BankSA Internet and Phone Banking.

Terms and Conditions and Important Information.

Effective date: 3 July 2026

You've got questions? We've got time to talk.

13 13 76
7.30am to 7.30pm
Monday to Saturday

Visit us in branch

banksa.com.au

Accessibility support.

If you are deaf, hard of hearing, or have speech/communication difficulty, you can message us within the BankSA App or communicate with us using the National Relay Service.

If English is not your preferred language, contact us and a banker can arrange a language interpreter.

Visit BankSA Accessibility for further information on our more accessible products and services for people with disability, who are neurodivergent or where English is not your preferred language.

This document sets out terms and conditions for BankSA Internet, Mobile and Phone Banking along with important information about these services.

This document does not contain all of the terms and conditions that apply to your use of Internet, Mobile and Phone Banking. Further terms and conditions (including information about fees and charges) are set out in the terms and conditions that apply to accounts that you access using Internet Banking and Phone Banking (including Mobile Banking for services available using Mobile Banking).

Further information about our products and services is available by visiting our website **banksa.com.au**

Contents.

Important Information. 5

Security. 5

Stopping or altering payments. 5

Scheduled transactions and payments. 5

Other transactions and payments. 5

Faults and service difficulties. 5

Limits on your use of Internet and Phone Banking. 5

Table A. 6

Table B. 7

Warning – authorised signatories. 7

Section 1 – Internet and Phone Banking. 8

1. Internet & Phone Banking terms and conditions. 8
2. Using Internet and Phone Banking. 8
3. Valid payment direction and cut-off times. 12
4. Receipts and records. 13
5. Delayed transactions. 13
6. Stopping or altering payments. 13
7. Availability, cancellation, suspension. 15

Section 2 – Secure Code Service. 16

8. Secure Code Service terms and conditions. 16

Section 3 – Mobile Banking. 16

9. Mobile Banking terms and conditions. 16

Section 4 – BPAY. 20

10. BPAY terms and conditions. 20
11. How to use BPAY. 20
12. Valid payment direction. 20
13. Information you must give us. 21
14. Stopping or altering payments. 21
15. Liability for BPAY mistaken payments, unauthorised transactions and fraud. 22
16. Suspension. 23
17. Cut-off times. 23
18. When a Biller cannot process your payment. 23
19. EFT Account records. 24

20. Consequential damage. 24
21. Privacy. 24

Section 5 – PayID and PayTo. 25

22. PayID and PayTo. 25

Section 6 – Verify with Confirmation of Payee service. 31

23. Verify with Confirmation of Payee service. 31

Section 7 – Alerts Services. 32

24. Alerts Services. 32

Section 8 – Telegraphic Transfers. 33

25. Telegraphic Transfer terms and conditions. 33

Section 9 – General matters. 34

26. Security of your Internet and Phone Banking Access Codes. 34
27. Liability for unauthorised Internet, Mobile and Phone Banking transactions. 37
28. Electronic banking system malfunction. 39
29. Mistaken Internet Payments. 39
30. Industry codes. 42
31. Changes to the Terms and Conditions. 42
32. Communications. 44
33. Appropriate use of our services. 44
34. Trade practices. 44
35. GST. 45
36. Fees and charges. 45
37. Assignment. 45
38. Feedback and Complaints. 45
39. Electronic notices and correspondence. 46
40. Privacy Statement and Consent Request. 47
41. Duty of Confidentiality. 47
42. Technical and other information. 47
43. Meaning of words. 48

Important Information.

Security.

The security of your Access Codes (including your Internet and Phone Banking Security Number and Internet Banking Password, and any Mobile Banking Device) is very important. They can be used to access information about you and your EFT Accounts. They can be used to ask us to perform transactions on each of your EFT Accounts. You must make every effort to ensure that your Access Codes, and any record of them, are not misused, lost or stolen. You must tell us as soon as possible if any Access Codes are lost or stolen.

Stopping or altering payments.

Except for BPAY® Payments and Telegraphic Transfers, we use only the BSB and account number, or PayID where a PayID is provided instead of a BSB and account number, to process payments and transfers to accounts held with financial institutions other than BankSA. Please make sure any BSB and account number or PayID you provide us with are correct. We will not check the account name you provide.

If you believe that you have made a mistake in an Internet Banking or Phone Banking transaction or payment, you must contact us as soon as possible on the Internet & Phone Banking Helpdesk, 24 hours a day, seven days, and give full details so that we can locate the transaction or payment and take action.

Scheduled transactions and payments.

You may stop or alter an Internet Banking transaction or payment (including a BPAY Payment) that is a Scheduled Payment by instructing us before midnight on the Business Day immediately prior to the day the transaction or payment is to be made.

Other transactions and payments.

In some limited circumstances it may be possible to stop or cancel a Telegraphic Transfer (this may depend on whether the payment has been processed by us), see clause 6 for further details.

We can only accept a request to stop or alter a transaction or payment that is a Scheduled Payment or Telegraphic Transfer, after you have instructed us to make it.

Faults and service difficulties.

Please tell us about any service fault or difficulty with any of these services by calling the Internet & Phone Banking Helpdesk, 24 hours a day, seven days.

Limits on your use of Internet and Phone Banking.

Monetary limits and thresholds apply to your use of specific Internet Banking (including Mobile Banking, unless separate limits apply) and Phone Banking transactions. The limits in the table below apply unless you have asked for, and we have confirmed, a different limit for a particular account, Biller or payee or transaction. Where more than one limit applies in the circumstances of a particular transaction, your use of Internet Banking and Phone Banking will be limited by the lowest applicable limit. For transactions available through Internet and Phone Banking, the limits may be accumulative.

Note that from 17 March 2024, you will no longer be able to make third party payments via Phone Banking except for BPAY payments. Instead, you can make third party payments through Internet Banking.

Table A.

Daily limits on transactions (excludes Maxi Saver, Business Access Saver and redraws).	
Daily limits on transfers and payments.	
Limit on the total value of transfers (per account) from one or more of your personal or business accounts linked to your **Internet Banking** facility.	$1 million*
Limit on the total value of transfers and payments (per account) from one or more of your business accounts linked to your **Phone Banking** facility.	$25,000
Daily limits on specific activities for personal and business accounts (These transactions are also counted towards your Daily limits on transfers and payments from accounts above.)	
Telegraphic Transfers – Limit on the total value of Telegraphic Transfers using Internet or Phone Banking.	$50,000 (AUD)
Credit Cards – Limit on the total value of transfers to one or more credit card accounts linked to your Internet and Phone Banking facility (other than by BPAY Payments).	$25,000
BPAY Low Risk – Limit on the total value of payments via BPAY to one or more BPAY Billers that we consider to be low risk.	$100,000
BPAY High Risk – Limit on the total value of payments via BPAY to one or more BPAY Billers that we consider to be high risk.	$15,000
PayID – Limit on the total value of payments via PayID to one payee account using Internet Banking. Note: This limit only applies when using PayID and not when you make a payment to a BSB and account number.	A limit of $5,000 per PayID per day applies. A cumulative limit of $25,000 applies for payments made to PayIDs.
Limit on total value of payments to payee accounts (BSB and account number) using Internet Banking.	$25,000 (if maximum transfer amount of $5,000 per payee per day applies) or $100,000 (if maximum transfer amount of $25,000 per payee per day applies)
Limit on the total value of payments from one or more of your accounts using Internet Banking. This is a cumulative total for all payments made to a payee and PayID.	$100,000

*Merchants or other providers of facilities may impose additional limits.

Table B.

Daily limits on transactions Maxi Saver, Business Access Saver and redraws (subject to us approving your request).	
Daily limits on transfers from accounts.	
Limit on the total value of transfers from one or more Maxi Saver, Business Access Saver accounts.	$2 million
Limit on the total value of redraws each day for one or more home loans. **Note:** For fixed rate loans, only available funds that have been paid into the loan during the fixed rate period can be redrawn, up to the applicable prepayment threshold.	$100,000 (min amount $1)
Limit on the total value of redraws from one or more personal loans.	$30,000 (min amount $500)
For transactions that we consider to be an At Risk Transaction, we may require you to authenticate the transaction using our Secure Code Service.	

Warning – authorised signatories.

If you have provided an authority to operate adding a signatory to operate one of your accounts:

- The authorised signatory will have independent authority over, and control of, the accounts and will be able to see the accounts alongside their own accounts in their Internet Banking.
- You, as the account holder, may not be notified of, and may not have visibility of, the actions taken by the authorised signatory when the authorised signatory uses the account through their own Internet Banking.
- Once you have provided a signatory with the authority to operate your account, the signatory will have the same transfer and payment limits that you do as the owner of the account. This means that the transfer limit of $1 million rather than the payment limit of $100,000 may apply to the movement of funds from your account to any account the signatory has access to via their Internet Banking. This may include personal accounts that the signatory holds in their own name.

You can manage or remove authorised signatories by going to the branch and this cannot be completed via Internet Banking.

Section 1 – Internet and Phone Banking.

1. Internet & Phone Banking terms and conditions.

1.1 These Terms and Conditions apply each time you use Internet Banking or Phone Banking, but do not apply to the extent that these Terms and Conditions are expressly overridden by the terms and conditions of an EFT Account.

1.2 Separate terms and conditions govern Business Banking Online, the Access Methods for Business Banking Online and the security of the digital certificate. Business Banking Online is not available with all accounts. Please contact us on 1300 554 004 between 8am to 8pm, Monday to Saturday if you are interested in Business Banking Online.

Section 9 – General matters contains important information about security of your Access Codes, unauthorised and mistaken transactions and other consumer protection issues.

2. Using Internet and Phone Banking.

2.1 You accept these Terms and Conditions when you register for Internet Banking, Phone Banking or Mobile Banking or when any of Internet Banking, Mobile Banking or Phone Banking is first used in relation to an EFT Account.

Registration.

2.2 You must be registered to use Internet and Phone Banking and Mobile Banking. You may ask us to register you by visiting any of our branches or by calling the Internet & Phone Banking Helpdesk. We may automatically register you for Internet and Phone Banking or Mobile Banking. If we do so, we will give you notice.

If you register for Internet Banking, you will automatically be registered for Mobile Banking. If you register for Mobile Banking, you will automatically be registered for Internet and Phone Banking. However, you may choose to register for Phone Banking only without being registered for Internet Banking and Mobile Banking.

	You will automatically be registered for		
If you register for	**Internet Banking**	**Mobile Banking**	**Phone Banking**
Internet Banking	✓	✓	✓
Mobile Banking	✓	✓	✓
Phone Banking			✓

2.3 When you are registered for Internet and Phone Banking:

(a) we give you an Internet and Phone Banking Customer Access Number;

(b) you may select your own Internet and Phone Banking Security Number (however, we will issue you an Internet and Phone Banking Security Number if you do not select an Internet and Phone Banking Security Number within the time we allow); and

(c) you will be registered for our Secure Code Service (note that some services require the use of our Secure Code Service) – see Section 2.

When you are registered for Internet Banking we give you an automatically generated Internet Banking Password. When you first logon to Internet Banking, you will be prompted to change that automatically generated password.

For your security, we recommend that you choose an Internet and Phone Banking Security Number and an Internet Banking Password that are unrelated to any of your ATM/EFTPOS PINs, and that you can remember without writing it down.

It is highly recommended that you use an Internet Banking Password that is different from any other passwords you use for online services.

We give each of you different Customer Access Numbers, Internet and Phone Banking Security Numbers and Internet Banking Passwords, including if you are a joint account holder.

2.4 When you first logon to Internet Banking after 3 March 2018, you will also be required to agree to receive notices, documents and communications for your current and future accounts electronically through Internet Banking and be notified to your email address when a document is available to retrieve (see clause 39).

2.5 It is your responsibility to ensure any Electronic Equipment, software or service (such as a telephone or internet service) required to use Internet Banking or Phone Banking is available to you, working properly, and that you know how to use it to access Internet Banking or Phone Banking. You must take all reasonable steps to protect the security of your Electronic Equipment's hardware and software, including ensuring that your Electronic Equipment does not have any viruses or any form of program or mechanism capable of recording your Access Methods.

Functionality.

2.6 You can use your Internet and Phone Banking facility to access a range of banking services for accounts linked to your Internet and Phone Banking facility, including:

- transferring funds between EFT Accounts;
- obtaining EFT Account information, such as account balances, and ordering account statements; and
- making BPAY Payments, and payments to accounts that are not linked to your Internet and Phone Banking facility (such as accounts held at other financial institutions). Additional banking services are available through Internet Banking, including:
  - setting up Scheduled Payments;
  - ordering Telegraphic Transfers; and
  - opening and closing a range of eligible accounts.

Some of these Internet and Phone Banking services can be accessed through Mobile Banking – see Section 3. Not all banking services are available using Internet and Phone Banking for all EFT Accounts. See the EFT Account terms and conditions for further information.

2.7 If you are seeking Internet and Phone Banking to use in relation to an EFT Account which requires two or more to sign, you may only use Internet and Phone Banking or Mobile Banking to debit the account via funds transfer or BPAY if all authorised parties to the EFT Account have informed us in writing and we have approved your use of Internet and Phone Banking and Mobile Banking.

2.8 We may impose limits on your use of Internet Banking and Phone Banking, including daily limits on withdrawals. Details of limits we impose are set out in the front of these Terms and Conditions, and are available by visiting our website **banksa.com.au**.

Open Banking – Consumer Data Right.

Open Banking gives you the ability to share banking information with Accredited Data Recipients that you trust, online.

2.9 From 1 July 2021, individual customers will have the ability to share selected banking data with trusted third parties, including other banks, online through Open Banking – the banking sector's implementation of the Consumer Data Right. To use Open Banking and share your data, you will need to be registered for Internet Banking as well as satisfy other eligibility criteria. If you ask us to share your data via Open Banking, this will not affect any existing data sharing permissions on your accounts in Internet Banking.

Visit **banksa.com.au/openbanking** for further information about Open Banking.

Open Banking for joint accounts held by individual customers.

2.10 Clauses 2.10 to 2.15 are effective from 4 August 2022, only relate to joint accounts held by individual customers and only apply with respect to Open Banking activities.

2.11 From 4 August 2022:

(a) individual customers will have the ability to share data on eligible joint accounts with trusted third parties

(b) BankSA will enable all eligible joint accounts for data sharing. See clause 2.12 for information on what a joint account being 'enabled' for data sharing means.

2.12 The joint account must be 'enabled' for an account holder to authorise BankSA to share data on that joint account. When a joint account is 'enabled', any Open Banking data sharing authorisations created by one account holder are taken to have been pre-approved by all account holders. This means that any joint account holder can authorise BankSA to share data on the joint account with an Accredited Data Recipient, without requiring further approval from any other joint account holder, when BankSA receives a valid data sharing request from an Accredited Data Recipient in respect of that joint account. This is despite any existing banking authorities (i.e. method of operation) that apply to the joint account such as a 'two to sign', 'two or more to sign' or 'all to sign' authority.

2.13 Any joint account holder can at any time view the joint account's data sharing option or change it to 'disabled' at any time through the online consent dashboard in Internet Banking. When a joint account is 'disabled' for data sharing, this means that BankSA will not share any data relating to the joint account with an Accredited Data Recipient (even if BankSA receives a valid data sharing request from an Accredited Data Recipient).

2.14 Once the data sharing is 'disabled':

(a) data sharing will cease for the joint account with respect to any existing data sharing authorisations;

(b) no joint account holder will be able to share data from that account;

(c) any subsequent request made on the online consent dashboard in Internet Banking to enable data sharing on the joint account will need to be approved by all joint account holders within a specified period of time.

2.15 Joint account holders will be notified whenever the data sharing status of the joint account changes. Account holders will also be notified when another joint account holder creates, amends or withdraws an authorisation to share data with an Accredited Data Recipient or an authorisation has expired, unless the joint account holder has nominated not to receive these notifications.

Open Banking for accounts held by Organisations

2.16 Clauses 2.16 to 2.20 are effective from 30 October 2022 and only relate to accounts held by Organisations.

2.17 In order for Organisations to share data with Accredited Data Recipients, they must:

(a) be registered either for BankSA Internet Banking or Business Banking Online; and

(b) first, nominate Nominated Representative(s) (using the form required by BankSA) to share data on their behalf.

2.18 Prior to their appointment, all Nominated Representatives must be individually registered for BankSA Internet Banking (and have their own BankSA Internet Banking credentials).

2.19 Once the Nominated Representative is appointed:

(a) A Nominated Representative can give, amend and manage authorisations to share the Organisation's Open Banking Account data with Accredited Data Recipients.

(b) All of the Organisation's Open Banking Accounts will be available to the Nominated Representative to select some or all of these Open Banking Accounts for data sharing. Open Banking Accounts include accounts that are open, closed, not visible in Internet Banking and accounts the Nominated Representative may not have access to in Internet Banking or Business Banking Online.

(c) The Nominated Representative will access the consent dashboard for the Organisation via their own individual Internet Banking credentials. All Nominated Representative(s) operating on behalf of the Organisation will view the same consent dashboard.

(d) If the Organisation does not have access to BankSA Internet Banking and only has access to Business Banking Online, the Organisation acknowledges that the Nominated Representative will manage authorisations to share the Organisation's Open Banking Account data through BankSA Internet Banking only.

2.20 The Organisation can revoke a Nominated Representative at any time (using the method required by BankSA), and their ability to give, amend and manage authorisations on behalf of the Organisation. Authorisations created by that Nominated Representative will continue until the authorisation expires or until another Nominated Representative removes consent. The Nominated Representative whose appointment is revoked will retain their individual Internet Banking access but will no longer have the ability to share data with Accredited Data Recipients or access the consent dashboard on behalf of the Organisation.

Chat service in Internet Banking.

2.21 We may give you access to our chat service in Internet Banking, where you may interact with the virtual assistant (bot). The virtual assistant provides self-service support and generic, factual information only. It does not take into account your personal circumstances or any information you may provide through the chat service or have previously provided to us. You may be connected to an available member of our staff if needed.

2.22 The virtual assistant and our staff cannot perform any internet banking transaction over the chat service.

2.23 Where the virtual assistant or our staff (if you have been connected to a human) is not able to assist with your query over the chat service, we may refer you to our Phone banking team or a BankSA branch. The terms and conditions that apply to Phone banking set out in this document apply.

2.24 Please do not provide personal information over the chat service unless specifically requested. BankSA's Privacy Statement, which is available at **banksa.com.au/privacy/privacy-statement**, applies to your use of the chat service.

2.25 If the chat service is not available, please call Phone banking.

2.26 You may have access to historic transcripts through the chat service unless cookies and browser history are cleared. You can also request a copy of a transcript from us through the chat service.

3. Valid payment direction and cut-off times.

3.1 We will treat any instruction to transfer funds or make a payment as authorised by you if your Access Method has been used.

3.2 Except for BPAY Payments and Telegraphic Transfers, we only use the BSB and account number, or PayID where a PayID is provided instead of a BSB and account number, to process payments and transfers to accounts held at financial institutions other than BankSA. Please make sure any BSB and account number or PayID you provide us with are correct. We will not check the account name you provide. In some cases, the financial institution receiving the funds may check the account name, and may reject the payment if the account name is incorrect. However, the receiving institution is not obliged to check the account name.

3.3 If you tell us to make an Internet Banking or Phone Banking transaction or payment (other than a BPAY Payment) before the applicable cut-off time, it will in most cases be treated as having been made on the same day. Please see below for more information on cut-off times and payment processing.

Cut-off times (other than for BPAY Payments).

- For payments other than Telegraphic Transfers and Osko® Payments – 5.30pm each Business Day.
- For Telegraphic Transfers – 5.00pm each Business Day.
- For Osko Payments (including payments addressed to a PayID) – typically credited to the recipient account in near real time (although can take longer).

Instructions received after these cut-off times may not be processed until the next Business Day depending on the payment method. This may be the case even if Internet Banking or Phone Banking shows a change in account balances resulting from the instruction given. Different cut-off times apply to different payment methods.

Other than where the payment is an Osko Payment, it usually takes at least two Business Days for a transfer or payment to be received by a payee.

3.4 When transferring funds between St.George Banking Group accounts held by you using Phone Banking or when transferring funds from your account and another account held with St.George Banking Group using Internet Banking, account balances and transaction lists may be updated straight away (except for credit cards, home loans and transfers to a foreign currency account made after the payment cut-off time).

Even where a payment or 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 Business Day.

4. Receipts and records.

4.1 We will provide you with a transaction receipt number each time you make an Internet Banking and Phone Banking transaction.

4.2 If you ask, we will email an electronic receipt for a Scheduled Payment once we make the payment. Otherwise, you agree that we will not issue a receipt to you for a Scheduled Payment. We recommend that you check after the due date for a Scheduled Payment to ensure the Scheduled Payment was made.

4.3 We issue an electronic receipt for other Internet Banking and Phone Banking transactions at the time of the transaction. However, an Internet and Phone Banking transaction may not be processed until the next Business Day.

4.4 You should check your receipts carefully and promptly report any error to us. You can do so (and raise any queries you have with us) by calling the Customer Contact Centre phone number at the end of these Terms and Conditions.

4.5 You acknowledge and agree that we may record Internet Banking and Phone Banking transactions in any manner we choose. We may use these records to, amongst other things, establish or verify that a particular transaction was effected through the use of your Internet Banking or Phone Banking Access Methods.

5. Delayed transactions.

We will endeavour to process all transactions promptly however there may be delays in transactions you initiate through Internet Banking or Phone Banking that are caused by factors beyond our control.

6. Stopping or altering payments.

6.1 If you believe that you have made a mistake in an Internet Banking or Phone Banking transaction or payment, you must contact us as soon as possible by calling the Internet & Phone Banking Helpdesk 24 hours a day, seven days and give full details so that we can locate the transaction or payment and take action.

Scheduled transactions and payments.

6.2 You may stop or alter an Internet Banking or Phone Banking transaction or payment (including a BPAY Payment) that is a Scheduled Payment by instructing us before midnight on the Business Day immediately prior to the day the transaction or payment is to be made.

Other transactions and payments.

6.3 In some limited circumstances it may be possible to stop or cancel a Telegraphic Transfer (this may depend on whether the payment has been processed by us). If you want to attempt to stop or cancel a Telegraphic Transfer you must contact us as soon as possible by visiting a branch, or calling the Internet & Phone Banking Helpdesk 24 hours a day, seven days.

6.4 Further information about stopping or altering BPAY Payments and Telegraphic Transfers is set out in clauses 15 (for BPAY Payments) and 25.7 (for Telegraphic Transfers).

6.5 We will charge you a fee for receiving your instruction to trace or recall an Internet Banking or Phone Banking transaction.

Anti-Money Laundering and Counter-Terrorism Financing Obligations.

When we may delay or refuse transactions.

6.6 In some circumstances, including where we consider it reasonably necessary 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, without giving you notice, take such action including:

- block or place a stop on your card;
- delay, block, freeze or refuse a transaction; and/or
- return a transaction amount to the account from which it was received or as we reasonably consider appropriate.

Examples of when we may take these measures include where we have reasonable grounds to believe that: a transaction breaches Australian law or sanctions (or the law or sanctions of any other country); or a transaction involves a payment to, from or through a Sanctioned Jurisdiction; or your account, Internet Banking and/or card is being used fraudulently or in a way that might cause you or us to lose money; or a payment made to your account is or may be a payment in error (including but not limited to fraudulent payments, or payments relating to a scam); or you do not provide us with any document or information we reasonably request from you.

We may take these measures for as long as we reasonably need. BankSA and its correspondents are not liable for any loss you suffer (including consequential loss) in connection with the relevant product or Internet Banking.

You provide us with the following undertakings and indemnify us against any potential losses arising from any breach by you of such undertakings:

- you will not 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 Internet banking in a Sanctioned Jurisdiction; and
- the underlying activity for which Internet Banking is being provided does not breach any Australian law or sanctions (or the law or sanctions of any other country).

You should also be aware that:

- we may from time to time require additional information from you to assist us to comply with our regulatory and compliance obligations or to manage associated risk; and
- where legally permitted to do so, we may disclose the information gathered to regulatory and/or law enforcement agencies, other banks, other members of the Westpac Group, service providers or to other third parties.

Payments made in error.

6.7 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 the funds to the account from which they were received, or as we reasonably consider appropriate. 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. 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. If you

receive a Mistaken Internet Payment into your account, we may be required to act in accordance with the ePayments Code. See clause 29 (Mistaken Internet Payments) for more information.

7. Availability, cancellation, suspension.

7.1 We will make reasonable efforts to:

(a) ensure that Internet Banking and Phone Banking is available during the hours specified by us from time to time; and

(b) ensure that information we make available to you through Internet Banking and Phone Banking is correct.

7.2 You agree that you will not use Internet Banking to transmit any content, including via any payment methods (for example, text in payment description/reference for Osko, PayID Payments), that in our opinion:

- includes inappropriate, crude or insulting language;
- is defamatory or otherwise unlawful; and/or
- promotes or is, harassing, abusive, intimidating or threatening, including any threats of physical violence or mental harm, to any other person.

If, in our opinion, you do not comply with this clause we may refuse to process a payment and/or suspend or terminate your use of Internet Banking and Phone Banking in accordance with clause 7.3.

7.3 We may suspend or terminate your access to Internet and Phone Banking or any other account access methods without prior notice if we reasonably believe it is necessary or appropriate, for example where we believe that there is a risk of fraud or security, you do not comply with clauses 6.6 and 7.2 above or where we reasonably suspect that you are residing in a Sanctioned Jurisdiction. Should you require assistance, please call the Internet & Phone Banking Helpdesk 24 hours a day, seven days. If you want to use Internet Banking and Phone Banking at a later time, you may ask us to register or activate you again.

If you are travelling to a Sanctioned Jurisdiction, we may without giving you notice suspend your access to Internet Banking or any other account access methods while you are in that jurisdiction.

7.4 We may from time to time require additional documentation or information from you to assist us to comply with our regulatory and compliance obligations or to manage associated risks. Where you do not provide us with any document or information we reasonably request, we may, with reasonable notice, suspend or terminate your access to Internet and Phone Banking or to certain Internet and Phone Banking features. We may choose not to provide you with notice if we determine it is reasonably necessary.

7.5 You can cancel your registration for Internet and Phone Banking by making a request in the Mobile Banking App, visiting any of our branches or by calling the Internet & Phone Banking Helpdesk, 24 hours a day, seven days. This action will also cancel your registration for Mobile Banking. If you want to use Internet and Phone Banking or Mobile Banking at a later time, you may ask us to register you again.

7.6 We may change your Internet or Phone Banking access to an “inactive status” if you do not access Internet or Phone Banking within 120 consecutive days. You can re-activate your access by calling the Internet & Phone Banking Helpdesk 24 hours a day, seven days.

Section 2 – Secure Code Service.

8. Secure Code Service terms and conditions.

8.1 When you use your Internet Banking Access Methods to initiate a transaction, certain transactions may be identified by us as being an At Risk Transaction.

At times we may offer you the option to log in to Internet or Mobile Banking through the use of our Secure Code Service. We will request you to authenticate your identity by using the Secure Code provided by us for each log in attempt.

8.2 At Risk Transactions can only be performed and completed if they are authenticated by our Secure Code Service. This includes using the Secure Code provided by us for each At Risk Transaction. We will provide you with the Secure Code by sending it to your nominated Australian Mobile Phone Number by SMS.

8.3 To perform certain At Risk Transactions, you may be required to be registered for Internet Banking (you will need to perform those transactions using Internet Banking and verify them with a Secure Code).

8.4 If for some reason you are unable to participate in our Secure Code Service, you may discuss with us your special circumstances by contacting the Internet & Phone Banking Helpdesk.

Section 3 – Mobile Banking.

9. Mobile Banking terms and conditions.

9.1 You can use Mobile Banking to perform some of the activities available through Internet and Phone Banking, and Mobile Banking Services.

Where there is any inconsistency between this Section 3 and the remainder of the Internet and Phone Banking Terms and Conditions, this Section 3 prevails.

Registration.

9.2 Registering for Internet Banking automatically registers you for Mobile Banking (however you need not activate Mobile Banking). You can also choose to register for Mobile Banking at the time of registering for Phone Banking.

Using Mobile Banking.

9.3 Not all Electronic Equipment is capable of accessing and using Mobile Banking as your authenticated mobile device. You are responsible for using, having or obtaining a compatible mobile device in connection with any use of the service. We are not responsible for:

(a) any ability of a mobile device to access the service; or

(b) any loss or damage to a mobile device resulting from your access or use or attempted use of Mobile Banking.

9.4 If you travel outside of Australia you may still have access to Mobile Banking. You should check with your telephone communications provider that the mobile device will be able to use relevant network in those countries in which you are travelling. We are not liable for any additional costs you incur.

Any conditions of use and charges relating to a mobile device are your responsibility.

9.5 You may incur charges from your internet or mobile service provider for using Mobile Banking. Any such charges are your sole responsibility and any matters regarding these charges should be raised with your internet or mobile service provider.

9.6 You will use your Access Codes (such as your Internet and Phone Banking Customer Access Number, Security Number and Internet Banking Password) to logon your mobile device to Mobile Banking. Once you have done so, it becomes your Mobile Banking Device and is treated as an Access Method. If you use an eligible mobile device to access Mobile Banking, you can register to logon by using your Security Number, Internet Banking Password or biometric information (if supported, see clause 9.13).

(The list of mobile device operating systems which is compatible with Mobile Banking can be found under the 'Supported Device' link within the Mobile Banking section of the website **banksa.com.au**. Check on the app store for your operating system to see whether your mobile device is compatible with the Mobile Banking App).

To avoid doubt, a tablet-format mobile device which is compatible with a BankSA Mobile Banking App for tablet devices is able to be a Mobile Banking Device.

9.7 You can reset your preferred logon credentials for your Mobile Banking Device at any time on the logon page of the Mobile Banking App.

9.8 Not all Internet and Phone Banking services and features are available for Mobile Banking. The following are limitations of Mobile Banking:

(a) Not all At Risk Transactions that need to be authenticated by our Secure Code Service can be performed using Mobile Banking. Please refer to Section 2 for further information on At Risk Transactions.

(b) The transaction limits set out in Table A at the start of these Terms and Conditions may not apply. You may only perform such transaction where the transaction amount will not be regarded as an At Risk Transaction.

Notifications on your Mobile Banking Device.

9.9 We may send you notifications, including any Alerts Service, to your Mobile Banking Device (for example, 'push' local and broadcast notifications or notifications based on the location of your Mobile Banking Device).

Some notifications are "actionable" which means that once you receive a notification, you can select it in order to access more information or perform an instruction (for example, make a payment to your credit card account).

Anyone who has access to your Mobile Banking Device (including if you lend it to someone else or it is lost or stolen) will be able to see your notifications. You can enable or disable Mobile Banking App notifications at any time by changing the settings on your Mobile Banking Device.

In some instances, notifications may not reach your Mobile Banking Device due to the requirements or limitations of the communications network or system outages or due to factors beyond our control, such as your internet connection.

Where it is reasonable for us to do so or where it is necessary for us to maintain the security or integrity of our systems, we may, with no prior notice to you, temporarily suspend or terminate our notification service to you.

Section 7 applies to the notifications feature described in clause 9.9, and references to "Alerts Services" in that clause should be read as including "notifications under clause 9.9".

Set a PIN on your mobile device to increase your Mobile Banking security.

9.10 To protect your privacy, we recommend setting a PIN or password on your Mobile Banking Device (or logon using biometric information under clause 9.13), and, for additional protection, installing/enabling remote wipe software on your mobile device.

Make sure nobody else knows the PIN for your Mobile Banking Device. Because your Mobile Banking Device is an Access Method, any person who knows your mobile device PIN can instruct us to perform transactions and we will assume that you have authorised the transaction.

Important: The manufacturer of your mobile device is responsible for the security of the device, including the security of "lock" screens, management of PINs and passwords, and the reliability of any biometric methods of unlocking the mobile device (such as fingerprint or face recognition). Before activating a Mobile Banking Device, you should be confident that you are satisfied about the security of your Mobile Banking Device and the ways it can be unlocked.

Preserve the security of your Mobile Banking Device and Mobile Banking.

9.11 When you have a Mobile Banking Device, you must:

(a) not act fraudulently or maliciously in relation to the Mobile Banking App or any of its features. As examples, you will not copy, modify, adversely effect, reverse engineer, hack into or insert malicious code into the Mobile Banking App or your Mobile Banking Device software.

(b) only install approved applications on your mobile device, and that you will not override the software lockdown on your mobile device (i.e. jailbreak your phone).

Lost or stolen Mobile Banking Device.

9.12 If you suspect the security of your Access Codes has been breached, your Mobile Banking Device or your PIN has been lost, stolen or misused, or an unauthorised transaction has occurred on your account you must ensure you call us on the Internet & Phone Banking Helpdesk to change your Access Code (if possible) and ensure that your Mobile Banking Device is de-authorised as a Mobile Banking Device and for any Mobile Banking Services.

Logon using biometric information.

9.13 Where your Mobile Banking Device allows you to control access to it using biometric information such as the fingerprints or facial data you store in the device, Mobile Banking may provide a means for you to use the stored biometric information to authorise Internet and Phone Banking services as a preferred logon credential (e.g. fingerprint logon). You can only do this where you have logged on to Mobile Banking using your full logon credentials. If you wish to logon using biometric information for Internet and Phone Banking services, you should ensure that only your biometric information is stored on the device.

9.14 Each time the Mobile Banking Device detects that biometric information logon has been used to authorise any transactions through Mobile Banking, you instruct us to perform those services.

We do not collect any information about your biometric information. If you activate biometric information logon (e.g fingerprint logon), the Mobile Banking App can tell when your Mobile Banking Device detects that a stored biometric information has been used to authorise a transaction. The Mobile Banking App confirms to us that this has happened, which is an Access Method, and passes that message to us.

Section 9 – General matters contains important information about security of your Access Codes, unauthorised and mistaken transactions and other consumer protection issues.

9.15 We will make reasonable efforts to:

(a) ensure that Mobile Banking is available during the hours specified by us from time to time; and

(b) ensure that information we make available to you through Mobile Banking is correct.

Cancelling and suspending use of Mobile Banking.

9.16 You agree that you will not use Mobile Banking to transmit any content, including via any payment methods (for example, text in payment description/reference for Osko, PayID Payments), that in our opinion:

- includes inappropriate, crude or insulting language;
- is defamatory or otherwise unlawful; and/or
- promotes or is, harassing, abusive, intimidating or threatening, including any threats of physical violence or mental harm, to any other person.

If, in our opinion, you do not comply with this clause we may refuse to process a payment and/or suspend or terminate your use of Mobile Banking in accordance with clause 9.17.

9.17 We may suspend or cancel your access to Mobile Banking without prior notice if we reasonably believe it is necessary or appropriate, for example where we believe that there is a risk of fraud or security breach, you do not comply with clause 9.16 above. Should you require assistance, please call the Internet & Phone Banking Helpdesk 24 hours a day, seven days. If you want to use Mobile Banking at a later time, you may ask us to register or activate you again.

However, we assume no duty to cancel any access. In relation to these Mobile Banking Terms and Conditions, no delay or failure to act will be construed as a waiver of or in any way prejudice, any of our rights. No waiver will be effective unless it is in writing. A waiver of a breach will not waive any other breach.

9.18 To cancel your registration for Mobile Banking, you can cancel your registration for Internet and Phone Banking by making a request in the Mobile Banking App, visiting any of our branches or by calling the Internet & Phone Banking Helpdesk 24 hours a day, seven days. If you want to use Internet and Phone Banking or Mobile Banking at a later time, you may ask us to register or activate you again.

9.19 If you change or no longer use your Mobile Phone Number, you must ensure that the mobile device you no longer use is no longer your authenticated mobile device for Mobile Banking purposes. Call us on the Internet & Phone Banking Helpdesk, 24 hours a day, seven days to update your details and de-activate Mobile Banking and any Mobile Banking services. To re-activate Mobile Banking with any new Mobile Phone Number or device you will need to logon to Mobile Banking with the new mobile device or Mobile Phone Number.

9.20 We may change your Internet or Phone Banking access to an "inactive status" if you do not access Internet or Phone Banking for 120 consecutive days. You can re-activate your access by calling us on the Internet & Phone Banking Helpdesk, 24 hours a day, seven days.

Section 4 – BPAY.

10. BPAY terms and conditions.

10.1 The BPAY terms and conditions set out in this Section 4 apply if you ask 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.

10.2 You may choose to make a BPAY Payment using Internet and Phone Banking or any other payment method accepted by the Biller. You may be able to make a transfer from an account at another financial institution, which is a member of the BPAY Scheme, to an account you have with us through the BPAY Scheme.

10.3 When you ask us to make a BPAY Payment, you must give us the information specified in clause 13. We will then debit the EFT Account you specify with the amount of that BPAY Payment. We may decide not to make a BPAY Payment if there are not sufficient cleared funds in that EFT Account at the time and when you tell us to make that payment.

10.4 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.

11. How to use BPAY.

11.1 You can ask us to make BPAY Payments from an EFT Account if these terms and conditions permit you to make withdrawals from that EFT Account.

11.2 We may impose restrictions on the accounts from which a BPAY Payment may be made. In addition to the limits imposed under clause 2.8, a BPAY Biller may set limits on the amount of a BPAY Payment to that Biller. Some Billers will not accept BPAY Payments from certain accounts (for example, credit card accounts).

11.3 If there is any inconsistency between this terms and conditions document and the BPAY Scheme terms and conditions set out in this Section 4, then the BPAY Scheme terms and conditions will apply to the extent of that inconsistency.

11.4 When you use a credit card to pay a bill through the BPAY Scheme, we treat that payment as a credit card purchase transaction.

11.5 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.

12. Valid payment direction.

We will treat any instruction to make a BPAY Payment as authorised by you if, when it is given to us:

(a) your Internet and Phone Banking Security Number and Internet and Phone Banking Customer Access Number are entered, if you make the BPAY Payment by Phone Banking;

(b) your Internet and Phone Banking Security Number, Internet Banking Password and Internet and Phone Banking Customer Access Number are entered, if you make the BPAY Payment by Internet Banking; or

(c) the instruction is authorised through Mobile Banking under Section 3.

13. Information you must give us.

13.1 To instruct us to make a BPAY Payment, you must give us the following information:

(a) the EFT Account you want us to debit the payment from;

(b) the amount you wish to pay;

(c) the biller code of the Biller you wish to pay (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).

13.2 Instructions are given by entering the correct numbers into your touch-tone telephone (where you are using Phone Banking), your computer keyboard (where you are using Internet Banking), or your Mobile Banking Device (where you are using Mobile Banking).

13.3 We are not obliged to effect a BPAY Payment if you do not give us all of the above information or if any of the information you give us is inaccurate.

14. Stopping or altering payments.

14.1 If you believe that you have made a mistake in a BPAY Payment, you must contact us as soon as possible by calling the Internet & Phone Banking Helpdesk, 24 hours a day, seven days and give full details so that we can locate the transaction and take action.

14.2 You may stop or alter a BPAY Payment that is a Scheduled Payment by asking us to before midnight on the Business Day immediately prior to the day the transaction or payment is to be made.

14.3 We cannot accept a request to stop or alter a BPAY Payment that is not a Scheduled Payment after you have instructed us to make it.

14.4 Subject to clause 17, 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 17) on a Banking Business Day; or

(b) on the next Banking Business Day, if you tell us to make a BPAY Payment either after our Payment Cut-Off Time (see clause 17) on a Banking Business Day or on a non-Banking Business Day.

14.5 A delay might occur in the processing of a BPAY Payment where:

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

(b) you tell 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.

14.6 While it is expected that any delay in processing a BPAY Payment for any reason set out in clause 14.5 will not continue for more than one Banking Business Day, any such delay may continue for a longer period.

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

(a) the amount you told us to pay was greater than the amount you needed to pay, you must contact the Biller to obtain a refund of the excess; or

(b) the amount you 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.

15. Liability for BPAY mistaken payments, unauthorised transactions and fraud.

15.1 BPAY participants undertake to promptly process BPAY Payments.

You must tell us promptly:

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

(b) if you did not authorise a BPAY Payment that has been made from an EFT Account; or

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

15.2 We will attempt to rectify any such matters in relation to your BPAY Payments in the way described in clauses 15.3 to 15.5. If the ePayments Code applies to an EFT Account and a BPAY Payment is made on the EFT Account without your knowledge or consent, liability for that unauthorised BPAY Payment will be determined in accordance with clause 27. Otherwise, except as set out in clauses 15.3 to 15.5 and clause 20 and subject to clause 28.3, we will not be liable for any loss or damage you suffer as a result of using the BPAY Scheme.

15.3 If a BPAY Payment is made to a person or for an amount which is not in accordance with your instructions (if any), and an EFT Account was debited for the amount of that payment, we will credit that amount to the EFT Account. However, if you 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.

15.4 If a BPAY Payment is made in accordance with a payment direction which appeared to us to be from you or on your behalf but for which you did not give authority, we will credit the EFT Account with the amount of that unauthorised payment. However, you must pay us the amount of that unauthorised payment if:

(a) 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.

15.5 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.

15.6 If a BPAY Payment you have made falls within the type described in clause 15.4 and also clause 15.3 or 15.5, then we will apply the principles stated in clause 15.4.

15.7 If a BPAY Payment you have made falls within both the types described in clauses 15.3 and 15.5, then we will apply the principles stated in clause 15.5.

15.8 Except where a BPAY Payment is a mistaken payment referred to in clause 15.3, an unauthorised payment referred to in clause 15.4, or a fraudulent payment referred to in clause 15.5, BPAY Payments are irrevocable. No refunds will be provided through the BPAY Scheme where you have a dispute with the Biller about any goods or services you may have agreed to acquire from the Biller. Any dispute must be resolved with the Biller.

Important – Even where your BPAY Payment has been made using a Visa Debit Card, no chargeback rights will be available under BPAY Scheme rules. Please see the EFT Account terms and conditions for further information on chargebacks.

15.9 Your obligation under clauses 15.3 and 15.4 to pay us the amount of any mistaken or unauthorised payment (as applicable) is subject to any of your rights referred to in clause 20.

15.10 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:

(a) did not observe any of your obligations under this section; or

(b) acted negligently or fraudulently in connection with these terms and conditions.

15.11 If you tell us that a BPAY Payment made from an EFT 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 of 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.

16. 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.

17. Cut-off times.

If you tell us to make a BPAY Payment before the times specified, it will in most cases be treated as having been made on the same day.

Payment cut-off times (for BPAY Payments):

7 days, 5.30pm. However, if you tell 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 BPAY Payment as soon as they receive its details, the payment may take longer to be credited to a Biller.

18. When a Biller cannot process your payment.

If we are informed that your payment cannot be processed by a Biller, we will:

(a) inform you of this;

(b) credit your EFT 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.

19. EFT Account records.

You should check your EFT 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 you did not authorise or you think were made by someone else without your permission.

20. Consequential damage.

20.1 This clause does not apply to the extent that it is inconsistent with or contrary to any applicable law or code of practice to which we have subscribed. If those laws 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.

20.2 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.

21. Privacy.

21.1 You agree to our disclosing to Billers nominated by you 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 information 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, rectify or trace your BPAY Payments. Your BPAY Payments information will be disclosed by BPAY Pty Ltd, through its agent, to the Biller's financial institution. Also, we may disclose such of your transactional information as is necessary to rectify or trace a BPAY Payment you make by mistake to the Biller that received the payment and the Biller to whom you intended to make the payment or the financial institution of either or both Billers.

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

21.3 You can request access to your information held by us by contacting us, or by contacting BPAY Pty Ltd or its agent, Cardlink Services Limited.

21.4 If your 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 5 – PayID and PayTo.

22. PayID and PayTo.

PayID.

22.1 A PayID® is a unique identifier that can be used to receive and make payments made from accounts held with participating financial institutions throughout Australia.

22.2 Once you have created a PayID with us, your PayID will be linked to one PayID Account. When you would like a person to make a payment to your PayID Account, you can give them your PayID, rather than the BSB and account number of your PayID Account. You may also make payments to another person by using their PayID (whether their account is held with us or another financial institution). Payments to a PayID count towards the daily limits on transactions on your account – see Limits on your use of Internet and Phone Banking in Important Information.

22.3 Your PayID (and the details linked to it) will be held in a central register by NPP Australia Limited that will be accessible to participating financial institutions. Because your PayID is a unique identifier, a PayID can only be registered with a single participating financial institution, and linked to one account. We may require your PayID to contain certain details (such as by requiring your PayID to be consistent with your Internet Banking identity).

22.4 When we process a payment to a PayID we check only that the details you provide match a registered PayID. We do not check the owner of the PayID, or the account that is linked to that PayID. You and any User are responsible for providing correct details for any payment made or received using a PayID (including amounts and PayID details). We have no liability to you or any User for any payment made in accordance with details provided by you or the User.

22.5 You may include a short description when you make a payment to a PayID, making it easier to know what a payment is for. You must not enter inappropriate payment descriptions such as insulting or defamatory text (see clause 7.2 and 9.16). We will not be liable to you or any other person for inappropriate payment descriptions.

> A payment to a PayID cannot be stopped after you have instructed us to make it.

Creating and managing your PayID.

22.6 Creating PayID is optional, and we will not create a PayID for you without your consent. You can create a PayID with us through Internet Banking. When you create a PayID with us you will need to link your PayID to an eligible PayID Account. To transfer an existing PayID to us, you need to contact the financial institution where your PayID is currently registered and tell them you would like to transfer your PayID to us (we cannot transfer it for you) and then register it with us through Internet Banking.

Please note not all BankSA accounts can be linked to a PayID, and we may not allow all types of PayIDs to be linked to an Account. For an eligible Account that is held jointly, more than one PayID may be created for the Account provided each PayID is unique. You can find out more about the accounts that can be linked to a PayID at BankSA, and the types of PayIDs that can be used to make or receive payments, by visiting our website **banksa.com.au**

22.7 We will only allow you to create a PayID and receive and make payments using your PayID if we are satisfied that you have the right to use the PayID. (For example, your PayID must reasonably represent the identity of your business. Your PayID should not mislead a payer into sending you

NPP Payments intended for another payee.) We may ask you to provide information that, in our reasonable opinion, establishes that you have the right to use the PayID. If there is a conflict or dispute over a PayID we may lock or close the PayID.

22.8 As your PayID is linked to your PayID Account, it is important that you keep your PayID details up to date at all times. Contact us if you would like us to:

- change your PayID, or update your PayID details, such as when your Mobile Phone Number changes;
- change the PayID Account linked to your PayID – you will need to be authorised to transact on the changed account;
- transfer your PayID to another participating financial institution; or
- close, lock or unlock your PayID.

You must notify us immediately if your PayID details change.

If you ask us to transfer, lock or close your PayID, your account will remain linked to your PayID, and your PayID may be used to make and receive payments, until we are able to complete processing your request (including, for transfers, where the other financial institution processes the request).

You can instruct us to:

- transfer your PayID to a different account you hold with us,
- initiate a transfer of your PayID to another financial institution, or
- close your PayID, by calling Internet & Phone Banking Helpdesk.

We will typically give effect to your instruction within 24 hours. Please note, if you wish to transfer your PayID to an account with another financial institution, you are responsible for registering your PayID with that financial institution during the two week period (starting from the day we receive your instruction). After this period, the transfer request will lapse.

If you have asked us to transfer your PayID to another financial institution, and that financial institution does not process the transfer request within the timeframes required under the rules applying to PayID transfers, your transfer request will be cancelled (and your PayID will remain registered with us and linked to your PayID Account).

Locked PayIDs, closed PayIDs.

22.9 You may lock your PayID by contacting us at any time on 13 13 76. While your PayID is locked:

- your PayID will not be able to receive and make payments; and
- you will not be able to update your PayID or transfer your PayID to another financial institution.

If you suspect any unauthorised use of your PayID, you must contact us as soon as possible.

We may, acting reasonably, lock or close your PayID at any time. Without limiting the reasons why we may do so, this may happen if:

- we reasonably suspect that you may not have the right to use a PayID (including where you change your Mobile Phone Number with us without changing that number for your PayID);
- we reasonably consider you have induced us to create or register a PayID by fraud;
- your linked PayID Account is blocked or suspended;
- we believe your PayID is being used in a way that may cause loss to you or us;
- we suspect your PayID is being used fraudulently; or
- we believe your PayID has become inactive.

22.10 We may also close your PayID if your access to Internet Banking facility is closed, cancelled or suspended (and your PayID has not been transferred to another financial institution).

PayTo.

Creating a Payment Agreement.

22.11 You may establish and authorise Payment Agreements with merchants or Payment Initiators who offer PayTo® as a payment option, for an eligible EFT Account (as determined by us from time to time).

To create a Payment Agreement for an eligible EFT Account:

Step 1.

You will be required to provide the merchant or Payment Initiator with your personal information, including the BSB and Account number or PayID, of the eligible EFT Account. You must ensure your details are correct.

Step 2.

The merchant or Payment Initiator will create and submit a record of the Payment Agreement to their financial institution or payments processor to record in the Mandate Management Service.

Step 3.

Once the Mandate Management Service notifies us that a Payment Agreement has been created using your EFT Account or PayID details, we will notify you via Internet or Mobile Banking, email (to your nominated email address) or SMS, and ask you to confirm the Payment Agreement by providing you with details of the:

- merchant or Payment Initiator,
- payment amounts and payment frequency (where provided in the Payment Agreement).

Step 4.

You may confirm or decline the Payment Agreement:

- if you **confirm**, we will record your confirmation against the record of the Payment Agreement in the Mandate Management Service and the Payment Agreement will become effective (i.e. we will process payment instructions under the Payment Agreement).
- if you **decline**, we will record that against the record of the Payment Agreement in the Mandate Management Service.

(Note: if you believe that the payment amount or frequency, or any other detail presented in the Payment Agreement is incorrect, you may decline the Payment Agreement, contact the merchant or Payment Initiator, and have them amend and resubmit the Payment Agreement creation request.)

If a Payment Agreement requires your confirmation within a timeframe stipulated by the merchant or Payment Initiator, and you do not provide confirmation within that timeframe, the Payment Agreement may be withdrawn by the merchant or Payment Initiator.

22.12 From 12 September 2025, to increase the security of your PayTo service, we may impose limits on PayTo Payment Agreements or restrict your use of the PayTo service with a certain group of billers. These restrictions may relate to the value of the payment or the classification of the biller's business by the type of goods or services they provide, such as cash or cash equivalents and high value consumer goods. PayTo Payment Agreements may be rejected where they do not comply with these restrictions.

22.13. If a PayTo Payment Agreement is rejected, the biller will not be able to initiate a payment from your account under that PayTo Payment Agreement. Rejected PayTo Payment Agreements will not appear in Internet Banking.

22.14. PayTo payments are not included in your account's daily limits on transactions.

22.15 Please ensure that the details of the Payment Agreement are correct before you confirm them. We will not be liable to you or any other person for loss suffered as a result of processing a payment instruction submitted under a Payment Agreement that you have confirmed.

Amending a Payment Agreement.

22.16 Your Payment Agreement may be amended by the merchant or Payment Initiator from time to time, or by us on your instruction.

You may instruct us to amend your Account details in the Payment Agreement. EFT Account details may only be replaced with the BSB and account number (or PayID) of an EFT Account.

We may decline to act on an instruction to amend your Payment Agreement if we are not reasonably satisfied that the request is legitimate. You may not request us to amend the details of the merchant or Payment Initiator, or another party.

22.17 We will send you a notification of proposed amendments to the Payment Agreement via Internet or Mobile Banking, email (to your nominated email address) or SMS for your authorisation:

- if you **confirm**, we will promptly record the confirmation against the record of the Payment Agreement in the Mandate Management Service and the amendment will become effective.
- if you **decline**, the amendment will not be made. A declined amendment request will not otherwise affect the Payment Agreement.

If you decline the amendment request because of incorrect details, you may contact the merchant or Payment Initiator and have them resubmit the amendment request with the correct details. We are not authorised to vary the details in an amendment request submitted by the merchant or Payment Initiator.

- if you **do not confirm or decline** within 6 calendar days of the notification being sent to you (or if the amendment is withdrawn by the merchant or Payment Initiator), the amendment request will expire and will be deemed to be declined.

Pausing your Payment Agreement.

22.18 You may instruct us to pause and resume your Payment Agreement via Internet Banking. We will promptly act on your instruction by updating the record of the Payment Agreement in the Mandate Management Service. The Mandate Management Service will notify the merchant's or Payment Initiator's financial institution or payment processor of the pause or resumption.

During the period the Payment Agreement is paused, we will not process payment instructions in connection with it. We will not be liable for any loss that you or any other person may suffer as a result of the pausing of a Payment Agreement that is in breach of the terms of an agreement between you and the relevant merchant or Payment Initiator.

22.19 Merchants and Payment Initiators may pause and resume their Payment Agreements. If the merchant or Payment Initiator pauses a Payment Agreement to which you are a party, we will promptly notify you of that, and of any subsequent resumption, via Internet Banking, Mobile Banking, or email. We will not be liable for any loss that you or any other person may suffer as a result of the pausing of a Payment Agreement by the merchant or Payment Initiator.

Cancelling your Payment Agreement.

22.20 You may instruct us to cancel a Payment Agreement on your behalf by contacting us via Internet Banking. We will promptly act on your instruction by updating the record of the Payment

Agreement in the Mandate Management Service. The Mandate Management Service will notify the merchant's or Payment Initiator's financial institution or payment processor of the cancellation. The terms of an agreement between you and the relevant merchant or Payment Initiator may specify certain losses for which you may be liable as a result of that cancellation (e.g. you may be required to pay a cancellation fee after instructing us to cancel the Payment Agreement).

22.21 Merchants and Payment Initiators may cancel Payment Agreements. If the merchant or Payment Initiator cancels a Payment Agreement to which you are a party, we will promptly notify you of that cancellation via Internet Banking, Mobile Banking, or email. We will not be liable to you or any other person for loss incurred due to cancellation of your Payment Agreement by the merchant or Payment Initiator.

Migration of Direct Debit arrangements.

22.22 Merchants and Payment Initiators who have existing Direct Debit arrangements with their customers may establish Payment Agreements for these, as Migrated DDR Mandate, in order to process payments under those arrangements via the NPP rather than BECS (the Bulk Electronic Clearing System). If you have an existing Direct Debit arrangement with a merchant or Payment Initiator, you may be notified by them that future payments will be processed from your EFT Account under PayTo.

You are entitled to prior written notice of variations to your Direct Debit arrangement and changed processing arrangements, as specified in your Direct Debit Service Agreement, from the merchant or Payment Initiator. If you do not consent to the variation of the Direct Debit arrangement, you must advise the merchant or Payment Initiator. We are not obliged to provide notice of a Migrated DDR Mandate to you for you to confirm or decline. We will process instructions received from a merchant or Payment Initiator on the basis of a Migrated DDR Mandate.

22.23 You may amend, pause (and resume), cancel or transfer your Migrated DDR Mandate, or receive notice of amendment, pause or resumption, or cancellation initiated by the merchant or Payment Initiator, in the manner described in Section 5.

Your responsibilities.

22.24 You must:

- ensure that you carefully consider any Payment Agreement creation request, or amendment request made in respect of your Payment Agreement or Migrated DDR Mandate and promptly respond to such requests. We will not be liable for any loss that you suffer as a result of any payment processed by us in accordance with the terms of a Payment Agreement or Migrated DDR Mandate.
- notify us immediately if you no longer hold or have authority to operate the EFT Account from which payments under a Payment Agreement or Migrated DDR Mandate have been (or will be) made.
- promptly respond to any notification that you receive from us regarding the pausing or cancellation of a Payment Agreement or Migrated DDR Mandate for misuse, fraud or for any other reason. We will not be responsible for any loss that you suffer as a result of you not promptly responding to such a notification.
- ensure that all data you provide to us or to any merchant or Payment Initiator that subscribes to PayTo is accurate, up to date and permitted to be disclosed.
- ensure not to use PayTo to send threatening, harassing or offensive messages to the merchant, Payment Initiator or any other person.
- ensure any passwords/PINs needed to access the facilities we provide are kept confidential and are not disclosed to any other person.
- comply with all applicable laws in connection with your use of PayTo.

- ensure that you comply with the terms of any agreement that you have with a merchant or Payment Initiator, including any termination notice periods. You acknowledge that you are responsible for any loss that you suffer in connection with the cancellation or pausing of a Payment Agreement or Migrated DDR Mandate by you which is in breach of any agreement that you have with that merchant or Payment Initiator.
- ensure that you have sufficient funds in your EFT Account to meet the requirements of all your Payment Agreements and Migrated DDR Mandate. Subject to any applicable laws and industry codes, we will not be responsible for any loss that you suffer as a result of your EFT Account having insufficient funds. Please refer to the relevant EFT Account terms and conditions which will apply where there are insufficient funds in your EFT Account.

22.25 If you receive a Payment Agreement creation request or become aware of payments being processed from your EFT Account that you are not expecting, or experience any other activity that appears suspicious or erroneous, please report such activity to us as soon as possible via Internet Banking or Mobile Banking and submit a claim.

We will respond to all claims within 5 business days, and if the claim is founded, we will refund your EFT Account. We will not be liable to you for any payment made that was in fact authorised by the terms of your Payment Agreement or Migrated DDR Mandate.

22.26 If you use a smartphone to do your banking, we recommend that you allow notifications from us on your Mobile device (by enabling notifications on your Mobile device settings) so that you may receive and respond to Payment Agreement creation requests, amendment requests and other notifications in a timely way. (See “Notifications on your Mobile Banking Device” in Section 3.)

22.27 You acknowledge that PayTo functionality may be unavailable due to outages. Where we are unable to process your request (e.g. to cancel, amend or pause your Payment Agreement), we will notify you this in Internet or Mobile Banking, and you may need to contact your merchant or Payment Initiator to action your request.

Our responsibilities.

22.28 We will accurately reflect all information you provide to us in connection with a Payment Agreement or a Migrated DDR Mandate in the Mandate Management Service.

22.29 In addition to any other rights we may have to refuse a service, we may monitor your Payment Agreements or Migrated DDR Mandate for misuse, fraud and security reasons. You acknowledge and consent to us pausing or cancelling all or some of your Payment Agreements or Migrated DDR Mandate if we reasonably suspect misuse, fraud or security issues. We will promptly notify you of any such action to pause or cancel your Payment Agreement via Internet Banking, Mobile Banking, or email.

Intellectual property relating to PayTo.

22.30 All intellectual property, including but not limited to the PayTo trademarks and all documentation, remains our property, or that of our licensors (our Intellectual Property). We grant to you a revocable royalty free, non-exclusive licence (or where applicable, sub-licence) to use our Intellectual Property for the sole purpose of using PayTo in a way that is consistent with these Terms and Conditions.

22.31 Where an intellectual property infringement claim is made against you, we will have no liability to you under this agreement to the extent that any intellectual property infringement claim is based upon:

- modifications to our Intellectual Property by or on behalf of you in a manner that causes the infringement;

- use of any item in combination with any hardware, software or other products or services in a manner that causes the infringement and where such combination was not within the reasonable contemplation of the parties given the intended use of the item; your failure to use corrections or enhancements to our Intellectual Property that are made available to you (except where the use of corrections or enhancements would have caused a defect in PayTo or would have had the effect of removing functionality or adversely affecting the performance of PayTo); and
- your failure to use our Intellectual Property in accordance with these Terms and Conditions.

Privacy.

22.32 To help reduce the chances of mistaken payments, a person will be able to view your PayID and certain details linked to it (such as your name) when they use your PayID.

You agree to the disclosure and use of your personal information by, and to, participating financial institutions, users of PayID payment services, and the providers of the PayID payment facilities (including NPP Australia Limited and BPAY) and their service providers. If you do not agree, we will not be able to offer PayID payment facilities to you.

By confirming a Payment Agreement and/or permitting the creation of a Migrated DDR Mandate against your EFT Account, you authorise us to collect, use, disclose and store (among other information):

- your name and EFT Account details;
- details of your Payment Agreement(s) and Migrated DDR Mandate; and/or
- other personal information (including sensitive personal information such as health information); (together, the Details), in the Mandate Management Service, for the purposes of:
  - creating payment instructions and messages, and
  - enabling us to make payments from your EFT Account.

You acknowledge that the Details (including sensitive information) may also be:

- disclosed to the financial institution or payment processor for the merchant or Payment Initiator; and
- contained in Payment Agreements that may be viewed and managed by joint account holders and any nominated signatories to the EFT Account.

Any personal information or data you provide to the merchant or Payment Initiator will be subject to the privacy policy and terms and conditions of the relevant merchant or Payment Initiator.

Section 6 – Verify with Confirmation of Payee service.

23. Verify with Confirmation of Payee service.

25.1 The Verify with Confirmation of Payee service allows you to check the name of the person or business you intend to pay matches the name on the account. **Verify with Confirmation of Payee terms and conditions** apply, available on **banksa.com.au** by searching 'Verify with Confirmation of Payee'.

Section 7 – Alerts Services.

24. Alerts Services.

24.1 Where Alerts Services are available for your EFT Account, you can set up an Alerts Service for that EFT Account using Internet Banking. Once you are set up, we will provide you with information regarding your EFT Account by SMS or email or any other method of transmission as agreed between you and us to your Electronic Equipment. If you have a Mobile Banking Device, we can send Alerts Service communications to your Mobile Banking Device as a notification under clause 9.9.

24.2 All communications sent via the Alerts Service to the contact details registered by you with us (your Contact Details) will be deemed to be delivered to you at the time when the communication was sent by us. If in our opinion communications sent to your Contact Details have failed to reach you we may in our sole discretion stop sending further communications.

24.3 By creating an Alert you agree that communications sent to you as part of the Alerts Service do not have to contain a functional unsubscribe facility, and you acknowledge your consent to us supplying you with the communications you have nominated and applied for as part of the Alerts Service.

24.4 It is your responsibility to obtain and maintain any Electronic Equipment which you may need to have for you to use the Alerts Service. You should ensure that your Electronic Equipment is capable of receiving the Alerts Service messages you request from us.

24.5 You should not reply to any Alerts Service as we will not read or respond to such messages from you.

24.6 We may, acting reasonably, suspend or terminate the Alerts Service without notice to you for reasons such as invalid data, nominated EFT Account closure, insufficient funds within the nominated EFT Account, overdue payment, breakdown, maintenance, modification, expansion and/or enhancement work caused or initiated by a telecommunications company concerned in relation to their network or by any service provider in respect of the Alerts Service.

24.7 We will make reasonable efforts to ensure that the Alerts Service is provided on time and that the information we make available to you through the Alerts Service is correct. However, we do not guarantee the accuracy or delivery of an Alerts Service message sent to you.

Liability.

24.8 In relation to the Alerts Service, we are not liable or responsible for any loss, damage or other consequence arising out of or in connection with:

(a) any failure or delay in transmitting information to you;

(b) any error or inaccuracies in the information provided to you; or

(c) your act or omission to perform an instruction or undertake an action relating to the Alert or notification transmitted to you,

unless the loss, damage or consequence is as a direct result of our negligence or wilful default. Without limiting this clause, we are not liable or responsible for any loss or damage or the consequence arising out of or in connection with failure of your Electronic Equipment to receive information or the breakdown, failure, malfunction, interruption or incompatibility of telecommunications, equipment or installation.

Alert Services fees & charges.

24.9 Fees may be charged for each Alert. Please see the EFT Account terms and conditions (incorporating fees and charges) for your applicable EFT Account.

Section 8 – Telegraphic Transfers.

25. Telegraphic Transfer terms and conditions.

25.1 Where Telegraphic Transfers are available for an EFT Account, you may instruct us to transfer an amount to a beneficiary's account held at a financial institution overseas. A Telegraphic Transfer may be in Australian dollars or a foreign currency.

25.2 Amounts sent as a Telegraphic Transfer will usually be available to the beneficiary within 48 hours of your instructions being processed by us. However, in some circumstances a Telegraphic Transfer may take longer, such as where an amount is to be transferred to a place that is not a major financial centre.

25.3 If you instruct us to transfer an amount in a foreign currency, we will convert the Transfer Amount to Australian dollars using the retail exchange rate we make available for the foreign currency on that day. We will tell you details of the conversion (including the exchange rate, the foreign currency amount and converted Australian dollar amount) at the time you instruct us to make the transfer.

25.4 The services of other financial institutions may be used to carry out a Telegraphic Transfer. We may receive commissions or other benefits from other financial institutions.

25.5 In many cases, other financial institutions involved in carrying out a Telegraphic Transfer (such as the beneficiary's Financial Institution or an intermediary financial institution) will impose fees and charges. Such fees and charges will be deducted from the transferred amount (reducing the amount that will be transferred to the beneficiary).

25.6 Fees and charges imposed by other financial institutions are beyond our control. Unless you pay them at the time you request us to make a Telegraphic Transfer, any amount charged by another financial institution involved in carrying out a Telegraphic Transfer will be deducted from the Transfer Amount.

> In some limited circumstances it may be possible to stop or cancel a Telegraphic Transfer. If you want to attempt to stop or cancel a Telegraphic Transfer you must contact us as soon as possible by visiting a branch, or calling the Internet & Phone Banking Helpdesk, 24 hours a day, seven days.

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

25.8 If we are able to stop or cancel a Telegraphic Transfer:

(a) any fees and charges payable by you will usually be deducted from the amount refunded;

(b) where the amount to be transferred was in a foreign currency, we will convert the amount to be refunded to Australian dollars using an exchange rate we determine (this exchange rate will usually be different from the exchange rate used at the time you instructed us to make the Telegraphic Transfer).

27.9 Delays or errors in the transmission of a Telegraphic Transfer may be caused by matters beyond our control, such as the acts or omissions of another financial institution involved in carrying out the Telegraphic Transfer.

25.10 We collect your personal information in order to process your request and to comply with legal requirements, including anti-money laundering laws. If you do not give us all the personal information we require, we may not be able to make the payment you have requested. You may request access at any time to personal information held by us about you and ask us to correct it if you believe it is incorrect or out of date by calling our Customer Contact Centre or visiting one of our branches. We may disclose your personal information:

(a) to other financial institutions (including overseas financial institutions) and to the beneficiary, for the purposes of carrying out the transfer;

(b) to our external service providers that provide services for the purposes only of our business, on a confidential basis;

(c) if you request us to do so, or if you consent, or where the law requires or permits us to do so.

If you have provided information about another individual, you declare that the individual has been made aware of that fact and the contents of this clause.

25.11 Telegraphic Transfers may be subject to specific country, currency and minimum value restrictions. Please log in to Internet Banking for notification of any restrictions that may be relevant to your intended payment/s. These restrictions and conditions are subject to change from time to time at our discretion.

25.12 We may credit an inward Telegraphic Transfer to your account prior to us receiving the payment value from the sender's bank. If, after crediting your account, we do not receive the payment value from the sender's bank or correspondent bank, then we may debit that payment amount in full from your account, where there are sufficient available funds to do so, before we have resolved this matter with the sender's bank. Should we be able to resolve any non-payment by the sender's bank and we subsequently receive the payment value from the sender's bank, we will credit your account with the amount received.

Section 9 – General matters.

26. Security of your Internet and Phone Banking Access Codes.

26.1 You can:

- change your Internet and Phone Banking Security Number when you use Phone Banking; and
- change your Internet and Phone Banking Security Number and Internet Banking Password when you use Internet Banking.

For your security, we recommend that you use an Internet and Phone Banking Security Number and an Internet Banking Password that are unrelated to any of your ATM/EFTPOS PINs and that you can remember without writing it down.

It is highly recommended that you use an Internet Banking Password that is different from any other passwords you use for online services.

26.2 The security of your Access Codes (including your Internet and Phone Banking Security Number and Internet Banking Password or Secure Code, and any Mobile Banking Device) is very important. They can be used to access information about you and your EFT Accounts. They can be used to ask us to perform transactions on each EFT Account. You must make every effort to ensure that your Access Codes, and any record of them, are not misused, lost or stolen.

If we suspect the security of your Access Codes has been compromised, we will contact you and require you to change them.

If you fail to ensure the security of your Access Codes your liability for unauthorised transactions will be determined under clause 27.

Your obligations.

You must:

(a) not record your Internet and Phone Banking Security Number or Internet Banking Password or Secure Code on the computer or telephone that you use to access Internet or Phone Banking or your Mobile Banking Device;

(b) not record your Internet and Phone Banking Security Number or Internet Banking Password on any item that identifies your Internet and Phone Banking Customer Access Number or Internet Banking Password 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 Internet and Phone Banking Security Number or Internet Banking Password;

(d) not disclose your Internet and Phone Banking Security Number or Internet Banking Password or Secure Code or make them available to any other person (including a joint account holder, a family member, a friend or one of our staff);

(e) use care to prevent anyone else seeing your Internet and Phone Banking Security Number or Internet Banking Password being entered into any Electronic Equipment.

If you have a Mobile Banking Device, you must:

(f) not lose possession of your Mobile Banking Device, and let us know promptly if you do;

(g) use password or passcode protection for the Mobile Banking Device and not disclose the password or passcode;

(h) not leave your Mobile Banking Device unattended and left logged into Mobile Banking;

(i) lock your Mobile Banking Device or take other steps necessary to stop unauthorised use of Mobile Banking; and

(j) (where the Mobile Banking Device uses biometric information, such as a fingerprint logon, to unlock), not allow any other person's biometric information be a method for unlocking the Mobile Banking Device.

Can you record a memory aid for your Internet and Phone Banking Access Codes?

26.3 If you require a memory aid to recall your Internet and Phone Banking Security Number or your Internet Banking Password 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 Internet and Phone Banking Security Number or Internet Banking Password on any item that identifies your Internet and Phone Banking Customer Access Number;

(b) not to record your disguised Internet and Phone Banking Security Number or Internet Banking Password on the computer or telephone that you use to access Internet or Phone Banking;

(c) not to disguise your Internet and Phone Banking Security Number or Internet Banking Password by reversing the number sequence;

(d) not to describe your disguised record as an "Internet and Phone Banking Security Number record" or "Internet Banking Password record" or similar;

(e) not to disguise your Internet and Phone Banking Security Number or Internet Banking Password using alphabetical characters or numbers: A=1, B=2, C=3, etc;

(f) not to select or disguise your Internet and Phone Banking Security Number or Internet Banking Password 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 benefit numbers; or

(vi) licence numbers; and

(g) not to store your Internet and Phone Banking Security Number or Internet Banking Password in any low security electronic device of any kind, such as (but not limited to):

(i) mobile telephones;

(ii) personal computers; or

(iii) electronic organisers.

26.4 There may be other forms of disguise that may also be unsuitable because of the ease of another person working out your Internet and Phone Banking Security Number or Internet Banking Password. You must exercise extreme care if you decide to record a memory aid for your Internet and Phone Banking Security Number or Internet Banking Password. Please note that liability for losses arising from unauthorised transactions is determined under the relevant provisions of the ePayments Code, where the Code applies, despite your obligations in clauses 26.2, 26.3 and 26.4.

If your Internet and Phone Banking Security Number or Internet Banking Password is revealed or you suspect unauthorised transactions.

26.5 You must tell us as soon as possible if you suspect that your Internet and Phone Banking Security Number or Internet Banking Password is known to someone else or you suspect any unauthorised use of it or you suspect that unauthorised transactions have been made.

You may notify us by calling the Internet & Phone Banking Helpdesk, 24 hours a day, seven days.

26.6 If you do not notify us you may be liable for unauthorised use – see clause 27.

26.7 You will need to give us all relevant information you may have, so that we can suspend Internet and Phone Banking access to your EFT Accounts. You must confirm in writing any notice you give us by telephone. A failure to do so will not affect your liability for unauthorised transactions. However, it will help us to effectively deal with your report.

26.8 When you report the matter you will be given a notification number (or other form of acknowledgement). You should retain that number as confirmation of the date and time of your report.

26.9 If you are unable to report to us because our facilities are unavailable you are not liable for any unauthorised transaction that 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.

27. Liability for unauthorised Internet, Mobile and Phone Banking transactions.

27.1 You are not liable for unauthorised Internet and Phone Banking transactions or Mobile Banking transactions if it is clear you did not contribute to losses resulting from those transactions.

Otherwise, your liability for unauthorised Internet and Phone Banking transactions and Mobile Banking transactions will normally be limited to:

(a) $150;

(b) the balance of the EFT Accounts on which the unauthorised transactions were made and to which you have access by Internet and Phone Banking or Mobile Banking (as applicable); or

(c) the actual loss incurred before you notify us under clause 24.5 (excluding that portion of the loss incurred on any one day that exceeds the applicable daily transaction limit), whichever is the smallest amount.

In some circumstances, you may be liable for a greater amount of unauthorised Internet and Phone Banking transactions or Mobile Banking transactions. Please refer to clauses 27.3 and 27.4 for details of those circumstances.

27.2 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 (i.e. providers of goods or services) who are linked to the electronic funds transfer system or of their agents or employees; or

(b) unauthorised Internet and Phone Banking transactions or Mobile Banking transactions (as applicable) which occur after you have given us notice as required by clause 26.5; or

(c) unauthorised transactions before you receive your Internet and Phone Banking Security Number; or

(d) any Device, Identifier or Code that is forged, faulty, expired or cancelled; or

(e) unauthorised transactions that can be made using an Identifier without a Device or a Code; or

(f) unauthorised transactions that can be made using a Device and not a Code, provided the User did not unreasonably delay in reporting the loss or theft of the Device; or

(g) the same transaction being incorrectly debited more than once to the same account.

Note: Electronic Equipment that you supply, such as a computer or a Mobile Banking Device, is not a 'Device' mentioned in this clause if we do not originally supply it to you.

When you will be liable for actual losses resulting from an unauthorised transaction.

27.3 If you have contributed to the unauthorised use because you:

(a) engaged in fraud;

(b) voluntarily disclosed your Internet and Phone Banking Security Number or Internet Banking Password to anyone, including a family member or friend or gave them access to Mobile Banking through your Mobile Banking Device;

(c) indicated your Internet and Phone Banking Security Number or Internet Banking Password on any item that identifies your Internet and Phone Banking Customer Access Number;

(d) kept a record of your Internet and Phone Banking Security Number or Internet Banking Password (without making any reasonable attempt to disguise the Internet and Phone Banking Security Number or Internet Banking Password) with any article carried with any item that identifies your Internet and Phone Banking Customer Access Number or that is liable to loss or theft simultaneously with that item;

(e) selected an Internet and Phone Banking Security Number or Internet Banking Password which represents your birth date or an alphabetical code which is recognisable as part of your name immediately after you were specifically instructed not to select such an Internet and Phone Banking Security Number or Internet Banking Password and warned of the consequences of doing so; or

(f) act with extreme carelessness in failing to protect the security of your Internet and Phone Banking Security Number or Internet Banking Password or Mobile Banking 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 your Internet and Phone Banking Security Number or Internet Banking Password or Mobile Banking Device has been breached or we are notified of the existence of unauthorised transactions;

(ii) the funds available in your EFT Accounts 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.

27.4 You will be liable if you have contributed to the unauthorised transactions because you unreasonably delayed in notifying us that any applicable Device (or your Mobile Banking Device) has been lost, misused or stolen or your Internet and Phone Banking Security Number and/or Internet Banking Password has become known to someone else.

You will be liable for any losses directly attributable 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 became aware (or should reasonably have become aware) of the events described above and the time we were actually notified;

(b) the funds available in your EFT Accounts, 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.

27.5 Your liability for losses from unauthorised 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 a relevant card scheme against any other party to the card scheme (whether or not that claim or other right is actually exercised). Refer also to the EFT Account terms and conditions.

27.6 If more than one Access Code (for example Internet and Phone Banking Security, Internet Banking Password or any similar information) that a User is required to keep secret to make an EFT Transaction is used to make an EFT Transaction, and we prove that a User 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 probabilities, that the breach of the security requirements was more than 50% responsible for the losses.

27.7 You will not be liable under clauses 27.3 or 27.4 for losses incurred on any accounts which we had not agreed could be accessed using an applicable Device or Identifier and/or your Internet and Phone Banking Security Number and Internet Banking Password, or Mobile Banking Device as applicable. Your liability under clause 27.4 is also subject to us proving on the balance of probability that you contributed to the loss in one or more of the ways described in clause 27.4.

28. Electronic banking system malfunction.

28.1 Please tell us about any service fault or difficulty with our Internet and Phone Banking service by calling the Internet & Phone Banking Helpdesk, 24 hours a day, seven days.

28.2 We are responsible for loss caused by the failure of our Electronic Equipment or the EFT System to complete a transaction accepted by our Electronic Equipment or the EFT System in accordance with your instructions.

28.3 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 should reasonably have been aware that the equipment or the 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.

28.4 We will correct the loss by making any necessary adjustment to the appropriate account (including adjustment of interest or fees as a result of the malfunction).

29. Mistaken Internet Payments.

29.1 This clause does not apply to BPAY payments. See Section 4 of these terms for information about BPAY payments. This clause does not apply to Telegraphic Transfers sent outside of Australia. See Section 8 of these terms for information about Telegraphic Transfers.

Reporting mistaken internet payments.

29.2 You should report mistaken internet payments to us as soon as possible after you become aware of them. You can report mistaken internet payments to us by visiting one of our branches or by calling our Customer Contact Centre.

We will give you a notification number or some other form of acknowledgment 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 "Feedback and Complaints" section of this document.

Dealing with mistaken internet payments.

29.3 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 29.4 to 29.6 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.

Not withstanding 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 Departments 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.

29.4 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 transaction is made:

(a) **Where the report is made within 10 Business Days of the payment:**

(i) 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.

(b) **Where the report is made between 10 Business Days and 7 months of the payment:**

(i) The receiving institution will investigate the payment and complete the investigation within 10 Business Days of receiving a request.

(ii) 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.

(iii) 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).

(c) **Where a report is made after 7 months of payment:**

(i) 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.

29.5 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.

29.6 Where:

- both we and the sending institution are satisfied that a payment made to your account is a mistaken internet payment; and
- sufficient credit funds are available in your account to the value of that payment; and
- the mistaken internet payment is reported 7 months or less after the payment; and

- 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 29.4 (b) (i),

we will, without your consent and in accordance with the ePayments Code, 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 29.4.

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 or losses arising from internet payments.

29.7 You must ensure that internet payment details are correct. You and your User are 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.

30. Industry codes.

30.1 The Australian Banking Association's banking code of practice as updated, and adopted by us, from time to time (**Banking Code**) sets out the standards of practice and service in the Australian banking industry for individuals and small business customers, and their guarantors who are individuals.

The relevant provisions of the Banking Code apply to the banking services referred to in this document. This means that we will comply with the Banking Code, where it applies to the banking services provided to you.

You can view a copy of the Banking Code of Practice on our website or contact us for assistance.

30.2 We warrant that we will comply with the ePayments Code, where it applies.

31. Changes to the Terms and Conditions.

31.1 The Terms and Conditions can be changed by us at any time.

31.2 We will give notice of any change to the Terms and Conditions in accordance with the times set out in the table in clause 31.3, and in the manner described in clause 32.

However, advance notice may not be given where a change is required to immediately restore or maintain the security of a system or individual facility, including the prevention of systemic or individual criminal activity, including fraud. We can also give you a shorter notice period (or no notice) if we believe that it is necessary to avoid, or to reduce, a material increase in our credit risk or our loss.

31.3

Type of change or event	Notification we will give you
A. If we: (a) introduce a new fee or charge in relation to the use Internet, Mobile and Phone Banking, BPAY, and related services (other than a government fee or charge, see clause 32.4); (b) increase any fee or charge in relation to the use Internet, Mobile and Phone Banking, BPAY, and related services (other than a government fee or charge, see clause 32.4); (c) in relation to an EFT Transaction: (i) impose or increase charges relating solely to the use of an Access Method or for the issue of an additional or replacement Access Method; (ii) increase your liability for losses relating to EFT Transactions; or (iii) vary the daily or periodic transaction limits on the use of an Access Method, EFT Account or Electronic Equipment.	At least 30 days before the change takes effect.
B. If we make any other change	As soon as reasonably possible (which may be before or after the change is made) or, if we believe the change is unfavourable to you, at least 30 days before the change takes effect.
C. The introduction of, or change to, a government fee or charge that is payable directly or indirectly by you	In advance of the change, or reasonably promptly after the government, a government agency or representative body notifies us, unless the change has been published by the government, a government agency or representative body.

32. Communications.

32.1 We will notify you of changes to these Terms and Conditions in writing, either directly, by media advertisement or electronically in accordance with the provisions of the ePayments Code (see clause 32.5).

32.2 If we give a written notice directly, we will send it to the most recent address you have given us. You must promptly inform us of any change to your contact details. Where we send a written notice by ordinary mail, we will regard that notice as given 5 Business Days after we post it.

32.3 If we give a written notice directly and you are the holder of an EFT Account that is a joint account, and all account holders live at the same address, you agree that one account holder will be appointed the agent of the other account holders for the purposes of receiving communications from us. This means that only one copy of the notice will be sent and it will be considered to have been received by all joint account holders.

32.4 If the Government introduces or changes a government charge payable directly or indirectly by you, we will notify you in writing, electronically or through media advertisement unless the introduction or change is publicised by a government, government agency or representative body. You agree to receive notice in these ways.

32.5 In accordance with the ePayments Code, we may use electronic means to communicate with you. For example, we may use your email address to send you electronic notices, including changes to these Terms and Conditions or send you an email communication to tell you the changes are available for viewing within Internet Banking or on a website.

32.6 When the nature of the changes to the terms and conditions would require us to provide a summary of the changes to the terms and conditions or an updated version of the terms and conditions we will do so.

33. Appropriate use of our services.

33.1 Your use of the services we provide must not breach any law of Australia or any other country.

33.2 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 Westpac 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.

34. Trade practices.

Nothing in these terms and conditions has the effect of excluding, restricting or modifying any rights that by law cannot be excluded, restricted or modified.

35. GST.

35.1 We tell you if any fees we charge you are GST inclusive.

35.2 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.

35.3 We will tell you of any additional GST amount you must make on a payment.

36. Fees and charges.

Any fees and charges payable for your use of Internet and Phone Banking are set out in the EFT Account terms and conditions. Information about fees and charges is available on request.

37. Assignment.

You cannot assign your rights under the Terms and Conditions.

38. Feedback and Complaints.

Delivering on our service promise.

We're constantly striving to provide the best possible service, and we'll do our best to resolve any concern you have efficiently and fairly.

Our commitment to you.

If you're ever unhappy about something we've done – or perhaps not done – please give us the opportunity to put things right.

Our aim is to resolve your complaint within 5 business days, and where possible we will resolve your complaint on the spot. If we need additional time to get back to you, we will let you know. Should we be unable to resolve your concern at your first point of contact, we will then refer the complaint to our dedicated Customer Managers in our Customer Solutions team.

Our Customer Solutions Customer Managers are here to find a solution for you and will ensure that you're regularly updated about the progress we are making to resolve your complaint.

You can contact us:

Over the phone
Please call us from anywhere in Australia on 13 13 76.
If you are overseas, please call +61 2 9155 7850.

By post
BankSA Customer Solutions
Reply Paid 399
Adelaide SA 5001

In Branch
If you prefer to tell us in person, go to our website to locate your nearest branch.

Online
Using the secure feedback form at **eforms.banksa.com.au/olfmu/eforms/ConsumerFeedback/#/welcome**

For further information go to our website and search 'Feedback and Complaints'.

If you are still unhappy.

If you are not satisfied with our response or handling of your complaint, you can contact the external dispute resolution scheme, the Australian Financial Complaints Authority (AFCA).

Australian Financial Complaints Authority.

The Australian Financial Complaints Authority (AFCA) provides a free and independent service to resolve complaints by consumers and small businesses about financial firms (e.g. banks), where that complaint falls within AFCA's terms of reference.

The contact details for AFCA are set out below.

Australian Financial Complaints Authority

Online: **www.afca.org.au**

Email: **info@afca.org.au**

Phone: 1800 931 678 (free call)

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

39. Electronic notices and correspondence.

39.1 This section does not apply to Internet Banking communications provided in accordance with clauses 31 and 32 of these terms and conditions. Clause 32 continues to operate despite any withdrawal of consent from receipt of electronic account communications in accordance with this section.

39.2 You may receive notices, documents and communications electronically for current and future eligible accounts and insurance policy types, including through Internet Banking, instead of having paper documents mailed to you. You can withdraw your consent to receiving documents electronically at any time and revert to paper documents by changing your preferences by account type in Internet Banking. To review the account types, and make any changes, go to your mail settings in the services menu in Internet Banking.

39.3 For some accounts and insurance policy types we can't send documents electronically, including because the law requires some things to be sent by post.

39.4 If you receive notices and communications through Internet Banking we'll send an email to your nominated email address (notification), advising that you have new documents available. It's your responsibility to check your email regularly for these notifications and to access the documents promptly following our email. You must also keep your nominated email address current and let us know if you can't access your email or Internet Banking for any reason. While you are receiving documents through Internet Banking, you can't opt out of receiving these notifications; however you can change your nominated email address at any time.

39.5 You will be able to print or download the documents provided electronically through Internet Banking for up to 18 months. Once the documents are no longer available through Internet Banking, they will continue to be available to you (for up to 7 years from their creation) by contacting us.

40. Privacy Statement and Consent Request.

Privacy Statement.

Our Privacy Statement explains how we collect, use and disclose your personal information and credit-related information. Our Privacy Statement also provides information about how you can access and correct your personal information, and make a complaint and is available at **banksa.com.au/privacy/privacy-statement** or by calling us on 13 13 76.

In certain circumstances, additional documents might also apply to our collection, use and disclosure of your personal information (including sensitive information).

- If you verify your identity electronically, our Electronic Verification Notice contains further information about how we collect, use and disclose your personal information.
- If you require additional support to do your banking, our Vulnerable Customer Notice contains further information about how we collect, use and disclose your personal information (including sensitive information).
- If you make a hardship application, our Hardship Information Collection Notice contains further information about how we collect, use and disclose your personal information (including sensitive information).

Marketing communications.

We will use your personal information to send you offers for products and services we believe may be of interest and value to you (including by email, SMS or other means) unless you have previously told us that you do not want to receive marketing offers from us. The products and services offered may be provided by us or one of our third-party partners. If you do not want to receive direct marketing offers from us, you can manage your marketing preferences in your online banking profile, let us know using the contact details in our Privacy Statement or follow the opt-out instructions in the message.

41. Duty of Confidentiality.

BankSA has a general duty of confidentiality towards you, except in the following circumstances:

- where disclosure is compelled by law;
- where there is a duty to the public to disclose;
- where the interests of Westpac Group require disclosure;
- where disclosure is made with your express or implied consent.

42. Technical and other information.

We may also collect technical information to help us detect security threats and for fraud analysis and prevention. Such technical information may include information about your device or computer such as operating system version, how your device or computer connects to our services, your device or computer settings (for example, version, screen size and language settings) and how you interact with your web browser. This information may also be used or stored in combination with your personal information for these purposes, including to enable us to contact you if we detect a security threat.

Internet Banking and Mobile Banking.

When you use Internet Banking or Mobile Banking, we may collect, store and retain information from your device or computer, including your device ID, your location information, certain preferences, settings and information about apps installed on your device to verify that you are using a trusted device, your use of

the Internet Banking or Mobile Banking (including transactions), or to monitor your device or computer for security purposes. Location information is also used to customise the look and feel of the Mobile Banking App.

To access some services within the Mobile Banking App, we may need to request access to certain features on your device. If we cannot access certain features, we may not be able to provide the service you requested.

We may access a range of features on your Mobile Device including:

- your biometrics stored on the mobile device to logon to the Mobile Banking App with **supported devices**
- contact information stored on your device to make a payment or to send a payment notification (e.g. a phone number)

We may also collect general statistics in relation to your activity. This data is used to improve your experience on the Mobile Banking App and our products and services.

Cookies.

The Westpac Group uses cookies to secure and tailor your Internet Banking and Mobile Banking experience. **Learn more** about why we use cookies and how to manage them.

Who do we share your personal information with?

We may share your personal information with companies within the Westpac Group, our partners and third parties (some of which are located outside of Australia or the EEA).

Further information.

For more details on how we collect, hold, use and disclose your personal information please see our Privacy Statement which is available at banksa.com.au/privacy/privacy-statement or overseas privacy and data protection policies.

Contact us.

If you are not satisfied with how we may handle your personal information or you would like to make a complaint you can contact: our Privacy Officer by, calling 13 13 76, using the **Feedback Form** or writing to us at Reply Paid 5265, Sydney NSW 2001.

43. Meaning of words.

"Access Codes" means a code or other secure procedure you can use to access Internet and Phone Banking or Mobile Banking, including:

(a) your Internet and Phone Banking Customer Access Number;

(b) your Internet and Phone Banking Security Number;

(c) your Internet Banking Password;

(d) your Mobile Banking Device (and any passwords or access codes used to unlock that Mobile Banking Device); and

(e) any Secure Code we may send you.

"Access Method" means a method we authorise you to use to instruct us through Internet and Phone Banking and Mobile Banking in respect of an EFT Account.

It comprises the use of one or more components including an Internet and Phone Banking Security Number, Internet and Phone Banking Customer Access Number or Internet Banking Password or Mobile Banking Device or combinations of these.

It does not include a method requiring your manual signature as the main way in which we ensure you gave us an instruction.

"account holder" means the person(s) in whose name the relevant Cardless Cash Account is held and who is responsible for all transactions on the account.

"Accredited Data Recipient" is as defined in the *Competition and Consumer Act 2010*.

"Alerts Service" means the provision of information regarding your EFT Account by SMS (SMS Alert) or email (Email Alert) or any other method of transmission as agreed between you and us to your Electronic Equipment.

"At Risk Transaction" means an Internet Banking transaction or request identified by us as requiring further authentication by our Secure Code Service to complete that transaction.

"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 Service" means any Internet Banking or Phone Banking service to which these terms and conditions apply.

"BankSA" means the Division of Westpac Banking Corporation ABN 33 007 457 141 AFSL and Australian credit licence 233714

"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.

"BPAY Pty Ltd" means BPAY Pty Ltd ABN 69 079 137 518.

"BPAY Scheme" means the scheme described in Section 4.

"Business Day" means a day we are open for business, but does not include Saturday, Sunday or any public holiday.

"card" means:

(a) any authorised card issued by us for your EFT Account or which we allow you to link to your EFT Account; and

(b) includes any corresponding card that is loaded onto Electronic Equipment (such as a Mobile Banking Device) for the purpose of making a contactless transaction, and, for the purpose of these terms and conditions, each of (a) and (b) are considered to be one and the same card.

"Cardlink Services Limited" means Cardlink Services Limited ABN 60 003 311 644.

"contactless terminal" means Electronic Equipment (such as a merchant terminal) which can be used to make a contactless transaction.

"contactless transaction" means a transaction made by holding your card or Mobile Banking Device (which is capable of making a contactless transaction) in front of a contactless terminal.

"Device" means an article we give to a User to perform EFT Transactions.

"Direct Debit" has the meaning given to the term 'Direct Debit Request' in the BECS Procedure available at **auspaynet.com.au/resources/direct-entry**

"EFT Account" means an account for which we agree you may give us instructions or access account information using Internet and Phone Banking.

"EFT System" means the network of electronic systems used for the transmission of EFT Transactions.

"EFT Transaction" means a transfer of funds initiated by an instruction you give through Electronic Equipment to debit or credit an EFT Account.

"Electronic Equipment" includes a computer, terminal, television, fax, telephone, or any other equipment which is capable of creating, receiving or displaying information sent or to be sent via SMS, email or any other method of transmission.

"Email" means Electronic Mail Message.

"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 a User knows and must provide to perform an EFT Transaction but is not required to keep secret.

"Including" or **"such as"** or **"for example"** 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.

"Internet and Phone Banking" means any service we offer from time to time through a communication network (including the internet and telephone) to enable you to receive information from us and to transmit instructions to us electronically in relation to an EFT Account, or other matters we specify.

"Internet and Phone Banking Customer Access Number" means the number used in conjunction with the Internet and Phone Banking Security Number and Internet Banking Password to access Internet and Phone Banking.

"Internet and Phone Banking Security Number" means the personal identification security number used in conjunction with the Internet and Phone Banking Customer Access Number and Internet Banking Password to access Internet and Phone Banking.

"Internet Banking" means any service we offer from time to time through a communication network (including the internet and telephone) to enable you to receive information from us and to transmit instructions to us electronically in relation to an EFT Account, or other matters we specify, including Mobile Banking (unless expressly stated otherwise) but excludes Phone Banking.

"Internet Banking Password" means the password you select for use in conjunction with the Internet and Phone Banking Customer Access Number and the Internet and Phone Banking Security Number to access Internet Banking.

"Mandate Management Service" means the central, secure database operated by NPP Australia Limited of Payment Agreements. Payment Agreements must be recorded in the Mandate Management Service to process NPP payments.

"Migrated DDR Mandate" means existing Direct Debit arrangements which have been converted into Payment Agreements in order to process payments under those arrangements via the NPP rather than BECS (the Bulk Electronic Clearing System).

"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) or 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 or PayID. This excludes payments made as a result of a scam.

"Mobile Banking" means a service we offer from time to time through an internet protocol telecommunications network to enable you to access information about EFT Accounts and transmit instructions to us electronically through the Mobile Banking App and a mobile device.

"Mobile Banking App" means software approved by us in connection with mobile banking and downloaded directly to your mobile device from the App store that is appropriate to your mobile device.

"Mobile Banking Device" means a mobile device, to which you have loaded the BankSA Mobile Banking App and which you have registered to access your EFT Accounts using Mobile Banking.

"mobile device" means Electronic Equipment provided by you (such as a smartphone), capable of running the Mobile Banking App.

"Mobile Phone Number" means the telephone number associated with a mobile device.

"Nominated Representative" means an individual who has been authorised to engage in Open Banking data sharing on behalf of an Organisation.

"NPP" means the New Payments Platform operated by NPP Australia Limited.

"NPP Australia Limited" means NPP Australia Limited ABN 68 601 428 737.

"Open Banking Accounts" means any account held by you with BankSA that is eligible for Open Banking data sharing in accordance with the Consumer Data Right legislation, rules and requirements. This includes accounts that are open, closed and not visible in Internet Banking.

"Open Banking" or **"Consumer Data Right"** refers to the Australian regulatory regime established under PartIVD of the *Competition and Consumer Act 2010* that enables access to information about BankSA's goods or services, and enables disclosure by BankSA of specific data relating to a customer (including both individuals and organisation customers), held by BankSA, to the consumer or to Accredited Data Recipients.

"Organisation" in the context of Open Banking means a business customer (except for sole traders).

"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" means the password or number used in conjunction with your EFT Account and which is not a PIN.

"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 Agreement" means an agreement established by you and an approved merchant or Payment Initiator, by which you authorise us to make payments from your EFT Account via the NPP.

"Payment Cut-Off Time" means the BPAY Payment Cut-Off Time.

"Payment Initiator" means an approved payment service provider who, whether acting on behalf of you or a merchant, is authorised by you to initiate payments from your EFT Account via the NPP.

"PayTo" means the service which enables us to process NPP payments (i.e. electronic payments cleared and settled by participating financial institutions via the NPP) from your EFT Account in accordance with and on the terms set out in a Payment Agreement you have established with a merchant or Payment Initiator that subscribes to the service.

"Phone Banking" means any service we offer from time to time through a telecommunications network to enable you to receive information from us and to transmit instructions to us electronically in relation to an EFT Account, or other matters we specify, using an interactive voice response system. Phone Banking does not include communicating with a member of our staff directly by telephone and does not include Mobile Banking.

"PIN" means a personal identification number used in connection with your card.

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

"Scheduled Payment" means a payment (including a BPAY Payment) or a funds transfer that you request us to make at a later date.

"Secure Code" means a randomly generated code that we send to you to authenticate an At Risk Transaction or to perform some other services. This form of authentication is in addition to your Internet Banking Password and Internet and Phone Banking Security Number.

"Secure Code Service" means our method of Two Factor Authentication where we send you a Secure Code to authenticate an At Risk Transaction performed by you using Internet Banking.

"Small Business" has the same meaning given to it by the Banking Code of Practice.

"SMS" means Short Message Service.

"St.George Banking Group" means the Divisions of Westpac trading as St.George Bank, Bank of Melbourne and BankSA.

"Telegraphic Transfer" means an electronic transfer to an account held with a financial institution outside Australia.

"Transfer ID" means a unique identification number generated by the Mandate Management Service in connection with a request to transfer one or more Payment Agreements.

"Two Factor Authentication" means a security authentication process in which a customer provides a financial institution with two types of identification information to authenticate their identity. The first type of identification information is a piece of information known to the customer. The second type of identification information is information sent by the financial institution to the customer's physical device, e.g. a mobile telephone.

"User" means you or any person authorised by you in accordance with these terms (or other terms with us relating to an EFT account) to perform EFT Transactions, and in relation to a Cardless Cash transaction means a person(s) authorised by you to perform the Cardless Cash transaction.

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

"Westpac Group" means Westpac Banking Corporation ABN 33 007 457 141 AFSL and Australian credit licence 233714 and its related bodies corporate.

"Westpac Group partner ATM" refers to a third party ATM operator who Westpac has an arrangement with. The available ATM locations can be found on our website at the ATM locator **banksa.com.au/locator** or via the BankSA Mobile Banking App.

"you" means the user of Internet banking, Phone Banking and Mobile Banking.

Unless otherwise specified, a reference in the Terms and Conditions:

- to a time is a reference to that time in Sydney.
- to a dollar amount means that amount in Australian Dollars.

BankSA is a shareholder of Australian Payments Plus Ltd, a public company limited by shares, and has a director on the board of Australian Payments Plus. Australian Payments Plus is a member based organisation operating Australia's three domestic payment schemes, BPAY, eftpos and the New Payments Platform. BankSA has policies and procedures in place to manage any actual, potential and perceived conflicts of interest.

BankSA acknowledges the Traditional Owners as the custodians of this land, recognising their connection to land, waters and community. We pay our respects to Australia's First Peoples, and to their Elders, past and present.

PayID and PayTo are registered trademarks of NPP Australia Limited.

Osko and BPAY are registered trademarks of BPAY Pty Ltd ABN 69 079 137 518. © BankSA – A Division of Westpac Banking Corporation ABN 33 007 457 141 AFSL and Australian credit licence 233714. WBCBSA02715 0726