do this in writing or over the telephone if you identify yourself appropriately.

If you change your address, you as the owner are responsible for updating your details within BBO, otherwise you are taken to be notified if we write to the old address.

2.6 If the Government introduces or changes a government charge payable directly or indirectly by you, you agree to receiving notice in the media or in writing. We will notify you reasonably promptly after the government notifies us of the introduction or change (however, we do not have to tell you about the change if the government publicises the introduction or change).

2.7 We need not give you any advance notice if a change has to be made because of an immediate need to maintain or restore the security of Business Banking Online or any of our other systems or *Payment Services*. We can give you a shorter notice period (or no notice) where it's reasonable for us to manage a material and immediate risk.

2.8 If any other information about Business Banking Online or BPAY is made available, it may be accessed by calling **1300 554 004**, between 7.30am–7.30pm, Monday to Friday or by visiting our website **banksa.com.au**

2.9 Where the ePayments Code and the *Banking Code* permit and if you agree, we may use electronic means to communicate with you.

For example, sending you electronic statements, written notices or other communications about our products and services.

3 Security.

- 3.1 For your own security against loss, passwords, any *authentication devices* and any other security devices should be protected. If you or a user believe that a *user's password, authentication device* or any other security device has been compromised, you or they must take immediate action to limit your liability. Further information about:
- a. keeping *passwords, any authentication devices* or any other security device secure is set out in clause 22; and
 - b. your liability for unauthorised transactions is set out in clause 6.
- 3.2 Your obligations – You must:
- a. not record your *password or authentication device* details on the computer or telephone that you use to access Business Banking Online or BPAY;
 - b. not record your *password or authentication device* details on any item that identifies your Business Banking Online access details or on any article normally carried with any such item and which is liable to loss or theft with that item;
 - c. not permit any other person to use your *password or authentication device* details;
 - d. not disclose your *password or authentication device* details or make them available to any other person (including a family member, a friend or one of our staff);
 - e. use care to prevent anyone else seeing your password or *authentication device* details being entered into any *electronic equipment*.
 - f. comply with any instruction, direction or notice given to you by us through *Business Banking Online* or otherwise concerning managing your online security. Failure to do so may result in restriction or suspension of your use of *Business Banking Online* without notice.

Can you record a memory aid for your *password* or *authentication device* details?

3.3 If you require a memory aid to recall your *password* or *authentication device* details, you may make such a record provided the record is reasonably disguised.

However, we do not consider that the following examples provide a reasonable disguise, and you agree:

- a. not to record your disguised *password* or *authentication device* details on any item that identifies your Business Banking Online access details;
- b. not to record your disguised *password* or *authentication device* details on the computer or telephone that you use to access Business Banking Online;
- c. not to disguise your *password* or *authentication device* details by reversing the number sequence;
- d. not to describe your disguised record as a "Business Banking Online *password*" or "Business Banking Online *authentication device*" or similar;
- e. not to disguise your *password* or *authentication device* details using alphabetical characters or numbers:
e.g. A=1, B=2, C=3, etc;
- f. not to select or disguise your *password* or *authentication device* details using any of the following combinations (or parts of them):
 - i. dates of birth
 - ii. personal telephone numbers
 - iii. car registration numbers
 - iv. family members' names
 - v. government issued identification numbers
 - vi. licence numbers; and

- g. not to store your *password* or *authentication device* details in any low security electronic device of any kind, such as (but not limited to):
 - i. calculators
 - ii. personal computers
 - iii. electronic organisers
 - iv. mobile phones.

3.4 There may be other forms of disguise which will be unsuitable because of the ease of another person discerning your *password* or *authentication device* details.

You must exercise extreme care if you decide to record a memory aid for your *password* or *authentication device* details.

Please note: Liability for losses, including where liability is limited, resulting from unauthorised *EFT transactions* is determined under the relevant provisions of the ePayments Code, where that Code applies, despite the obligations set out at clauses 3.2 to 3.4 above.

If your password or authentication device details are revealed or you suspect unauthorised transactions.

3.5 You must tell us as soon as possible if you suspect that your *password* or *authentication device* details are known to someone else or you suspect any unauthorised use of these details or that unauthorised transactions have been made. You may notify us by telephoning us on 1300 554 004 between 7.30am–7.30pm, Monday to Friday.

3.6 If you do not notify us you may be liable for unauthorised use – see clause 6.

3.7 You will need to give us all relevant information you may have, so that we can suspend Internet access to your *accounts*. You must confirm in writing any notice you give us by telephone within 7 days.

3.8 If you are unable to report to us because our facilities are unavailable you must tell us within a reasonable time after our facilities become available again.

4 Transacting on accounts.

4.1 Authority.

If there is more than one of you, each *client* authorises the others to use Business Banking Online in the manner contemplated in these terms and conditions in respect of any of the *accounts*, whether or not that *account* is held by that client.

4.2 Stopping a transaction.

- a. To stop or alter a Business Banking Online transaction, you must contact us as soon as possible and give full details so that we can locate the transaction and take action. In some instances, we will not be able to stop or alter a transaction after you have instructed us to make the transaction.

For example, refer to clause 36 in this context as it applies to *BPAY payments*.

- b. We are not liable to you if you request that a transaction be stopped or altered but we have already debited the amount to your *account* or we are liable to pay the amount of the transaction to another person, unless we are liable to you under a statute, the *Banking Code* or the *ePayments Code*.
- c. We are not liable for any loss or costs as a result of any delay or error in transit or transmission of any direction you give us by Business Banking Online or relating to a *BPAY* transaction, except to the extent that it is caused by our fraud, negligence, wilful misconduct or any breach of a legal obligation we have to you including under the *ePayments Code* and any *Banking Code* obligation where we have to act fairly and/or reasonably.

4.3 Availability.

We will make reasonable efforts to:

- a. ensure that Business Banking Online, *BPAY*, *Debit Direct Entry* and *Credit Direct Entry* are available during the hours specified by us from time to time;

- b. you may access Business Banking Online through compatible devices. Not all functionality may be available when accessing Business Banking Online through some devices or at some screen resolutions; and
- c. ensure that information we make available to you through Business Banking Online is correct.

4.4 Transaction Limits.

Transaction limits are established and maintained by the *company administrator* on a *client* and/or *user* basis.

In addition to any limit established by the company administrator we may impose additional limits for transactions of specific types or between specific accounts. You may obtain further information about these limits by contacting us or visiting banksa.com.au/bbo

4.5 Instructions and directions.

You must comply with any instruction, direction or notice given to you by us through Business Banking Online or otherwise.

Failure to do so may increase your liability (see clause 6) or we may, acting reasonably, restrict or suspend your use of *Business Banking Online* without notice.

4.6 Payments made in error.

Where we reasonably believe that a payment made to your account may be a payment made in error, we may, without your consent, deduct from your account an amount no greater than the payment amount made in error and return it to the understood source of origin or as required by law, code or regulation. A payment made in error includes a fraudulent payment, a payment as a result of a scam affecting you or another person, an over payment, a duplicate payment or a payment error made by us. We will take steps, acting reasonably, to contact you in relation to a payment made in error where we consider it relates to a scam or fraud, unless we are unable.

See the 'Mistaken internet payments' section for more information.

5 Problems and Complaints.

- 5.1 If you have a problem or complaint or believe an error has been made, please notify us by calling 1300 554 004 between 7.30am–7.30pm, Monday to Friday.
- 5.2 To assist us in resolving your problem or complaint, you should:
- a. report it promptly;
 - b. state clearly the nature of the problem or your particular grievance; and
 - c. have available all documents and background information.
- 5.3 If the matter is not resolved to your immediate satisfaction, you can follow the dispute procedures set out in this clause 5.
- 5.4 You can lodge a complaint at any of our branches or by telephone or in writing to the Senior Manager, Customer Relations at our head office in Sydney.
- The relevant contact details are set out at the end of these terms and conditions.
- 5.5 If we do not immediately resolve your complaint to your satisfaction, we will advise you in writing of our procedures for investigating and handling complaints. We will notify you of the name and contact number of the person who is investigating your complaint.
- 5.6 If the ePayments Code applies to a transaction initiated by an instruction through Business Banking Online, then the following conditions apply in relation to that transaction:
- a. If it is unclear whether you have contributed to the loss that is the subject of any complaint you make to us, we will consider all reasonable evidence, including all reasonable explanations for the transaction occurring. The fact that your account has been accessed with the correct

password and *authentication device*, whilst significant, is not conclusive evidence that you have contributed to the loss.

- b. We do not require you to raise complaints or disputes in relation to the processing of *EFT transactions* with any other party to the shared EFT system (such as a retailer or a merchant). Where we have been notified by another party to the shared EFT system, or from the view, that a transaction has been debited or credited incorrectly to your EFT account, we will investigate.

We will make any corrections to your *EFT account* we consider appropriate in the circumstances. Any correction is included in your next statement. We will also notify you as soon as practicable after reversing an incorrect credit.

- c. If you request, we will provide you with further details about any correction shown on your *account statement*.
- d. We will respond to you about any complaint (normally within 21 days). If we need more time or details to complete our investigation, we will advise you in writing. Unless there are exceptional circumstances, we will complete our investigation within 45 days.
- e. Where an investigation continues beyond 45 days, we will inform you of the reasons for the delay, give you monthly updates on the progress of the investigation and a date when a decision can reasonably be expected. We do not do this if we have requested a response from you and we are waiting for that response.
- f. If you refer the dispute to us in writing or you request a written response from us, or if the dispute relates to an *EFT transaction*, we will advise you in writing of the outcome. If the dispute relates to an *EFT transaction*, or otherwise is not resolved to your satisfaction, we will advise you of the reasons in writing and of any further action you can take to resolve the dispute.

- g. The next available step is a free, independent external dispute resolution scheme (as long as the external dispute resolution scheme has the power to deal with your dispute). The contact details of external dispute resolution scheme are listed on the back cover of these Terms and Conditions.
 - h. If, in relation to an *EFT transaction*, we fail to observe these Terms and Conditions when we allocate liability or when conducting our complaint investigation and dispute resolution procedures, and as a result there is unreasonable delay or the outcome of our investigation is prejudiced, we accept full liability for the amount that is the subject of the complaint.
- 5.7 If you have a complaint which relates to the *BPAY scheme* and you are not an individual, then we will resolve your dispute in accordance with the dispute resolution procedures established under the *BPAY scheme*.

6 Liability.

Our liability.

- 6.1 Not Used.
- 6.2 Where any relevant law or code implies into these terms and conditions (or any transaction initiated by any instructions through Business Banking Online, BPAY or RGTS) any term, and the law or code voids or prohibits any term or condition in this agreement that seeks to exclude, restrict or modify that term, then the term is taken to be included in these Terms and Conditions.
- Our liability for breach of such a term, if permitted and not prohibited by law or code, is limited to one of the following remedies:
- a. the supply of Business Banking Online, BPAY, *Debit Direct Entry* or *Credit Direct Entry* (or Corporate Solution) again; or

- b. the payment of the cost of having Business Banking Online, BPAY, *Debit Direct Entry* or *Credit Direct Entry* (or Corporate Solution) supplied again.
- 6.3 Subject to clauses 6.2 and 6.11, we exclude all liability to you for consequential loss or costs except to the extent caused by our fraud, negligence, wilful misconduct or any breach of a legal obligation we have to you arising from or connected in any way to this agreement.

Your liability for unauthorised transactions.

- 6.4 If the ePayments Code applies to a transaction initiated by an instruction through Business Banking Online, *Debit Direct Entry* or *Credit Direct Entry*, you are not liable for an unauthorised transaction if it is clear that you did not contribute to the losses resulting from those transactions.

Otherwise, if the ePayments Code applies, your liability will normally be limited to:

- a. \$150; or
 - b. the balance of the *EFT account* on which the unauthorised transactions were made, including any agreed line of credit, to which you have access by Business Banking Online; or
 - c. the actual loss incurred before you notify us under clause 22.1(j) (excluding that portion of the loss incurred on any one day which exceeds any applicable daily transaction limit), whichever is the smallest amount, although in some circumstances you may be liable for a greater amount for unauthorised Business Banking Online, *Debit Direct Entry* or *Credit Direct Entry* transactions. Please refer to clauses 6.7 to 6.9 and 55 for details of those circumstances.
- 6.5 However, you are not liable for losses caused by:
- a. the fraudulent or negligent conduct of our staff or agents or of companies involved in networking arrangements or of merchants who are linked to the electronic funds transfer system or of their agents or employees; or

- b. any *authentication device*, *Identifier* or *Code* that is forged, faulty, expired or cancelled; or
- c. unauthorised transactions that can be made using an *Identifier* without an *authentication device* or *Code*; or;
- d. unauthorised transactions that can be made using an *authentication device* and not a *Code*, provided you did not unreasonably delay in reporting the loss or theft of the *authentication device*.
- e. unauthorised transactions through Business Banking Online, *Debit Direct Entry* or *Credit Direct Entry* which occur after you have given us notice as required by clause 22.1(j);
- f. unauthorised transactions through Business Banking Online, *Debit Direct Entry* or *Credit Direct Entry* before any user receives their password and *authentication device*; or
- g. the same transaction being incorrectly debited more than once to the same *account*.

When you will be liable.

- 6.6 You will be liable for losses resulting from transactions which are carried out by you, a person authorised by you or another person with your knowledge and consent.
- 6.7 If the ePayments Code applies to a transaction initiated by an instruction through Business Banking Online, *Debit Direct Entry* or *Credit Direct Entry* and you or a user have contributed to the unauthorised use on the *account* because you or a *user*:
 - a. engaged in fraud; or
 - b. failed to comply with any instruction, direction or notice given by us; or
 - c. voluntarily disclosed a *user's* password or *authentication device* to anyone, including a family member or friend or allowed anyone to use a *user's authentication device*; or
 - d. where an *authentication device* is also needed to perform a transaction, kept a record of a *user's password* or *authentication device* (without

making any reasonable attempt to protect the security of it) with any article carried with the *authentication device* or in a way that it was liable to loss or theft simultaneously with that *authentication device*; or

- e. selected a *password* which represents a *user's* birth date or an alphabetical code which is recognisable as part of a *user's* name immediately after the user is specifically instructed not to select such a password and warned of the consequences of doing so; or
- f. acted with extreme carelessness in failing to protect the security of a *user's password* or *authentication device*, your liability will not exceed the smallest of:
 - i. the actual loss incurred up to the time we are notified that the security of a *user's password* or *authentication device* has been breached or notice of the existence of unauthorised transactions; or
 - ii. the funds available in the *EFT account* including any agreed line of credit; or
 - iii. the total amount you would have been allowed to withdraw on the days that unauthorised use occurs.

If more than one *Code* is required to perform a transaction and we prove that you breached the security requirements for one or more, but not all, of those *Codes*, you will be liable under this clause only if we also prove, on the balance of probability, that the breach of the security requirements was more than 50% responsible for the losses.

- 6.8 If the ePayments Code applies to a transaction initiated by an instruction through Business Banking Online, *Debit Direct Entry* or *Credit Direct Entry* and you have contributed to an unauthorised transaction on the *account* because you or a user unreasonably delayed in notifying us that a *user's password* or *authentication device* has become known to someone else, you will be liable for any losses directly attributed to that delay that were

incurred before notification. Your liability for these losses will not exceed the smallest of:

- a. the actual loss which could have been prevented from occurring in the period between when you or a *user* became aware (or should reasonably have become aware) of the events described above and the time we were actually notified; or
- b. the funds available in the *EFT account* including any agreed line of credit; or
- c. the total amount you would have been allowed to withdraw on the days that unauthorised use occurs.

If the ePayments Code applies to a transaction initiated by an instruction through Business Banking Online, *Debit Direct Entry* or *Credit Direct Entry*, your liability for losses from unauthorised *EFT transactions* will not exceed the amount of the loss that would result after the exercise of any claim or other right we have under the rules of any card scheme against any other party to that card scheme (whether or not that claim or other right is actually exercised).

- 6.9 If you are unable to report to us because our facilities are unavailable and the ePayments Code applies, you are not liable for any unauthorised *EFT transaction* which could have been prevented if you had been able to tell us, provided you tell us within a reasonable time after our facilities become available again.

Malfunctions.

- 6.10 You are not liable for loss caused by the failure of our electronic equipment or Business Banking Online, *BPAY*, *Debit Direct Entry* or *Credit Direct Entry* service to complete a transaction accepted by our *electronic equipment* or Business Banking Online, *BPAY* or *Credit Direct Entry* service in accordance with a *user's* instructions.
- 6.11 Notwithstanding anything else in these terms and conditions, for transactions governed by the ePayments Code, we do not deny your right to claim consequential damages resulting from a

malfunction of a system or equipment provided by a party to a shared electronic payments network that you are entitled to use pursuant to these terms and conditions (such as a merchant or us) except where you or a user should reasonably have been aware that the equipment or system was unavailable for use or malfunctioning, in which case our liability may be limited to the correction of any errors in the account, and the refund of any charges or fees imposed on you as a result.

- 6.12 We correct the loss by making any necessary adjustment to the appropriate *account* (including adjustment of interest or fees as a result of the malfunction).
- 6.13 Please tell us about any service fault or difficulty with our *electronic equipment* by calling 1300 554 004, between 7.30am–7.30pm, Monday to Friday.
- 6.14 You will not be liable under clauses 6.7 and 6.8 for any losses incurred on any BankSA accounts which we had not agreed could be accessed using a *user's password* or *authentication device*. Your liability under clause 6.7 is also subject to us, proving, on the balance of probability, that you contributed to the losses in one or more of the ways described in clause 6.7.

Warranty.

- 6.15 We warrant that we will comply with the ePayments Code, where it applies. If your facility is designed primarily for use by a business and established primarily for business purposes, the ePayments Code will not apply to it.

Processing transactions when *Business Banking Online* is unavailable.

- 6.16 Please contact us on 1300 554 004, between 7.30am – 7.30pm, Monday to Friday for information on processing transactions if Business Banking Online is unavailable.

7 Mistaken internet payments.

7.1 This clause 7 does not apply to BPAY payments. See Section E for information about BPAY payments.

Reporting *mistaken internet payments*.

7.2 You should report *mistaken internet payments* (including mistaken Osko Payments and Basic Single Credit Transfers made by an individual) to us as soon as possible after you become aware of them. You can report *mistaken internet payments* to us by visiting a BankSA branch or by calling 13 13 76 within Australia.

We will give you a notification number or some other form of acknowledgement which you should retain as evidence of the date and time of your report.

If we are satisfied that you have made a mistaken internet payment, we will, as soon as reasonably possible (and by no later than 5 business days of your report), send a request to the receiving institution for the return of the funds.

If the receiving institution subscribes to the Code and they are satisfied that a mistaken internet payment was made, they are required to follow the process for recovering the payment that we described under the section, "Where you receive a mistaken internet payment".

We will acknowledge receipt of your report of a mistaken internet payment, conduct an investigation into that mistaken internet payment, and inform you in writing of the outcome of our investigation within 30 business days of the day on which you made the report.

If you are unhappy with how your report was dealt with, you have a right to complain to us. Information on our complaints procedure is set out in this document. If you are still not satisfied with our response or handling of your complaint, you have the right to complain to the external resolution scheme, the Australian Financial Complaints Authority (AFCA). AFCA's contact details are set out in the "Disputes" section of this document.

Dealing with *mistaken internet payments*.

7.3 *Mistaken internet payments* will be dealt with by us in accordance with the ePayments Code, where that Code applies to the payment or where the payment is an Osko Payment (including payments made to a PayID). Set out at clauses 7.4 to 7.5 is a summary of the processes in that Code.

We may be the sending institution, namely the financial institution whose customer made the payment or the receiving institution, namely the financial institution whose customer received the payment (this customer is the unintended recipient of the payment). We will be the sending institution where the payment is made from your account. We will be the receiving institution where the payment is made to your account.

Where a financial institution other than us is the receiving or sending financial institution, we cannot guarantee that it will follow the processes in the ePayments Code. A financial institution is unlikely to follow these processes if it is not an authorised deposit-taking institution for the purposes of the Banking Act. We are not liable for any loss suffered if it does not follow those processes.

Where the sending institution is not satisfied that a payment is a *mistaken internet payment*, it is not required to take any further action.

Notwithstanding anything set out below, where the unintended recipient of the *mistaken internet payment* is receiving income support payments from Services Australia or the Department of Veterans' Affairs, the receiving institution must recover the funds from that recipient in accordance with the Code of Operation: Recovery of Debts from Customer Nominated Bank Accounts in receipt of Services Australia income support payments or Department of Veterans' Affairs payments.

Where you or another financial institution advises us that you are, or we think you may be, the sender or recipient of a *mistaken internet payment*, you must give us, as soon as reasonably

practicable and within the time we request, any information we reasonably require to enable us to determine whether the payment was a *mistaken internet payment*.

Where sufficient funds are available in the unintended recipient's account.

- 7.4 Where the sending institution is satisfied that the mistaken *internet payment* occurred and there are sufficient credit funds available in the account of the unintended recipient to the value of the *mistaken internet payment*, the process that will apply will depend upon when the report of the *mistaken internet payment* is made:

Where the report is made within 10 business days of the payment:

- a. if the receiving institution is satisfied that a *mistaken internet payment* has occurred, it will return the funds to the sending institution within 5 business days of the request or any reasonably longer period up to a maximum of 10 business days.

Where the report is made between 10 business days and 7 months of the payment:

- a. the receiving institution will investigate the payment and complete the investigation within 10 business days of receiving a request;
- b. if the receiving institution is satisfied that a *mistaken internet payment* has occurred, it will prevent the unintended recipient from withdrawing the funds for a further 10 business days and notify the unintended recipient that they will withdraw the funds if that recipient does not establish they are entitled to the funds within that 10 day period.
- c. if the unintended recipient does not establish they are entitled to the funds within that time, the receiving institution will return the funds to the sending institution within 2 business days of that period (during which time the recipient will be prevented from withdrawing the funds).

Where a report is made after 7 months of payment:

- a. If the receiving institution is satisfied a *mistaken internet payment* occurred, it must seek the consent of the unintended recipient to return the funds.

In each case where the receiving institution is not satisfied that a *mistaken internet payment* has occurred, it may (but is not required to) seek consent of the unintended recipient to return the funds.

Where the funds are returned to the sending institution, it will return the funds to the holder as soon as practicable.

Where sufficient funds are not available.

- 7.5 Where both the sending and receiving institution are satisfied that a *mistaken internet payment* has occurred but there are not sufficient credit funds available in the account of the unintended recipient, the receiving institution will use reasonable endeavours to recover the funds from the unintended recipient.

Where you receive a *mistaken internet payment*.

- 7.6 Where:
 - a. both we and the sending institution are satisfied that a payment made to your account is a *mistaken internet payment*; and
 - b. sufficient credit funds are available in your *account* to the value of that payment; and
 - c. the *mistaken internet payment* is reported 7 months or less after the payment; and
 - d. for *mistaken internet payments* reported between 10 business days and 7 months of the payment, you do not establish that you are entitled to the payment within the relevant 10 business day period referred to in clause 7.4,we will, without your consent, and in accordance with the ePayments Code where applicable deduct from your account an amount equal to that mistaken payment and send that amount to the

financial institution of the payer in accordance with clause 7.4 above.

If there are insufficient funds in your *account*, you must co-operate with us to facilitate payment by you of an amount of the *mistaken internet payment* to the payer.

We can prevent you from withdrawing funds the subject of a *mistaken internet payment* where we are required to do so to meet our obligations under the ePayments Code.

Liability for losses arising from internet payments.

- 7.7 You must ensure that internet payment details are correct. You and your user are solely responsible for providing correct payment details including amount and payee details. We will return to you any funds recovered by us on your behalf from an unintended recipient in respect of a mistaken internet payment but otherwise have no liability to you or your user for any payment made in accordance with details provided by you or your user including *mistaken internet payments*.

8 GST.

- 8.1 We will tell you if any fees we charge are *GST* inclusive.
- 8.2 If there is a situation in which we are required to pay *GST* on a payment you make to us, you agree to increase the amount of the payment to include the *GST* amount.
- 8.3 We will tell you of any additional *GST* amount you must make on a payment.

9 Significant tax implications.

There are no significant tax implications in relation to Business Banking Online, *Credit Direct Entry*, *Debit Direct Entry* or BPAY.

10 Restriction, suspension and termination.

- 10.1 The *primary client* may terminate the agreement constituted by these Terms and Conditions (and Corporate Solution) at any time by notice in writing.
- 10.2 We may terminate the agreement constituted by these Terms and Conditions (and Corporate Solution) at any time by giving 30 days' written notice to the primary client. This notice will be sent to the current address of the *primary client* that we have on file.
- 10.3 Subject to clause 10.1 and 10.2, following termination by either party all access rights will be cancelled by us as soon as practicable.
- 10.4 The termination of the agreement constituted by these Terms and Conditions does not affect rights accrued to either party before the termination.
- 10.5 We may restrict or suspend your use of *Business Banking Online* without prior notice where we believe that there is a risk of fraud or security breach, you have failed to comply with any instruction, direction or notice given by us concerning managing your online security, or where you have not accessed *Business Banking Online* for a period of 6 months or more.

11 Banking Code.

The relevant provisions of the *Banking Code* apply to these Terms and Conditions if you are a *small business* or an individual who is not treated as a business under the *Banking Code*.

12 Governing Law.

These Terms and Conditions are governed by the law in force in the State in which you entered into the agreement constituted by these Terms and Conditions, and you agree to submit to the non-exclusive jurisdiction of the courts of that state for any dispute concerning the agreement constituted by these Terms and Conditions.

12A Appropriate use of our Services.

Your use of Business Banking Online and services we provide must not breach any law of Australia or any other country.

Where it is necessary for us to meet our regulatory and compliance obligations:

- a. you must provide us with the necessary information we reasonably request to meet the obligation;
- b. we will disclose information we hold to regulatory and law enforcement agencies, other financial institutions, third parties and members of the BankSA Group; and
- c. we may delay, block or refuse to provide any of our services.

We will not be liable to you or any other person for any loss or damage of any kind that may be suffered as a result of us properly and reasonably exercising our rights under this clause.

12B Privacy.

You must comply with the *Privacy Act 1988* (Cth) in relation to any personal information you provide to us, including the personal information of another person, in connection with these Terms and Conditions, and if you engage in activities in a jurisdiction other than Australia, you must comply also with the privacy laws in that jurisdiction.

12C External service providers.

We may subcontract any of our rights and obligations to another person in Australia or overseas.

We may disclose or share any information you provide to us with any such person. Details of the countries where the overseas recipients are likely to be located are included in our privacy statement which is available at banksa.com.au/privacy/privacy-statement or by calling 13 13 76.

Section D – Terms and Conditions that apply to Business Banking Online.

13 Agreeing to Business Banking Online terms and conditions.

13.1 Agreement

By completing our application for Business Banking Online, you are taken to offer to enter into an agreement with us on the terms of that application and these Terms and Conditions. We are to be taken to have accepted that offer when we notify the *company administrator* nominated in the application for Business Banking Online signed by you that you have been registered as a user of Business Banking Online. This notice is given by a letter to the *company administrator*.

13.2 Accounts at other financial institutions

Accounts held with other financial institutions cannot be accessed through Business Banking Online to make withdrawals. Only deposits can be made to those *accounts* using Business Banking Online by using the payee payment option.

14 *User's acceptance of terms and conditions.*

Before a *user* first uses Business Banking Online, we require the *user* to agree to be bound by these terms and conditions.

15 *Company administrator's first access of Business Banking Online.*

When you apply to use Business Banking Online, the *primary client* must nominate an individual to be the *company administrator*. When we notify the *company administrator* that your offer to use Business Banking Online is accepted, we provide the *company administrator* with a *user*

identification and *password*. You must ensure that the *company administrator* accesses Business Banking Online and changes their *password* as soon as practicable and in any event within 48 hours of receiving their initial *password* from us.

If the *primary client* nominates more than one *company administrator*, the *primary client* must also advise whether the *company administrators* may act independently, or whether they must act jointly, in giving authorisations under clause 16.1.

16 Company administrator.

16.1 The *company administrator* may authorise any individual, including themselves, aged 18 years or older to be a *user* with authority to carry out one or more of the following functions in connection with any *account*:

No Access.

Prevents access to certain *accounts*.

View.

The right to view all information in Business Banking Online in connection with the *accounts* (except that they cannot initiate or *authorise* payment requests).

Create.

The same as view plus the right to create and import Direct Entry payment files, initiate payment requests and submit payment requests to us after they have been authorised by someone with *authorise* rights. Please refer to the Business Banking Online fees and charges brochure for fees and charges associated with Direct Entry payments.

Authorise.

The same as create plus the right to *authorise* payment requests (including under the *BPAY scheme* – see Section E of this PDS).

Authorise/SAM admin.

The same as *authorise* plus access to Sub-Accounting admin.

Administrator (admin only).

The right to do anything the *company administrator* may do other than view, *create* or *authorise*.

Admin only/SAM admin.

The same as *administrator (admin only)* plus access to Sub-Accounting admin.

Administrator (admin/authorise).

The right to do anything the *company administrator* and *authorise user* may do.

Admin/SAM admin/Authorise.

The same as *administrator (admin/authorise)* plus access to Sub-Accounting admin.

- 16.2 When granting a person access rights to Business Banking Online, the *company administrator* must issue them with a *user* identification and *password*. You and the *company administrator* must ensure that the *user* accesses Business Banking Online and changes their *password* within 48 hours of receiving their initial *password* from the *company administrator*.
- 16.3 When granting a person access rights to Business Banking Online, the *company administrator* must submit to us, in respect of the person, a request to appoint them a *user*.
- 16.4 When granting a person *authorise access*, the *company administrator* must give the person access to *authorise* payment requests either on their own or with another person in accordance with the access advised in the request to appoint them a *user*.
- 16.5 Any *view*, *create*, *authorise* or *administrator* rights given for Business Banking Online relate to Business Banking Online only and any authorities to operate your *accounts* still apply to those *accounts*.

17 Personal accounts.

- 17.1 The only personal *account(s)* that may be accessed through Business Banking Online are those of *principals* or *third party accounts* (see clause 28).
- 17.2 Any costs, fees or charges incurred in relation to the use of a *principal's* personal *account* accessed through Business Banking Online must be met personally by that *principal*. Any such costs, fees or charges may not be debited from any *account* of a *client*. Please refer to the Business Banking Online fees and charges brochure for information about the fees and charges payable.
- 17.3 We provide *access* and *authorise* rights to personal *accounts* in accordance with those rights given in accordance with these terms and conditions irrespective of authorities to operate those *accounts* advised through other channels and even if they are inconsistent.

18 Disclosure.

You *authorise* us to disclose information concerning accounts to each of you (if there is more than one of you) and any person (including *company administrators* and *users*) authorised by you to access an *account*.

If you are a *principal*, this authority permits disclosure about you to the *primary client*, *additional parties*, others of you who are principals, *company administrators* and *users*.

19 Cut-off time.

If a *user* tells us to transact on an account before the time specified below, the transaction will in most cases be treated as having been made on the same day:

Cut-off time: Monday to Friday, 5 days per week, 5.00pm (AEST)

However, a transaction which is a payment may take longer to be credited to the payee if a user tells us to make a payment on a Saturday, Sunday or public holiday or if any other financial institution involved in the transaction does not process the payment as soon as they receive details of it. Details of cut-off times for RTGS and telegraphic transfers can be obtained by contacting BankSA treasury.

You acknowledge that an instruction to us by a user that we receive after the cut-off time will be processed on the next banking business day.

Even where a Osko payment or a Basic Single Credit Transfer results in an account balance and transaction list being updated straight away, that payment may not be included in the balance of the account for other purposes (such as interest, fees or overdrawing calculations) until the next banking business day.

20 *Users.*

- 20.1 We allow *users* to carry out the functions they are allowed to do within the level of access granted to them pursuant to these Terms and Conditions. If there is more than one user you will need to complete an *authentication device* application for each user who is to have *authorise* or *administrator* rights of access. We will issue users who have *authorise* or *administrator* rights with an *authentication device* and require that certain functions be performed only if the *authentication device* is used.
- 20.2 A valid direct entry user identification is required to make each external payment to payee *accounts* within Australia and to make payments to creditors and employees. If you do not have an existing direct entry user identification number, you will need to complete a direct entry user application form.

20.3 We are not to be taken to have any notice of any limitation that you (or *users who have authorise or administrator rights*) impose on *users*. Accordingly, we may allow or process any function or instruction carried out by a *user* if it is within the rights generally granted to *users* of that category pursuant to these Terms and Conditions.

20.4 You acknowledge that an instruction to us by a *user* using Business Banking Online whose access and *user rights* have not been cancelled by you, the user or us constitutes a valid and irrevocable authority to us to follow that instruction.

This includes instructions to make periodic payments or payments in the future even if those payments fall due after an *authentication device* used to *authorise* the payment expires, the user's access or user are cancelled or your right to use Business Banking Online is cancelled.

You should contact us immediately if you require any periodic payments or future scheduled payments to be stopped in these circumstances.

20.5 We may assume that any access and use of Business Banking Online in accordance with our operating requirements has been made by a user. You are responsible to ensure that only an authorised user is accessing and using Business Banking Online.

20.6 A *client or principal* is liable for any use of any of its *accounts* by a user as if the *account* had been used by the *client or principal* (including when a *user* uses their *authentication device*). You should ensure that *users* read and understand these terms and conditions.

20.7 Any one of you, us, or a person who has *administrator (admin only)* or *administrator (admin/authorise)* access may cancel the access rights to Business Banking Online of a *user* at any time. You must ensure that there is always at least one person with *administrator (admin/authorise)* access rights.

- 20.8 *Users* may continue to use Business Banking Online unless their right to do so is cancelled in accordance with these Terms and Conditions or, for functions requiring the use of an *authentication device*, the *authentication device* expires and has not been renewed.
- 20.9 We deny access to Business Banking Online if someone trying to access it enters an incorrect password on three consecutive occasions . If this happens to a user, they should contact their *company administrator*.
- 20.10 The *company administrator* must set a daily transaction limit on Business Banking Online for each *client* and may also set individual transaction limits for *users* with the role of *authorise*.
- 20.11 You agree that we may record, by whatever means, transactions effected through Business Banking Online and that we may use these records to, amongst other things, establish or verify that a particular transaction was effected through the use of a *user's password* or *authentication device*. If the ePayments Code applies to a transaction initiated by an instruction through Business Banking Online, we must do so in accordance with the ePayments Code.

21 Additional parties.

- 21.1 If the *primary client* and us agree that another person may become an additional party for the purpose of these terms and conditions ("*new additional party*"), then the *new additional party* is taken to be a party for the purposes of these terms and conditions. The rights and obligations and the restrictions imposed on the *new additional party* are the same in all respects as if the *new additional party* had agreed to these Terms and Conditions as an additional party from the date on which we agree to the *new additional party* becoming a party to the agreement constituted by these Terms and Conditions.

If an *additional party* wants access to Corporate Solution, they must also sign a Corporate Solution Agreement with us.

21.2 Any *additional party* may at any time provide us with a notice that they no longer want to be a party to the agreement constituted by these Terms and Conditions.

21.3 If any *additional party* gives us an exit notice ("*departing additional party*"), then:

- a. it is no longer obliged to meet any of its obligations to us under the agreement constituted by these Terms and Conditions on and from the date of the exit notice, other than those relating to actual or contingent liabilities existing at the time the *exit notice* is given, indemnities or disclosure of information;
- b. we will cease to accept instructions on any *account* that the *departing additional party* holds; and
- c. you must pay us any fees that have been incurred by the *departing additional party* even if those fees have not been billed at the date of the *exit notice*. Please refer to the Business Banking Online fees and charges brochure.

21.4 The agreement constituted by these Terms and Conditions is a continuing obligation between us and the remaining *clients*. Our rights and the obligations of the remaining *clients* are not affected by the release of the *departing additional party*.

21.5 If the *departing additional party* has any actual or contingent liabilities to us, they must be repaid in full to us on or before the date that the *departing additional party* is released from its obligations under the agreement constituted by these Terms and Conditions in accordance with clause 21.3 (unless we otherwise expressly agree).

22 Obligations of users.

22.1 Users must:

- a. not permit any other person to use their *password, authentication device* or other security device we establish;
- b. not disclose their *password, authentication device* or other security device to any other person (including ensuring, when they are accessing Business Banking Online or using their *authentication device*, that their password is not observed);
- c. take reasonable steps to ensure that their *authentication device* or other security device cannot be used by any other person;
- d. on their first use of the *authentication device*, update their password;
- e. not make a record of their *authentication device* password unless the record is kept securely and separately from any place where the *authentication device* is stored.

For example, they must not keep a record of their *authentication device* password on the media or computer on which their *authentication device* is stored;

- f. not record or store any other *password* anywhere;
- g. not use any *authentication device* we issue to them other than for the purpose of accessing and using Business Banking Online or any other of our Internet services which we have agreed to supply to you and which you have, with our agreement, authorised them to use, and then only in accordance with that authorisation;
- h. destroy, in accordance with our instructions, the *authentication device* if the *authentication device* is no longer used to access Business Banking Online or any other Internet services that they are authorised to access and use with the *authentication device*;

- i. not duplicate the *authentication device* to allow multiple points of access to Business Banking Online or any other Internet services that they are authorised to access and use with the *authentication device*;
- j. contact us immediately by telephoning 1300 554 004, between 7.30am–7.30pm, Monday to Friday if their password becomes known to anyone else, the *authentication device* or the computer used to access Business Banking Online is lost, stolen or fraudulently accessed, or they become aware of or suspect any unauthorised transaction, or error on an account which can be accessed by, use of the *authentication device* or a *password*;
- k. contact us immediately if the authorisation to use the services to which the *authentication device* enables access or use, is revoked or suspended;
- l. tell us about any service fault or difficulty with Business Banking Online by calling 1300 554 004, between 7.30am–7.30pm, Monday to Friday;
- m. Adhere to any software requirements that are necessary to use Business Banking Online, as notified by us. Failure to do so may result in restrictions or suspension from access to Business Banking Online, as per clause 4.5; and
- n. You provide us with the following undertakings and indemnify us against any potential losses arising from any breach by you of such undertakings:
 - you must not use Business Banking Online or any of the services covered under these terms and conditions to initiate, engage in or effect a transaction that may be in breach of Australian law or sanctions (or the law or sanctions of any other country) or that involves a payment to, from or through a Sanctioned Jurisdiction;
 - you will not access or use your Business Banking Online in a Sanctioned Jurisdiction.

In some circumstances, including where we reasonably consider it necessary or appropriate, including to meet our regulatory and compliance obligations (including those relating to anti-money laundering and counter-terrorism financing) or to manage associated risk, we may suspend or terminate your access to Business Banking Online without prior notice.

For example where we reasonably suspect that you are residing in a Sanctioned Jurisdiction. If you are travelling to a Sanctioned Jurisdiction, we may without giving you notice suspend your access to Business Banking Online while you are in that jurisdiction.

- 22.2 If a user is obliged to contact us under this clause 22, they must give us all relevant information they have, so that we can suspend Business Banking Online to the *accounts*. The user must confirm in writing any notice they give us by telephone.

When a user reports the matter they are given a notification number (or other form of acknowledgement). This should be retained as confirmation of the date and time of the *user's* report.

If a *user* is unable to report to us because our facilities are unavailable, the *user* must tell us within a reasonable time after our facilities become available again.

23 Your obligations.

- 23.1 You must:
- a. check the *accounts'* records regularly and carefully, and contact us as soon as you identify any apparent discrepancy;
 - b. ensure that *users* carry out their obligations under clause 22;

- c. comply with all laws and codes of conduct that apply to Business Banking Online and your use of it;
- d. ensure that *users* use Business Banking Online in accordance with any instructions for use that we issue;
- e. take all reasonable steps to protect the security of all your and your user's networks, devices and computers used to access *Business Banking Online*. This includes compliance with any instruction, direction or notice given to you by us through *Business Banking Online* or otherwise concerning managing your online security;
- f. contact us by telephoning 1300 554 004, 7.30am–7.30pm, Monday to Friday if any of the events referred to in clause 22.1 (j) occurs.

23.2 We do not warrant that Business Banking Online will always be available. Accordingly, you must ensure at your own expense that alternative methods of accessing and authorising transactions on the *accounts* are in place to enable you to use the *accounts* if Business Banking Online is unavailable.

23.3 Clause 22.2 applies equally to you in respect of your obligation to contact us under this clause 23. References in clause 22.2 to a "user" are taken to be references to "you" for the purpose of this clause 23.3.

Please note: Liability for losses, including where liability is limited, resulting from unauthorised *EFT transactions* is determined under the relevant provisions of the ePayments Code, where that code applies, despite the obligations set out at clauses 22 and 23.

24 Sub-accounting.

24.1 This clause 24 applies if we agree to provide you with sub-accounting functionality.

24.2 Business Banking Online enables you to divide an account into segments ("sub-accounts") for your internal accounting purposes.

- 24.3 You acknowledge that:
- a. we are not able to access sub-accounts; and
 - b. although we create sub-accounts on your instructions we do not monitor or recognise balances or the names assigned to them.
- 24.4 You acknowledge that the creation of sub-accounts in no way impacts on your obligations to us under this agreement or the account terms and conditions.
- 24.5 Business Banking Online enables you to restrict a user's use of Business Banking Online to specified sub-accounts. These restrictions are for your own internal procedures, and are not recognised by us.
- 24.6 Our right to rely on the authority of a *user* (set out in clause 20) is unaffected by the creation of sub-accounts or by you restricting a *user's* access to Business Banking Online.
- 24.7 You undertake to hold all money in the *account* in your own capacity and not to use the sub-accounting service to create a trust or agency relationship with any person.
- 24.8 Cheques may be drawn only by authorised signatories in accordance with the terms and conditions applying to the *account*.

25 Payment facilities available through Business Banking Online.

- 25.1 The terms and conditions for RTGS services are contained in clause 59 and as otherwise advised to you prior to completing an RTGS transaction.
- 25.2 The terms and conditions for telegraphic transfers are contained in clause 60 and as otherwise advised to you prior to completing a telegraphic transfer transaction.
- 25.3 Please refer to the Business Banking Online fees and charges brochure for the fees and charges associated with RTGS and Telegraphic Transfers.

26 **Corporate Solution.**

If we agree, you may use BankSA *Corporate Solution* through Business Banking Online. All rights and obligations arising under these Terms and Conditions also apply when a user is using Corporate Solution.

27 **Indemnity.**

You indemnify us against, and you must therefore pay us on demand for, liability, loss or costs we suffer or incur:

- a. if you or a *user* is in default under the agreement constituted by these Terms and Conditions or any other agreement entered into in connection with this agreement (including Corporate Solution); or
- b. as a result of unauthorised use by any person of Business Banking Online, any *authentication device* which may be used to access or use Business Banking Online or Corporate Solution; or
- c. as a result of any claim against us by a third party (including the owner of a BankSA Co-branded Stockbroker account, BankSA Investor Account or BankSA 360 Account) in connection with wilful misconduct or a negligent, illegal or fraudulent act or omission by *you* or any *user* in relation to an *account* (including an Investor Account or a Co-branded Stockbroker Account).

This is a continuing obligation, independent of your other obligations under the agreement constituted by these terms and conditions.

It is not necessary for us to incur expense or make payment before enforcing this right of indemnity provided that such indemnity does not apply to the extent that any liability or loss is caused by our fraud, negligence, wilful misconduct or any breach of a legal obligation we have to you including the Banking Code obligation we have to act fairly and/or reasonably.

28 Third Party Accounts.

- 28.1 This clause 28 applies when a user uses Business Banking Online to access *third party accounts*.
- 28.2 The *primary client* warrants that it has all necessary authority from the owner of each *third party account*:
- a. for it and *users* to give instructions in respect of the *third party account*;
 - b. allowing it and *users* to have access to information on the *third party account* (including balances); and
 - c. allowing it and *users* to debit or credit the *third party account*.
- 28.3 If we request, the *primary client* must provide us with written authority in a form acceptable to us signed by the owner of a *third party account* permitting it and *users* to carry out any of the functions described in clause 28.2 in respect of the *third party account*.
- We need not act in accordance with any instructions relating to a *third party account* until we have received the authority for that *third party account*.
- 28.4 Sub-accounting is not available on *third party accounts*. Other restrictions may apply to access of *third party accounts*; refer to the terms and conditions governing the *third party account*.

Section E – Terms and Conditions that apply to BPAY.

29 Features and benefits of the *BPAY scheme*.

The *BPAY scheme* is a facility that allows you to make electronic payments by requesting us to debit an amount from your *account* to pay organisations who agree that you can make payment to them through the *BPAY scheme*.

This Section E applies if a *user* with *authorise* access asks us to make a payment on your behalf through the *BPAY scheme*. We are a member of the *BPAY scheme*. We will tell you if we are no longer a member of the *BPAY scheme*.

30 Significant risks that apply to the *BPAY scheme*.

There is a risk of mistaken, fraudulent or unauthorised transactions occurring on your *account* because of computer or human error or fraud. Please see clause 37 for information about when you will be liable for unauthorised transactions.

There is also a risk that payments will not be received on time due to systems or telecommunications link unavailability, scheduled outage, equipment failure or other reasons.

31 What is the *BPAY scheme*?

- 31.1 The *BPAY scheme* is an electronic payments scheme through which a user with *authorise* access can ask us whilst we are a member of that scheme to make payments on your behalf to organisations (“*billers*”) who tell you that you can make payments to them through the *BPAY scheme* (“*BPAY payments*”).
- 31.2 A user with *authorise* access may choose to make a *BPAY payment* using Business Banking Online.

32 Payments using the *BPAY* scheme.

When a *user* with *authorise* access asks us to make a *BPAY* payment they must give us the information specified in clause 35 below. We will then debit the *account* specified with the amount of that *BPAY* payment. We may decide not to make a *BPAY* payment if there are not sufficient cleared funds in the *account* at the time and when the user tells us to make that payment.

When we make a *BPAY* payment on your behalf we are not acting as your agent or the agent of the *biller* to whom that payment is directed.

33 How to use the *BPAY* scheme.

33.1 A *user* with *authorise* access can ask us to make *BPAY* payments from an *account* if its terms and conditions permit you to make withdrawals from that *account*.

We may impose restrictions on the *accounts* from which a *BPAY* payment may be made. We may impose limits on the amount of *BPAY* payments.

33.2 If there is any inconsistency between the terms and conditions of an *account* and the *BPAY* scheme terms and conditions in this Section E, then the *BPAY* scheme terms and conditions will apply to the extent of that inconsistency.

33.3 A mistaken or erroneous payment received by a *biller* does not constitute under any circumstances part or whole satisfaction of any underlying debt owed between you and that *biller*.

34 Valid payment direction.

Your acknowledgment in clause 20.4 extends to instructions given to us by *users* with *authorise* access to make *BPAY* payments.

35 Information you must give us.

- 35.1 To instruct us to make a *BPAY* payment, the following information must be given:
- a. the *account* to be debited;
 - b. the amount to be paid;
 - c. the biller code of the *biller* to be paid (this can be found on your bill); and
 - d. your customer reference number (this can be found on *accounts* or invoices you receive from *billers*).

Instructions are given by entering the correct numbers into the *user's* computer.

- 35.2 We are not obliged to effect a *BPAY* payment if all of the above information is not given to us or if any of the information given is inaccurate.

36 Payments.

- 36.1 We will not accept an order to stop a *BPAY* payment once a user instructs us to make that *BPAY* payment.
- 36.2 You should notify us immediately if you become aware that a user may have made a mistake when instructing us to make a *BPAY* payment, or if a *user* with *authorise* access did not authorise a *BPAY* payment that has been made from an *account* (except for a mistake as to the amount meant to be paid – for those errors see clause 36.6 below). Clauses 37.2 to 37.4 describe when and how we will arrange for such a *BPAY* payment (other than in relation to a mistake as to the amount you must pay) to be refunded to you.
- 36.3 Subject to clause 39, *billers* who participate in the *BPAY* scheme have agreed that a *BPAY* payment you make will be treated as received by the *biller* to whom it is directed:
- a. on the date you make that *BPAY* payment, if you tell us to make the *BPAY* payment before our payment cut-off time (see clause 39 below) on a *banking business day*; or

- b. on the *next banking business day*, if a user tells us to make a *BPAY payment* after our payment cut-off time (see clause 39 below) on a *banking business day*, or on a *non-banking business day*.
- 36.4 A delay might occur in the processing of a *BPAY payment* where:
- a. there is a public or bank holiday on the day after a *user* tells us to make a *BPAY payment*,
 - b. a user tells us to make a *BPAY payment* either on a day which is not a *banking business day* or after our payment cut-off time on a *banking business day*;
 - c. another financial institution participating in the *BPAY scheme* does not comply with its obligations under the *BPAY scheme*; or
 - d. a *biller* fails to comply with its obligations under the *BPAY scheme*.
- 36.5 While it is expected that any delay in processing a *BPAY payment* for any reason set out in clause 36.4 will not continue for more than one *banking business day*, any such delay may continue for a longer period.
- 36.6 Users must be careful to ensure that they tell us the correct amount they wish to pay. If a user instructs us to make a *BPAY payment* and you later discover that:
- a. the amount they told us to pay was greater than the amount you wish to pay, you must contact the *biller* to obtain a refund of the excess; or
 - b. the amount they told us to pay was less than the amount you needed to pay, you can make another *BPAY payment* for the difference between the amount actually paid to a *biller* and the amount you needed to pay.

37 Liability for mistaken payments, unauthorised transactions and fraud.

- 37.1 *BPAY* scheme participants undertake to promptly process *BPAY* payments. You must tell us promptly:
- if you become aware of any delays or mistakes in processing your *BPAY* payments;
 - if a *BPAY* payment that has been made from an account was not authorised; or
 - if you think that you have been fraudulently induced to make a *BPAY* payment.

We will attempt to rectify any such matters in relation to your *BPAY* payments in the way described in this clause 37. If the ePayments Code applies and a *BPAY* payment is made on the account without your knowledge or consent, liability for that unauthorised *BPAY* payment will be determined in accordance with clauses 6.4 to 6.9. Otherwise, except as set out in clauses 37.2 to 37.4 and clause 42 and subject to clause 6.11, we will not be liable for any loss or damage you suffer as a result of using the *BPAY* scheme.

- 37.2 If a *BPAY* payment is made to a person or for an amount which is not in accordance with a *user's* instructions (if any), and an *account* was debited for the amount of that payment, we will credit that amount to the *account*. However, if you or a *user* were responsible for a mistake resulting in that payment and we cannot recover within 20 banking business days of us attempting to do so the amount of that payment from the person who received it, you must pay us that amount.
- 37.3 If a *BPAY* payment is made in accordance with a payment direction which appeared to us to be from a *user* with *authorise* access but for which a *user* with *authorise* access did not give authority, we will credit the account with the amount of that unauthorised payment. However, you must pay us the amount of that unauthorised payment if:
- we cannot recover that amount within 20 banking business days of us attempting to do so from the person who received it; and

- b. the payment was made as a result of a payment direction which did not comply with our prescribed security procedures for such payment directions.

37.4 If a *BPAY payment* is induced by the fraud of a person involved in the *BPAY scheme*, then that person should refund you the amount of the fraud-induced payment. However, if that person does not refund you the amount of the fraud-induced payment, you must bear the loss.

37.5 If a *BPAY payment* you have made falls within the type described in clause 37.3 and also clause 37.2 or 37.4, then we will apply the principles stated in clause 37.3.

If a *BPAY payment* you have made falls within both the types described in clauses 37.2 and 37.4, then we will apply the principles stated in clause 37.4.

37.6 Your obligation under clauses 37.2 and 37.3 to pay us the amount of any mistaken or unauthorised payment (as applicable) is subject to any of your rights referred to in clause 42.

37.7 You indemnify us against any loss or damage we may suffer due to any claim, demand or action of any kind brought against us arising directly or indirectly because you or any user:

- a. did not observe any of your or their obligations under the *BPAY scheme* terms and conditions; or
- b. acted negligently or fraudulently in connection with these terms and conditions.

37.8 If you tell us that a *BPAY payment* made from an *account* is unauthorised, you must first give us your written consent addressed to the *biller* who received that *BPAY payment*, consenting to us obtaining from the *biller* information about your *account* with that *biller* or the *BPAY payment*, including your customer reference number and such information as we reasonably require to investigate the *BPAY payment*. We are not obliged to investigate or rectify any *BPAY payment* if you do not give us this consent. If you do not give

us that consent, the *biller* may not be permitted under law to disclose to us information we need to investigate or rectify that *BPAY* payment.

38 Suspension.

We may suspend your right to participate in the *BPAY* scheme at any time if you or someone acting on your behalf is suspected of being fraudulent.

39 Cut-off times.

If a *user* tells us to make a payment before the times specified below, it will in most cases be treated as having been made on the same day:

However, the payment may take longer to be credited to a *biller* if a *user* tells us to make a *BPAY* payment on a Saturday, Sunday or a public holiday or if another participant in the *BPAY* scheme does not process a payment as soon as they receive its details.

40 When a *biller* cannot process your payment.

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

- a. advise you of this;
- b. credit your *account* with the amount of the *BPAY* payment; and
- c. if you ask us to do so, take all reasonable steps to assist you in making a *BPAY* payment to that *biller* as quickly as possible.

41 Account records.

You should check your account records carefully and promptly report to us as soon as you become aware of them, any *BPAY* payments that you think are errors or are *BPAY* payments that a *user* did not *authorise* or you think were made by someone else without your permission.

42 Consequential damage.

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

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

43 Privacy.

In addition to clause 35.2, if you register to use the *BPAY scheme*, you agree to us disclosing to *billers* nominated by you and *users* with authorise access and if necessary the entity operating the *BPAY scheme (BPAY Pty Ltd)* and any agent appointed by it from time to time, including *Cardlink Services Limited*, that provides the electronic systems needed to implement the *BPAY scheme*:

- a. such of your personal information (for example your name, email address and the fact that you are our customer) as is necessary to facilitate your registration for, or use of, the *BPAY scheme*; and
- b. such of your transactional information as is necessary to process your *BPAY payments*. Your *BPAY payments* information will be disclosed by *BPAY Pty Ltd*, through its agent, to the biller's financial institution and your information necessary to process your use of *BPAY view*, will be disclosed by *BPAY Pty Ltd*, through its agent, to the *biller*.

You must notify us, if any of your personal information changes and you consent to us disclosing your updated personal information to all other participants in the *BPAY scheme* referred to in this clause 43, as necessary.

You can request access to your information held by us, *BPAY Pty Ltd* or its agent, *Cardlink Services Limited*, at their contact details listed in Section H of this PDS.

If your personal information detailed above is not disclosed to *BPAY Pty Ltd* or its agent, it will not be possible to process your requested *BPAY payment*.

Section F – Terms and Conditions that apply to *Credit Direct Entry*.

44 Features and benefits of *Credit Direct Entry*.

Credit Direct Entry is a payment service that allows you to pay multiple creditors, employees or other third parties by transferring funds to any bank account in Australia with a single file.

Further details about the features and benefits of *Credit Direct Entry* are provided in Section A of this document.

45 Significant risks that apply to *Credit Direct Entry*.

There is a risk that payments will not be received on time using *Credit Direct Entry* due to systems or telecommunications link unavailability, scheduled outage, equipment failure or other reasons. Please see clause 6 for information about loss caused by the failure of electronic equipment.

If your password and any *authentication devices* are lost, stolen or compromised, the security of Business Banking Online may be affected. Please see clause 22 for further information about your obligations to keep your *passwords* and *authentication devices* secure and clause 6 for information about your liability if *passwords* or *authentication devices* are lost, stolen or compromised.

46 What is *Credit Direct Entry*?

You can use *Credit Direct Entry* to create a file which contains details of payments that you want to be made from your *account* to third parties. When you send this file to us, we will process the file and make payments to those third parties in accordance with the details you have entered into the file.

You can use template files to assist you create payrolls and other direct entry files. You can register payee accounts that can be incorporated into a file by clicking on the required payee. The files you create can be for immediate use or you can save them for later use.

47 Your use of Credit Direct Entry.

- 47.1 Prior to your use of *Credit Direct Entry* you will be required to complete a Credit User Application. You must agree to be bound by the terms contained in the Credit User Application as they will apply to your use of *Credit Direct Entry* together with these Terms and Conditions. The Credit User Application requires that you agree to:
- a. comply with all the obligations of a Credit User under the rules of the *BECS* payment system;
 - b. provide the correct title and account number of the account, into which a payment will be made;
 - c. indemnify and keep indemnified each participant in the *BECS* payment system for any loss you cause to them through your misuse of *Credit Direct Entry*;
 - d. agree to your obligations in respect of the *BECS* rules being enforced by other participants in the *BECS* payment system.
- 47.2 We may decide not to make a debit from your *account* if there are not sufficient cleared funds in your account at the time for the transfer of money. It is your responsibility to check whether a debit has been processed and if a debit has not been made in accordance with this clause, you should ensure sufficient cleared funds are made available in your account at the time your next payment is due to be processed.
- 47.3 When there is more than one payment requested by you, we will determine the order in which they are paid.
- 47.4 We will promptly process any complaint that a debit was unauthorised or was otherwise irregular.

Section G – Terms and Conditions that apply to Debit Direct Entry.

48 What is Debit Direct Entry?

Debit Direct Entry is a service that allows you to obtain payment from debtors, customers or other third parties that have authorised you to obtain those payments.

You can use *Debit Direct Entry* to create a file which contains details of payments that you are authorised to receive into your account from third parties. When you send this file to us, we will process the file through *BECS* and obtain payment into your *account* from those third parties, in accordance with the details you have entered into the file.

Set out in this Section G are the terms and conditions which apply to your use of *Debit Direct Entry*. Please read them carefully as its use must be strictly controlled and you may be required to pay any loss caused to others arising from misuse.

We are obliged under the *BECS* procedures to carry out a credit risk assessment of a user before we give them access to *Debit Direct Entry*. You may be required to provide us with further financial information about you before you can use *Debit Direct Entry*.

49 Your use of Debit Direct Entry.

- 49.1 We may authorise you to use *Direct Debit Entry* in our sole discretion. If we do not authorise you, you will not be able to use *Direct Debit Entry*.
- 49.2 After we have authorised your use of *Debit Direct Entry*, you may instruct us from time to time (by sending us a file of debit requests using *Debit Direct Entry*) to debit accounts through *BECS*.

- 49.3 Your instructions to us must be:
- a. in the format we agree from time to time;
 - b. strictly in accordance with the arrangements between you and the *third party payer* (which includes it being within the limits of the authority in the *Direct Debit Request* and in accordance with the terms of *DDR Service Agreement*); and
- 49.4 We will not be obliged to act on any instructions you give us where there is a material change in the format of your instructions (e.g. changes to file values and file frequency) unless you have given us 5 days advance notice.
- 49.5 You must keep a correct trace record for each instruction you give using *Debit Direct Entry*.
- 49.6 You must comply with any user guide or other procedures that we provide to you from time to time.
- 49.7 We will apply maximum limits for *Direct Debit Entry* files processed using Business Banking Online. Any Direct Debit file you give us must be within the limits we agree. If these limits are exceeded your Direct Debit file will not be accepted. You must ensure depending upon the type of limit we have agreed with you from time to time:
- a. Not to exceed the agreed maximum individual transaction limit. This is a limit agreed for each line included in a Direct Debit file; or
 - b. That the total of the Direct Debit file you send to us does not exceed the agreed maximum file limit; or
 - c. That the total maximum monthly limit for all files you give us during a 30-day period does not exceed the agreed monthly limit.

50 Direct Debit Requests and DDR Service Agreements.

- 50.1 Before you accept any Direct Debit Requests or enter into any *DDR Service Agreements*, you must obtain our approval to the format, content and medium of the *Direct Debit Request* and the *DDR Service Agreements*.
- 50.2 You must not vary any *Direct Debit Request* or *DDR Service Agreement*, which we have approved for your use, without our further approval.
- 50.3 Before you use *Debit Direct Entry* to instruct us to debit a *third party payer's* account under *BECS*, you must:
- a. obtain from the *third party payer* a valid and binding *Direct Debit Request* in the latest form we have approved for your use, which authorises the instructions you give to us; and
 - b. enter into and provide to the *third party payer* in writing a *DDR Service Agreement* in the latest form we have approved for you to use.
- 50.4 If you have not entered into a *DDR Service Agreement* with any *third party payer* who, prior to the date of the agreement, authorised you to debit amounts under *BECS*, you agree:
- a. to apply for the benefit of those *third party payers*, the procedures and policies set out in the latest *DDR Service Agreement* we have approved for you use; and
 - b. on enquiry by the *third party payer*, make available to them general descriptive information on those procedures and policies.

51 What you agree and acknowledge about Direct Debit Requests.

You must:

- a. ensure a *third party payer* specifies correct account information on any *Direct Debit Request* you accept from the *third party payer*. You acknowledge that we may be liable to other *BECS* users if you instruct us to initiate debits

relying on incorrect account information given by a *third party payer* in a *Direct Debit Request*. In turn, we may satisfy the liability by relying on the indemnity you give to us under these terms and conditions;

- b. ensure that your correct user identification number, assigned to you in relation to your use of *BECS*, appears on each *Direct Debit Request* you accept from a *third party payer* and all related correspondence you send to a *third party payer*;
- c. retain each *Direct Debit Request* given to you for a period of not less than seven years from the date of the last debit made under the *Direct Debit Request*. You will retain the *Direct Debit Requests* in a manner which:
 - i. secures them from theft or unauthorised disclosure; and
 - ii. allows them to be readily retrieved;
- d. produce any *Direct Debit Request* you retain under this clause on our request or on the request of the *third party payer's* financial institution to verify your authority to debit the *third party payer's* account;
- e. give each *third party payer* direct written notice of any change you propose to make to a *Direct Debit Request* given by the *third party payer*, at least 30 days prior to the change taking effect, and ensure the *third party payer* may cancel the *Direct Debit Request* in response to the change without penalty;
- f. always act in accordance with the terms of the *Direct Debit Request* a *third party payer* gives you and the terms of the latest form of the *DDR Service Agreement* we approved for use by you; and
- g. act promptly in accordance with any instruction given by the *third party payer* to cancel or suspend the *third party payer's Direct Debit Request* or to stop or defer drawings under that *Direct Debit Request*.

52 Investigating complaints.

You will:

- a. investigate and deal promptly and in good faith with any enquiry, claim or complaint that we make in relation to amounts drawn on your instructions;
- b. assist us with such enquiries and in dealing with those claims and complaints (including providing us with any further information or records as we may request of you); and
- c. respond to us in relation to any claim within any period we specify by either:
 - i. accepting the claim and paying the disputed amount to us in any manner agreed between us; or
 - ii. disputing the claim and providing us with full particulars of your reasons for disputing the claim, including, without limitation, evidence of your authority to make the debit.

53 Use of a direct debit system logo.

53.1 Australian Payments Clearing Association Limited (APCA) may agree to allow you to use a logo approved by APCA on the *Direct Debit Request* forms you publish and on related materials.

53.2 You acknowledge that you are entitled to use a logo approved by APCA only whilst continuing to act as a *BECS* user and fully complying with its obligations as a *BECS* user. You acknowledge that if:

- a. your access to *BECS* is withdrawn by us; or
- b. you otherwise cease to be a *BECS* user, your entitlement to use that logo ceases immediately and any further use of that logo by you is an infringement of APCA's rights in that logo.

54 Termination.

We may discontinue your use of *Debit Direct Entry* at any time by giving you at least 30 days' advance notice. You may terminate your *Debit Direct Entry* at any time by giving us at least 30 days' advance notice.

We may discontinue your *Debit Direct Entry* immediately at any time if:

- you breach any provision of the terms and conditions applying to your *Debit Direct Entry* and you have not remedied the breach within 14 days after we have given you written notice specifying the breach;
- you have not used your *Debit Direct Entry* for at least a 12 month continuous period and have not responded to communications from us notifying you of our intention to suspend or terminate the *Debit Direct Entry*; or
- we reasonably believe that terminating your *Debit Direct Entry* is necessary to enable us to comply with our obligations under any law or any obligation under the BECS procedures.

55 Indemnity.

- 55.1 You indemnify us against all claims, demands, actions, costs and expenses arising out of or in relation to:
- a. the debiting to the account of any person and payments to you of any amount:
 - i. the debiting of which was not at that time authorised by, or in accordance with, a *Direct Debit Request* given to you and in force at that time; and
 - ii. to which you were not at the time legally entitled;
 - b. the failure to make payment in accordance with a *Direct Debit Request* in force at the time; and
 - c. your failure to perform the terms of this agreement.
- 55.2 You will pay to us the amount of any demand we make under the indemnity in clause 55.1 but:
- a. that payment is not an admission by you of the validity of our claim; and
 - b. at your request and expense, we will reasonably assist you to investigate the circumstances on which our demand was based.

- 55.3 You are not liable under the indemnity in clause 55.1 to the extent that a court establishes or we expressly admit that the circumstances relating to the demand were caused or contributed to by our negligence or any of our employees or agents in processing your instructions provided using *Debit Direct Entry*.
- 55.4 The indemnity in clause 55.1 is a continuing indemnity and applies in all cases where any at your instructions have been or are given to us. That indemnity survives termination of this agreement.

56 Variation to these terms.

We may vary the Terms and Conditions which apply to your use of *Debit Direct Entry*. We will notify you of such variations in advance in accordance with the notice requirements set out in clause 2.3.

57 Debiting your account.

We may acting reasonably debit any account we hold in your name with any amount that you must pay to us under this agreement.

58 Inconsistency of terms.

- 58.1 The terms and conditions set out in this section G prevail over any other Terms and Conditions in this PDS to the extent that there is any inconsistency.
- 58.2 Clause 58.1 applies only to the extent that the ePayments Code does not apply to your use of *Debit Direct Entry* if the ePayments Code does apply, the Terms and Conditions in this PDS that relate to the ePayments Code prevail over those in this Section F to the extent of any inconsistency.

Section H – Terms and Conditions that apply to RTGS and Overseas Telegraphic Transfer.

59 RTGS.

59.1 If you complete a request to have a payment made by RTGS you acknowledge that the payment instructions to us will be effected in real time, which means that once given to us, payment instructions cannot be revoked and that settlement will be immediate.

We may not act upon an instruction given by you until there are sufficient clear funds in your account.

We may utilise the services of another bank or branch for the purpose of giving effect to your instructions.

Except as provided, we will act upon your instructions without delay and cannot be held responsible for any delay in receipt by the person named as the beneficiary (“the Beneficiary”).

We are not liable for any loss or costs as a result of:

- a. any delays, errors or omissions in transactions except to the extent that it’s caused by our fraud, negligence, wilful misconduct or any breach of a legal obligation we have to you; or
- b. any acts, default or negligence of:
 - i. you in providing your instructions; or
 - ii. other banks or agencies whose services are used by us in giving effect to your instructions.

You warrant to us that particulars in your instructions are correct.

Beneficiary Account.

We will rely solely on the Beneficiary’s account number that you have provided in order to make payment.

We are under no obligation to check prior to making payment that the Beneficiary's account number corresponds with the Beneficiary's details. In those circumstances, you acknowledge that you and not us will be responsible for the "recovery" of the payment if it was sent to someone who was not the intended beneficiary.

Unless otherwise stated, charges made by the receiving bank will be the responsibility of the Beneficiary and may be deducted from the Beneficiary's account.

We will debit any fees in relation to carrying out your instructions and that may be payable as a result of utilising the services of another bank or branch to your account.

60 Overseas Telegraphic Transfer.

60.1 We, our correspondents and/or relationship banks will not be liable for any loss or costs as a result of any delay or error in transit or transmission of an Overseas Telegraphic Transfer ("T/T"), except to the extent that it's caused by our or our correspondents' and/or relationship banks' fraud, negligence, wilful misconduct or any breach of a legal obligation we have to you.

We advise that where a T/T is requested prior to 5.00pm (AEST) on a business day, we will begin processing that request on the same business day. Where a T/T is requested after 5.00pm (AEST) on a business day (or where the request is received on any day that is not a business day), we will begin processing that request on the next business day.

If you have received a product disclosure statement for our treasury services and entered into a forward foreign exchange contract with us, you may request that a T/T occur at a specified future date. In that case, we will endeavour to process the T/T before 5.00pm (AEST) on the day that you specify.

In most cases involving T/Ts requested prior to 5.00pm (AEST) to overseas banks in major global financial centres, funds would normally be received by the overseas bank within 1–3 business days. For T/Ts to other destinations, the time that funds become available from the overseas bank is subject to the practice of the correspondents and/or relationship banks.

We may at our sole discretion utilise the services of any correspondents and/or relationship banks in order to effect the T/T.

Payment and the timing of the payment to the beneficiary is the responsibility of the correspondents and/or relationship banks. In order to facilitate your payment, other banks involved in the payment processing may convert the payment or impose additional fees or charges.

Where you have nominated the overseas bank charges to be levied to your account, a fee will be debited by us when the Telegraphic Transfer application has been accepted.

Where you have nominated the overseas bank charges to be borne by the beneficiary, these charges will be deducted from the Telegraphic Transfer proceeds by the correspondents and/or relationship banks. We may receive commissions or other benefits from other financial institutions.

If you agree to pay the overseas bank charges, payment will be made upon terms to be agreed between you and us from time to time. We do not have any control of when the funds will be paid to the beneficiary.

Regardless of whether a TT fee is charged, in order to make a TT through Business Banking Online, you must select an eligible fee account. To be an eligible fee account, it will need to be a St.George, BankSA or Bank of Melbourne account that can be charged fees but is not a Foreign Currency Account.

If you instruct us to transfer an amount in a foreign currency, we will convert the relevant amount to Australian dollars using an exchange rate notified to you at the time of submitting the transfer request. We may determine this exchange rate in our absolute discretion.

If you request us to stop or cancel a T/T you must pay any fees or charges imposed by another financial institution involved in carrying out the T/T (including any fees or charges imposed in relation to the request to stop or cancel the T/T). You must also pay and fees and charges imposed by us.

If we are able to stop or cancel a T/T:

- a. Any fees and charges payable by you will usually be deducted from the amount refunded;
- b. Where the amount refunded was in a foreign currency, we will convert the amount to be refunded to Australian dollars using an exchange rate we may determine in our absolute discretion (this exchange rate will usually be different from the exchange rate initially used in relation to the transfer).

Section I – Definitions.

access method means a method we authorise you to use to instruct us through *electronic equipment* to debit or credit an account. It comprises the use of one or more components, including a *password* or *authentication device*. It does not include a method requiring your manual signature as the main way in which we ensure you gave us an instruction.

account means:

- each BankSA account that is specified by you in the application for Business Banking Online or that is otherwise accessible through Business Banking Online; and
- includes each *third party account*, as changed by agreement between you and us from time to time.

additional party means each person who requests to become, and we accept as, an additional party in accordance with clause 21.

administrator means administrator (admin) only or administrator (admin/authorise) as the case requires.

administrator (admin only) has the meaning set out in clause 16.1.

administrator (admin/authorise) has the meaning set out in clause 16.1.

authentication device means a personal authentication device that is issued to a user to assist in validating transactions or changes (including administrative) that require authority in Business Banking Online. Each authentication device will have its own operating requirements.

authorise has the meaning set out in clause 16.1.

banking business day means any day on which banks in Melbourne or Sydney are able to effect settlement through the Reserve Bank of Australia.

Banking Code means the Australian Banking Association's banking code of practice as updated, and adopted by us, from time to time.

Basic Single Credit Transfer is a credit payment other than: Osko payment, or an international funds transfer instructions payment; sent using New Payments Platform (NPP) to the payee of another NPP participant.

BECS means the Bulk Electronic Clearing System which is an electronic payment system operated by the Australian Payments Clearing Association Limited.

biller has the meaning set out in clause 31.1.

BPAY payments has the meaning set out in clause 31.1.

BPAY Pty Ltd means BPAY Pty Ltd ABN 69 079 137 518 of Level 9, 20 Berry Street North Sydney 2060
Tel: (02) 9922 3511.

BPAY scheme means the electronic payments scheme promoted by BPAY Pty Limited and operated in accordance with the *BPAY scheme* rules and operating procedures.

Cardlink Services Limited means Cardlink Services Limited ABN 60 003 311 644 of Cnr Park Road and South Parade Auburn 2144 Tel: (02) 9646 9280.

Chargeable financial transaction means any transaction processed through Business Banking Online that attracts a fee as outlined in the Business Banking Online fees and charges brochure.

client means the *primary client* or any *additional party*.

Code means a *password* or *authentication device* or any similar information which may be required in order to make *EFT transactions* to or from an *EFT account* and which you are required to keep secret.

company administrator means the person nominated in your application for Business Banking Online to be the "Company Administrator", as changed by agreement between you and us from time to time.

Corporate Solution means the BankSA Corporate Solution system you may use as contemplated by clause 26 under separate agreement between you and us. Corporate Solution is not a financial product for the purposes of the *Corporations Act 2001* (Cwlth) and the terms and conditions of that system do not form part of this PDS.

create has the meaning set out in clause 16.1.

Credit Direct Entry means a service whereby you are able to pay multiple creditors, employees or other third parties by transferring funds to any bank account in Australia with a single file, resulting in a single debit to your *account*, in accordance with Section F of this PDS.

DDR Service Agreement means the agreement which you are required to enter into, or have entered into, with a *third party payer* from whom you obtain payments using *Debit Direct Entry*.

Debit Direct Entry means a service whereby you are able to obtain payment from *third party payers* by transferring funds from the payers account into your *account* in accordance with Section G of this PDS.

Direct Debit Request means the form containing an authority for you to obtain payments from a *third party payer* by using *Debit Direct Entry*.

EFT account means an *account* from or to which you can transfer funds through electronic equipment by use of an *access method*.

EFT transaction means a transfer of funds initiated by an instruction you give through *electronic equipment* using an *access method* to debit or credit an *EFT account* where the ePayments Code applies and not intended to be authenticated by comparing a manual signature with a specimen signature.

electronic equipment includes a computer, television and telephone.

exit notice means a notice issued in accordance with clause 21.3.

GST means any tax imposed on the supply of any goods, services, real or personal property or other similar things or similar tax.

Identifier means information that you know and must provide to perform an *EFT transaction* but are not required to keep secret.

Mistaken internet payment means a payment, other than one using BPAY, by an individual through a "Pay Anyone" internet banking facility and processed through the direct entry (Bulk Electronic Clearing) system, New Payments

Platform (Osko or Basic Single Credit Transfer) where the funds are paid into the account of an unintended recipient because the individual enters or selects a BSB and Account number or other identifying information that does not belong to the intended recipient as a result of the individual's error or the individual being advised of the wrong BSB and Account number and/or identifier. This excludes payments made as a result of a scam.

Osko means the Osko payment service administered by *BPAY Pty Ltd* that facilitates payments (including Osko Payments) between participating financial institutions. Although Osko is made available by participating members of the *BPAY scheme*, payments using Osko are not *BPAY payments* (and section 4 of these terms and conditions do not apply to payments using Osko).

Osko Payment means a payment made using the Osko payment service. An Osko Payment cannot be stopped after you have instructed us to make it.

password includes a passphrase used in connection with an *authentication device*.

PayID means a unique identifier held in a central register by NPP Australia Limited and accessible to participating financial institutions to facilitate payments to a PayID.

PayID Account means a St.George Banking Group eligible account which can have a PayID linked to it.

payment cut-off time means, with respect to a *banking business day*, the time specified in clause 39 for that day.

Payment Services means *BPAY, Credit Direct Entry, Debit Direct Entry, RTGS* and overseas telegraphic transfers.

primary client means the person identified as "Primary Company" in the Business Banking Online application.

principal means any of you who is a director or partner of, or the sole trader operating, the *primary client* or an *additional party*.

RTGS means the transfer of funds using local telegraphic transfers in real time.

Sanctioned Jurisdiction means a jurisdiction listed at banksa.com.au/osaccess

small business has the meaning given to it in the *Banking Code*.

Sub-accounting (SAM) means the functionality described in clause 24.

third party account means an *account* which the *primary client* has been authorised by the third party to access and operate and has been nominated in a "Third Party Accounts form" delivered to us by you.

third party payer means any person who makes, or will make, a payment to you through *Debit Direct Entry*.

user means the *company administrator* or any person given *view, create, authorise, administrator (admin only) or administrator (admin/authorise)* rights under clause 16.1. A user may be one of your employees or any person external to your organisation such as an accountant *view* has the meaning set out in clause 16.1.

we or **us** or **BankSA** or **the Bank** means BankSA – A Division of Westpac Banking Corporation ABN 33 007 457 141 AFSL and Australian credit licence 233714 and its successors and assigns.

you/your means each *primary client, additional party, principal* or *person* named on the application for *Credit Direct Entry* as a 'Credit User'. In the case of Overseas Telegraphic Transfer you/your means the requesting party. If there are more than one, you means each of them separately and every two or more of them jointly. You includes your successors and assigns.

In this PDS and any Corporate Solution agreement:

- a reference to these terms and conditions, an agreement or another instrument includes any variation or replacement of any of them;
- the word “person” includes a firm, a body corporate, a partnership, joint venture, an unincorporated body or association, or any government agency;
- “including” when introducing an example, does not limit the meaning of the words to which the example relates to that example or examples of a similar kind;
- the singular includes the plural and vice versa.

More Information.

There are booklets called “Corporate and Business Accounts and Payment Services Terms and Conditions – General Information” (“Terms and Conditions”) and “Corporate and Business Accounts and Payment Services Fees and Charges and how to minimise them” which are available on request from any of our BankSA branches.

The Terms and Conditions booklet contains all types of information about banking services and the *Banking Code*, such as account opening procedures, confidentiality and complaint handling procedures, combining accounts, bank cheques, cheques and cheque clearing, the advisability of your notifying us if you are in financial difficulty and the advisability of your reading the terms and conditions of any banking service we offer you.

Important contact details.

Business Banking Online Helpdesk

Call 1300 554 004, Monday to Friday 7.30am - 7.30pm.

Disputes.

If your complaint is not immediately resolved to your satisfaction, contact:

Manager, Customer Relations

PO Box 399

Adelaide SA 5001

If you are not satisfied with our response, you may be able to lodge a complaint with the Australian Financial Complaints Authority (AFCA). AFCA's contact details are:

Online: www.afca.org.au

Email: info@afca.org.au

Phone: 1800 931 678

Mail: Australian Financial Complaints Authority
GPO Box 3 Melbourne VIC 3001

By clicking "I agree" you agree:

- to be bound by these terms and conditions.

General customer enquiries

Call **13 13 76**, 7.30am to 7.30pm, Monday to Saturday.

Emergency Numbers

To report any loss or theft of your Debit Card or Credit Card, phone:

1800 028 208 (freecall)

24 HOURS – 7 days a week

Outside Australia: +61 2 9155 7850

Disputes

If your complaint is not immediately resolved to your satisfaction, contact:

Manager, Customer Relations
PO Box 399
Adelaide SA 5001

If you are not satisfied with our response, you may be able to lodge a complaint with the Australian Financial Complaints Authority (AFCA). AFCA's contact details are:

Online: www.afca.org.au

Email: info@afca.org.au

Phone: 1800 931 678

Mail: Australian Financial Complaints Authority
GPO Box 3 Melbourne VIC 3001