St.George Internet and Phone Banking

Terms and Conditions and
Important Information.

Effective 21 February 2017

st.george start something

This document sets out terms and conditions for St.George 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 **stgeorge.com.au**

Contents

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 to process payments and transfers to accounts held with financial institutions other than St.George. Please make sure any BSB and account number 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 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

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), or a Collection Code Pay to Mobile Payment, 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, Telegraphic Transfer, or a Collection Code Pay to Mobile Payment 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.

Table A

Daily limits on total transactions (excludes Maxi Saver, DIY Super Saver, Business Access Saver, Direct Saver, DIY Super Direct Saver, Express Saver, Express Saver for Business and redraws)	
Daily limits on transfers and payments from accounts	
Limit on total transfers and payments each day from one or more of your accounts linked to your Internet and Phone Banking facility.	$1 million*
Additional limits for personal customers transferring funds or making payments from one or more business accounts:	
(a) Limit on total transfers each day to one or more business accounts; and	$25,000
(b) Limit on total of all other transfers and payments from one or more business accounts.	$25,000
Daily limits on specific activities *(These transactions are also counted towards your Daily limits on transfers and payments from accounts above.)*	
Limit on total amount each day in bank cheques.	$25,000
Limit on total amount each day in Telegraphic Transfers.	$50,000 (AUD)
Limit on total amount transferred each day to one or more credit card accounts linked to your Internet and Phone Banking facility (other than by BPAY Payments).	$25,000
Limit on total BPAY Payments each day to one or more BPAY Billers that we consider to be low risk.	$100,000
Limit on total BPAY Payments each day to one or more BPAY Billers that we consider to be high risk.	$15,000
For the payer of a Pay to Mobile Payment – Limit on total Pay to Mobile Payments up to a maximum number each day.	$1,000 to a maximum of 10 transactions
For a Pay to Mobile Recipient – Limit on total Pay to Mobile Payments that can be claimed using a Collection Code from the one payer each day. For a Pay to Mobile Recipient – Limit on total Pay to Mobile Payments that can be claimed from the one payer each day.	$1,000
Limit on total of payments each day to one payee account that is not linked to your Internet Banking facility, and where you have provided the payee account details (or Australian mobile number) using Internet Banking. ▪ For the payer of a Pay to Mobile Payment, a Pay to Mobile Payment that is processed as a Straight Through Payment is counted towards this limit. ▪ For a Pay to Mobile Payment Recipient, the amount claimed in a Pay to Mobile Payment using a Collection Code is counted towards this limit.	$5,000 A limit of $25,000 can be requested and approved
Limit on total of payments to payee accounts that are not linked to your Internet Banking facility, and where you have provided the payee account details (or Australian mobile 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 total of payments each day to one or more payee accounts that are not linked to your Internet and Phone Banking facility, and where you have provided the payee account details using a hard copy form we provide.	$100,000

* If you have a BT Super For Life Account differing statutory limits may apply. Please refer to the Product Disclosure Statement for that product for more information.

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

Table B

Daily limits on total transactions Direct Saver#, Maxi Saver, DIY Super Saver, Business Access Saver, DIY Super Direct Saver#, Express Saver#, Express Saver for Business# and redraws (subject to us approving your request)	
Daily limits on transfers from accounts	
Limit on total transfers each day from one or more Maxi Saver, Business Access Saver, Direct Saver, Express Saver or Express Saver for Business accounts.	$2 million
Limit on total transfers each day from each DIY Super Saver and DIY Super Direct Saver account.	$2 million
Limit on total redraws each day from one or more home loans (excluding Get Set and Portfolio Loans).	$30,000 (min amount $1)
Limit on total redraws each day from one or more personal loans.	$30,000 (min amount $500)

Accounts no longer offered.

Table C

Limits on individual transactions	
Maximum amount for each Pay to Mobile Payment.	$250
Tap & Pay contactless transaction limit without card PIN (except where the merchant has set the limit at the merchants' contactless terminal).	$99.99
Maximum amount for each bank cheque.	$5,000
Maximum amount to transfer to a payee account that is not linked to your Internet Banking facility, and where you have provided the payee account details using Internet Banking. This amount is also the total amount of all transfers that can be made to a payee account each day. Refer to Table A for details on this limit and the daily limit applicable to all transfers to payee accounts.	$5,000 A limit of $25,000 can be requested and approved
Maximum amount for each transfer to a Direct Saver or DIY Super Direct Saver, Express Saver or Express Saver for Business account from a Linked Account, where the Linked Account is held at a financial institution other than St.George.	$5 million*
For transactions that we consider to be an At Risk Transaction, we may require you to authenticate the transaction using our Secure Code Service.	

* The financial institution with whom the Linked Account is held may impose a lower limit.

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

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 7 – 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 (even if you do not give us a Mobile Phone Number at that time). 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.

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 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

2.5 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 bank cheques and Telegraphic Transfers;
- opening a range of accounts;
- viewing and transferring funds between your BT Super for Life superannuation account; and
- viewing bills online through BPAY View

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 are available for all EFT Accounts. See the EFT Account terms and conditions for further information.

2.6 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.

2.7 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 stgeorge.com.au.

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 to process payments and transfers to accounts held at financial institutions other than St.George. Please make sure any BSB and account number 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 times specified, it will in most cases be treated as having been made on the same day. However, we may choose to process a transaction or payment on a day after the cut-off time for that day.

Cut-off times (other than for BPAY Payments)

- For payments other than Telegraphic Transfers – 5.30pm each Business Day.
- For Telegraphic Transfers – 5.00pm each Business Day.

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.

It usually takes at least two Business Days for a transfer or payment to be received by a payee.

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, except for a Collection Code Pay to Mobile Payment. For a Collection Code Pay to Mobile Payment the transaction receipt number will be issued once a payment is claimed. You should keep this number in case you have any queries in relation to the 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 It may be possible to stop or cancel a Collection Code Pay to Mobile Payment before the payment is claimed by the Pay to Mobile Recipient. If you want to attempt to stop or cancel you must logon to Mobile Banking and delete the payment as soon as possible.

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

6.5 Further information about stopping or altering BPAY Payments and Telegraphic Transfers is set out in clauses 17 (for BPAY Payments) and 28.7 (for Telegraphic Transfers).

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

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 We may cancel your access to Internet and Phone Banking and/or a service or a feature of Internet Banking or Phone 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, or where you have not accessed Internet Banking or Phone Banking for a lengthy period. We inform you in writing after we cancel your registration. If you want to use Internet Banking and Phone Banking at a later time, you may ask us to register you again.

7.3 You can cancel your registration for Internet and Phone Banking by 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.

7.4 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.

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;
- by sending it to your nominated Australian landline telephone number by interactive voice response message; or
- via any other method of transmission you agree, as elected by you from time to time.

8.3 If you are currently registered for Internet Banking, you will not be able to perform certain At Risk Transactions using Phone 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 and Phone Banking automatically registers you for Mobile Banking (however you need not activate Mobile Banking). If you are not already registered for Internet and Phone Banking and you wish to use Mobile Banking, we automatically register you for Internet and Phone Banking also.

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.

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

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 fingerprint logon (if supported, see 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 **stgeorge.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 St.George 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.

(c) Only limited transaction history can be viewed using Mobile Banking.

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.

We may without notice to you, temporarily suspend or terminate the notifications feature for any reason.

> Section 5 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".

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

To protect your privacy, we recommend setting a PIN or password on your Mobile Banking Device (or using fingerprint logon 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.

Using fingerprint logon

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

9.14 Each time the Mobile Banking Device detects that fingerprint 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 fingerprint. If you activate fingerprint logon, the Mobile Banking App can tell when your Mobile Banking Device detects that a stored fingerprint 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 7 – 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 We may 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, or where you have not accessed Mobile Banking for a lengthy period. We inform you in writing after we cancel your access. 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.

9.17 To cancel your registration for Mobile Banking, you can cancel your registration for Internet and Phone Banking by 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.

9.18 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.

9.19 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.

10. Mobile Banking – Tap & Pay

10.1 Tap & Pay is available to registered users of Mobile Banking using a compatible Mobile Banking Device. (Not all Mobile Banking Devices can be used for Tap & Pay.) Tap & Pay is a feature that enables you to use your Mobile Banking Device to make contactless transactions with contactless terminals by holding your Mobile Banking Device to the contactless terminal (**"Tap & Pay**").

10.2 Before you can use Tap & Pay, you need to first set up Tap & Pay in Mobile Banking and download any eligible card you would like to use for Tap & Pay to your Mobile Banking Device. You can choose any of your existing cards that are enabled with contactless technology. To find out which cards and mobile devices are eligible for Tap & Pay, visit stgeorge.com.au.

Getting Started with Tap & Pay

10.3 To get started, you must set up Tap & Pay on your Mobile Banking Device. You will need to:

(a) install the Mobile Banking App on a compatible Mobile Banking Device;

(b) be registered for Mobile Banking;

(c) logon to the Mobile Banking App and follow the Tap & Pay instructions to select the eligible cards you would like to download to your Mobile Banking Device; and

(d) install or enable any other requirements at a device level to enable Tap & Pay to work – for example some Samsung mobile devices may require software known as Samsung KMS Agent installed. You should check the instructions given by your mobile device manufacturer.

You can find out through the Mobile Banking App when your card has been successfully downloaded onto your Mobile Banking Device.

10.4 You can make Tap & Pay contactless transactions at contactless terminals without needing to enter the PIN for your card if the transaction amount is less than or equal to the contactless transaction limit set out in Table C or such other limit as the merchant has set.

For any transaction amount that is above the contactless transaction limit or the limit set by the merchant, you will need to enter the PIN for the card.

The transaction amount will be processed to the EFT Account linked to the card selected in the Mobile Banking App under the terms and conditions that apply to that EFT Account.

10.5 **Choosing Tap & Pay cards**

Visa Debit card

If you select your Visa Debit card to download to the Mobile Banking App, all Tap & Pay transactions will be processed against the primary account linked to your physical card only. You can change the linked account at any branch or by calling the Internet & Phone Banking Helpdesk, 24 hours a day, seven days.

Credit cards

If you select your card that is a credit card to download to the Mobile Banking App,

all Tap & Pay transactions will be processed against the linked credit card account only. Tap & Pay transactions will not be processed against any other account. Each Tap & Pay transaction will be treated as a purchase transaction (or a refund of that transaction). No cash advance transactions can be made.

You can select a different card by opening the Mobile Banking App, tapping on the "Tap & Pay" icon on the menu bar and selecting the card image of the chosen card.

Tap & Pay settings

10.6 You have the choice of three Tap & Pay payment settings in the Mobile Banking App. You can change the setting option at any time. Pay Fast is the default setting if you do not select a different one.

Pay Fast setting: From the download of your first eligible card, until you change the settings, the Tap & Pay functionality is on at all times, even if the Mobile Banking App is closed or even if your Mobile Banking Device is locked or 'asleep'. All Tap & Pay transactions will be processed to the account linked to the card that is selected at the time of the transaction (Refer to clause 10.5)

Open App & Pay setting: If you select this setting you will need to open the Mobile Banking App each time you wish to make a Tap & Pay transaction. The transaction will be processed to the account linked to the selected card image of the card on the screen of your Mobile Banking Device.

Open App & Sign In setting: In addition to opening the Mobile Banking App, you will need to enter your Internet and Phone Banking Customer Access Number and your preferred logon credential before you can make a Tap & Pay transaction. To do so, open the Mobile Banking App, enter your Internet and Phone Banking Customer Access Number preferred logon credential.

Tap & Pay contactless transactions

10.7 For each of the payment setting options, to make a Tap & Pay contactless transaction you need to hold your Mobile Banking Device to the contactless terminal until the transaction is completed.

You can check the card you wish to use before making a payment by logging into the Mobile Banking App and selecting 'settings' in Tap & Pay.

Deleting the Mobile Banking App (card data will remain on the Mobile Banking Device) or restoring the Mobile Banking Device to factory default (card data will be removed from the Mobile Banking Device) will disable Tap & Pay. You can request to close a card downloaded to your Mobile Banking Device for Tap & Pay by calling the Internet & Phone Banking Helpdesk, 24 hours a day, seven days.

10.8 **Your protection and liability for unauthorised transactions**

The requirements about protecting of your card and PIN and liability for unauthorised transactions provisions in your EFT Account terms and conditions apply (as practicable) to your use of your Mobile Banking Device and PIN to make Tap & Pay contactless transactions. Refer to your card's terms and conditions for what to do to protect your card and your PIN (because card details are downloaded to your Mobile Banking App and used with the Mobile Banking Device).

> Section 7 – General matters contains important information about security of your Access Codes, unauthorised and mistaken transactions and other consumer protection issues.

Suspension or termination

10.9 In addition to our right to suspend Mobile Banking under clause 9.16, we may suspend or terminate your use of Tap & Pay without notice at any time where we suspect unauthorised transactions have occurred, or that the Mobile Banking App is being misused, or to restore the security of our systems or of any individual card or account.

11. Mobile Banking – Pay to Mobile

11.1 With Pay to Mobile you can request us to make a payment to a Pay to Mobile Recipient by giving us that party's Australian mobile telephone number. Payments may be made to an Australian mobile telephone number rather than to an EFT Account or an account at another Australian financial institution. When you activate Pay to Mobile, you can also receive Pay to Mobile Payments as set out in this clause.

To use Pay to Mobile you will need to logon to Mobile Banking. To be eligible to use the service, your Mobile Phone Number has to be registered for our Secure Code Service, you need an eligible EFT Account and have registered your email address with us, and you must have a Mobile Banking Device associated with your EFT Account under clause 9.

Pay to Mobile fees & charges

11.2 Using Pay to Mobile will not incur any separate fees and charges from us, in addition to any fees

and charges payable for your use of Internet and Phone Banking, including Mobile Banking, that are set out in your EFT Account terms and conditions.

Pay to Mobile – your Mobile Phone Number

11.3 If you change or no longer use your Mobile Phone Number, you must contact the Internet & Phone Banking Helpdesk to update your details and de-activate Pay to Mobile for that Mobile Phone Number. To re-activate Pay to Mobile with any new Mobile Phone Number you will need to logon to Mobile Banking. You can have one Mobile Phone Number activated for Pay to Mobile at one time.

If you are also a Westpac customer, you are unable to register for the Westpac Pay to Mobile service with the same Mobile Phone Number used to activate the St.George Banking Group Pay to Mobile service.

If your Mobile Phone Number changes, any authorised Pay to Mobile Payments directed to that Mobile Phone Number will be directed to the EFT Account you last advised. However if the mobile telephone number is re-issued, the new holder may claim any payments directed to that mobile telephone number under clause 11.5 or 11.6.

To make payments

11.4 Pay to Mobile allows you to make a payment to a Pay to Mobile Recipient by providing:

(a) the amount to be paid;

(b) the Pay to Mobile Recipient's name and Australian mobile telephone number; and,

(c) an optional description of the payment.

It is your responsibility to ensure that the details provided in a Pay to Mobile Payment are correct to avoid an unsuccessful claim by the Pay to Mobile Recipient or funds being paid to an unintended account. We do not check that the details provided by you are correct.

You agree to advise the Pay to Mobile Recipient that you have provided us with their Australian mobile telephone number for the purpose of making a Pay to Mobile Payment.

If the Pay to Mobile Recipient wishes to dispute the amount or payment of the Pay to Mobile Payment, they must contact you directly.

Once you have authorised a Pay to Mobile Payment, the payment will be processed as specified in clause 11.5 or 11.6. If funds are credited back to your EFT Account for any reason, we do not pay interest on any amount credited to your EFT Account for the period that it is not credited to your EFT Account.

Straight Through Pay to Mobile Payments

11.5 For Pay to Mobile Recipients who are St.George Banking Group customers activated for Pay to Mobile, or Westpac customers registered for the Westpac Pay to Mobile service –

(a) Pay to Mobile Payments will be processed directly to their nominated account for the respective Pay to Mobile service at the time the payment is made, without further information or action required by you or by them. You will not be able to cancel this payment. If you believe you have made a mistake, please contact us. Refer to clause 6.1.

(b) The amount will be debited from your EFT Account at the time you authorise the Pay to Mobile Payment. Please allow up to 2 Business Days for the Pay to Mobile Recipient's account to be credited with the amount. Refer to the payment cut-off times in clause 3.3.

Collection Code Pay to Mobile Payments

11.6 For Pay to Mobile Recipients who are St.George Banking Group customers not activated for Pay to Mobile or Westpac customers not registered for the Westpac Pay to Mobile service or are customers of other Australian financial institutions –

(a) Following a request from you to make a Pay to Mobile Payment, we will send an SMS containing a Collection Code to the Pay to Mobile Recipient notifying them that you would like to pay them and how to receive the funds. We will use all reasonable endeavours to send this SMS as soon as possible after you have requested the Pay to Mobile Payment. However, we are not liable for any delay in sending this SMS.

(b) The nominated amount will not be debited from your EFT Account until the Pay to Mobile Recipient successfully claims the payment.

(c) It is your responsibility to tell your Pay to Mobile Recipient to protect and not share their Collection Code with anyone (other than us). If the Collection Code is known to any other person, that person may be able to claim the Pay to Mobile Payment and we are not liable for any loss or damage you or any person suffers.

(d) If you believe you have entered the wrong mobile telephone number you should cancel the Pay to Mobile Payment by logging into Mobile Banking and selecting to delete the payment in your Past Payments or calling the Internet & Phone Banking Helpdesk.

Important – If a Collection Code is sent to a person other than the intended Pay to Mobile Recipient, that person may be able to claim the Pay to Mobile Payment.

11.7 Once you have activated Pay to Mobile, you can also receive Pay to Mobile Payments directly to your EFT Account you nominated for Pay to Mobile. Pay to Mobile Payments will be processed directly to the EFT Account you have nominated without further information or action being required by you. You agree that the payer will be aware that you are a St.George Banking Group or a Westpac customer.

Where a Pay to Mobile Recipient is not activated for Pay to Mobile, the Pay to Mobile Recipient must claim the Pay to Mobile Payment from www.stgeorge.com.au by entering:

(a) their Australian mobile telephone number the payment was made to;

(b) the exact amount of the Pay to Mobile Payment;

(c) the Collection Code; and,

(d) the details of their eligible Australian bank account for the funds to be paid to.

If this information is entered incorrectly, the claim for Pay to Mobile Payment may be unsuccessful. However, if the information in (a) to (c) is entered correctly and a valid Australian bank account number is entered under (d), the payment will be made to that Australian bank account, even if the Pay to Mobile Recipient has made a mistake.

In processing payments, we do not check that the account number entered matches the account name or BSB details provided. We are not liable for loss arising from any error in instructions given by the Pay to Mobile Recipient.

If there is an error in instructions, you should let us know as soon as possible and the issue will be resolved under clause 32.

The Pay to Mobile Recipient must successfully claim the Pay to Mobile Payment by midnight Sydney time on the third calendar day following the day you authorised the Pay to Mobile Payment in Mobile Banking. If the Pay to Mobile Recipient does not successfully claim the Pay to Mobile Payment within this time they will not be able to receive the funds and if required a new Pay to Mobile Payment will need to be initiated by you.

(e) Further to any other clause in these Terms and Conditions, if on the day the Pay to Mobile Recipient claims the Pay to Mobile Payment:

(i) your EFT Account has been blocked, suspended or closed;

(ii) you have insufficient cleared funds available in your EFT Account for the transfer to proceed;

(iii) it causes you to exceed the limits or you do not meet the security requirements applying to your Internet and Phone Banking as set out in these Terms and Conditions, the claim for the Pay to Mobile Payment will be unsuccessful. You will need to initiate a new Pay to Mobile Payment if this occurs.

If the Pay to Mobile Recipient wishes to dispute the details or failure of a Pay to Mobile Payment they must contact you directly.

Liability and indemnity

11.8 Except as stated in clause 30, we will not be liable:

(a) to you for any loss or damage:

(i) arising from you or us cancelling a Pay to Mobile Payment prior to it being collected or from you causing an event set out in clause 11.7(e) to occur;

(ii) as a result of you entering the wrong mobile telephone number when making a Pay to Mobile Payment; or

(iii) if we delay, block, cancel or refuse to process a payment for any reason; nor

(b) to any other person if:

(i) a third party (other than the Pay to Mobile Recipient) becomes aware of the amount of the Pay to Mobile Payment or the Collection Code other than as a result of the fraudulent or negligent conduct of our employees or agents;

(ii) the amount of the Pay to Mobile Payment, the Collection Code or account details provided by the Pay to Mobile Recipient when claiming the Pay to Mobile Payment are entered incorrectly;

(iii) the Pay to Mobile Recipient fails to collect the Pay to Mobile Payment within the expiration time period set out in this clause;

(iv) you or we cancel the Pay to Mobile Payment prior to it being collected or if an event set out in clause 11.7(e) occurs; or

(v) if we delay, block, cancel or refuse to process a payment for any reason.

We will not be responsible for any inability of your mobile device to access or use Pay to Mobile, or for any loss or damage to your mobile device resulting from your access or use, or attempted access or use, of Pay to Mobile and you should satisfy yourself as to these matters before attempting to access or use Pay to Mobile.

Suspension and termination of Pay to Mobile

11.9 In addition to our right to suspend Mobile Banking under clause 9.16, we may suspend or terminate your use of Pay to Mobile without notice at any time where we suspect unauthorised transactions have occurred, that the Mobile Banking App is being misused or to restore the security of our systems or of any individual account.

12. Mobile Banking – Cardless Cash

12.1 Cardless Cash is a facility which may be used by holders and Users (see clause 12.6) of Cardless Cash Accounts to withdraw cash from a Cardless Cash Account without a card at St.George Banking Group ATMs and Westpac-branded ATMs in Australia.

Cardless Cash is unable to be accessed through non-St.George Banking Group ATMs and non-Westpac-branded ATMs in Australia or overseas ATMs.

12.2 You will be deemed to have agreed to these Terms and Conditions when you set up the Cardless Cash feature ("Get Cash") or use (or another person uses) a cash code supplied by us to you.

12.3 You can generate a cash code from a Cardless Cash Account by logging on to the Mobile Banking App using your Mobile Banking Device and selecting the Cardless Cash feature.

Setting up and using Cardless Cash

12.4 You can set up Cardless Cash by following the steps below. Once you have set up Cardless Cash the first time, you can use it by following steps (g) to (i).

(a) Open the Mobile Banking App on your Mobile Banking Device.

(b) Logon using your Mobile Banking credentials.

(c) Tap on the "Cash" icon on the menu bar.

(d) Tap "Get Started" to accept the Cardless Cash Terms and Conditions.

(e) Set up your device for Cardless Cash by requesting and entering the Secure Code.

Note: You will need to already be registered for our Secure Code Service before you can set up Cardless Cash.

(f) You can start using Cardless Cash once steps (a) to (e) are completed successfully.

(g) Start using Cardless Cash by selecting a Cardless Cash Account that you wish to make a withdrawal from. You should ensure that the Cardless Cash Account you nominate contains sufficient funds.

(h) Enter an eligible amount you wish to withdraw and tap 'Get cash code'.

(i) A cash code will be generated in the next screen. You also have the option to share the code with family and friends by tapping 'Share via SMS', see clause 12.6.

(j) After first time set up, you can continue to use the feature by logging in to Mobile Banking, tapping the "Cash" icon on the menu bar and following steps (g) to (i).

(k) To access Cardless Cash at a St.George Banking Group ATM or Westpac-branded ATM in Australia, you must press the "Cardless Withdrawal" button or the "Enter" button. You will be asked to enter your cash code and the amount you wish to withdraw (which must be no more than the amount you nominated when you requested a cash code).

If you access the St.George Mobile Banking App on multiple Mobile Banking Devices, and would like to use Cardless Cash on any of these devices, you will need to go through the above set up steps for each Mobile Banking Device.

Only one customer can access Cardless Cash per Mobile Banking Device at a time.

Only one cash code can be generated per customer for a Cardless Cash Account at any one time. This means that there can be only one "live" cash code at any time. If you suspect your cash code has fallen into the wrong hands, you should call us to cancel the code. You can also cancel the code and request for a new one via Cardless Cash at any time. See clause 12.10 in relation to loss, theft or misuse of cash code.

You should take care of your cash code and ensure that it is not given or made available to any person unless you want that person to be able to withdraw cash from your account using Cardless Cash. See clause 12.6.

Withdrawal limits

12.5 You may withdraw up to a maximum of the amount you nominate when you request a cash code, subject to a Cardless Cash daily limit of $500 and a weekly Cardless Cash limit of $1,000. These limits apply in addition to the daily withdrawal limits which apply to your

card. You may conduct up to three Cardless Cash transactions per day, subject to the daily transaction limit of $500. Please note that $20 is the minimum amount and $500 is the maximum amount you may withdraw per Cardless Cash transaction per day. The limits described above will apply:

(a) across all Cardless Cash Accounts held by an account holder

(b) across St.George Banking Group Mobile Banking Apps, and

(c) per customer for joint accounts.

Authorising a User to withdraw cash with a cash code

12.6 You may authorise another person to withdraw up to the amount of cash nominated by you from your Cardless Cash Account using Cardless Cash by passing a cash code to that person (a "User").

If you pass on a cash code to another person, you are authorising the User to withdraw up to the amount of cash nominated by you from your Cardless Cash Account.

A User:

(a) is limited to withdrawing up to the amount of cash nominated by you from your Cardless Cash Account following your instruction to us to issue you with a cash code, and may not perform any other transaction or give any other instruction; and

(b) will not be acting as agent for you (whether the User accesses funds through use of a cash code for itself or for you, that person does so as principal and not as agent).

Cash code expiry

12.7 The cash code will expire 3 hours after it is given to you and it may only be used once (even if you do not withdraw the maximum available amount when you use the cash code). To obtain a new cash code, request one through Cardless Cash on your Mobile Banking App.

Cardless Cash fees & charges

12.8 There is no additional charge to access Cardless Cash. Refer to the Terms and Conditions which apply to your Cardless Cash Account for standard fees and charges that apply to transactions that you make on your Cardless Cash Account.

If you currently incur transaction fees for St.George Banking Group ATMs or Westpac-branded ATM withdrawals, you will continue to incur these fees in accordance with the Terms and Conditions of your Cardless Cash Account.

Important: We may elect not to charge a fee, which we are otherwise entitled to charge, under the terms and conditions of the account. Any failure by us to charge a fee shall not constitute a waiver of that fee or of the right to charge that fee.

Security and liability for Cardless Cash

12.9 Protecting your cash code

To protect your cash code, you must

(a) not give it to another person unless you want that person to perform a Cardless Cash withdrawal from your Cardless Cash Account;

(b) try to memorise it;

(c) make sure that nobody watches you or hears you when you are entering or using your cash code at a St.George Banking Group ATM or Westpac-branded ATM (except for Users you have authorised to use your cash code);

(d) never enter your cash code in an ATM that does not look genuine, has been modified, has a suspicious device attached to it or is operating in a suspicious manner; and

(e) be ready to make a withdrawal when you approach a St.George Banking Group ATM or Westpac-branded ATM in Australia.

Important: Liability for losses resulting from unauthorised transactions is determined under the relevant provisions of the ePayments Code where that Code applies, despite the obligations listed above.

Loss, theft or misuse of a cash code

12.10 You should notify us if your cash code has been passed on inadvertently to another person, or a record of it is lost, stolen or misused. If you notify us, we will be able to cancel the cash code from the time our Customer Contact Centre receives the notice. You can also cancel the cash code yourself through Cardless Cash by tapping the "Cash" icon on the menu bar and tapping 'Delete code'. The best way to contact us is by visiting any branch or calling our Customer Contact Centre, 24 hours a day, seven days.

Suspension and termination of Cardless Cash

12.11 In addition to our right to suspend Mobile Banking under clause 9.16, we may suspend or terminate your use of Cardless Cash without notice at any time where we suspect unauthorised transactions have occurred, that the Mobile Banking App is being misused or to restore the security of our systems or of any individual Cardless Cash Account.

Section 4 – BPAY

13. BPAY terms and conditions

13.1 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.

13.2 You may also receive or access bills or statements electronically ("BPAY View") from participating Billers nominated by you using Internet Banking.

13.3 You may choose to make a BPAY Payment using Internet and Phone Banking or any other payment method accepted by the Biller. We are a Biller and you may nominate us as a Biller for the purposes of BPAY View. 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.

13.4 When you ask us to make a BPAY Payment, you must give us the information specified in clause 16 below. 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.

13.5 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.

14. How to use BPAY

14.1 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.

14.2 We may impose restrictions on the accounts from which a BPAY Payment may be made. In addition to the limits imposed under clause 2.7, 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).

14.3 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.

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

14.5 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.

15. 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.

16. Information you must give us

16.1 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).

16.2 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).

16.3 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.

17. Stopping or altering payments

17.1 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.

17.2 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.

17.3 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.

17.4 Subject to clause 22, 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 22) 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 22) on a Banking Business Day or on a non-Banking Business Day.

17.5 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.

17.6 While it is expected that any delay in processing a BPAY Payment for any reason set out in clause 17.5 will not continue for more than one Banking Business Day, any such delay may continue for a longer period.

17.7 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.

18. BPAY View

18.1 You may register to use BPAY View. You can register for BPAY View through Internet Banking if you are registered for Internet and Phone Banking.

18.2 If you register to use BPAY View, while you are registered you:

(a) agree to our disclosing to Billers nominated by you:

(i) such of your personal information (for example your name, email address and the fact that you are our customer) as is necessary to enable Billers to verify that you can receive bills and statements electronically using BPAY View (or telling them if you cease to do so); and

(ii) that an event in clause 18.3(b), (c), (d), (e) or (f) has occurred;

(b) agree to us or a Biller (as appropriate) collecting data about whether you access your emails, Internet Banking and any link to a bill or statement;

(c) state that, where you register to receive a bill or statement electronically through BPAY View, you are entitled to receive that bill or statement from the applicable Biller;

(d) agree to receive bills and statements electronically and agree that this satisfies the legal obligations (if any) of a Biller to give you bills and statements. Whilst you are registered, you may receive a paper bill or statement from the Biller only in the circumstances set out in clause 18.3. For the purposes of this clause, we are the agent for each Biller nominated by you under (a) above;

(e) agree to direct to a Biller any enquiry relating to a bill you receive electronically from that Biller; and

(f) agree that the BPAY View terms in these terms and conditions apply to you.

18.3 You may receive paper bills and statements from a Biller instead of electronic bills and statements:

(a) at your request to a Biller (a fee may be charged by the applicable Biller for supplying the paper bill or statement to you if you ask for this in addition to an electronic form);

(b) if you or a Biller de-register from BPAY View or you no longer have an EFT Account with us;

(c) if we receive notification that your email mailbox is full, so that you cannot receive any email notification of a bill or statement;

(d) if your email address is incorrect or cannot be found and your email is returned to us undelivered;

(e) if we are aware that you are unable to access your email or Internet Banking or a link to a bill or statement for any reason;

(f) if any function necessary to facilitate BPAY View malfunctions or is not available for any reason for an extended period.

18.4 You agree that when using BPAY View:

(a) if you receive an email notifying you that you have a bill or statement, then that bill or statement is received by you:

(i) when we receive confirmation that your server has received the email notification, whether or not you choose to access your email; and

(ii) at the email address nominated by you;

(b) if you receive notification through Internet Banking without an email then that bill or statement is received by you:

(i) when a notification is posted through Internet Banking, whether or not you choose to access Internet Banking; and

(ii) through Internet Banking;

(c) bills and statements delivered to you remain accessible through Internet Banking for the period determined by the Biller up to a maximum of 18 months, after which they will be deleted, whether paid or not;

(d) you will contact the Biller directly if you have any queries in relation to bills or statements.

18.5 You must:

(a) check your emails or Internet Banking at least weekly;

(b) tell us if your contact details (including email address) change;

(c) tell us if you are unable to access your email or Internet Banking or a link to a bill or statement for any reason;

(d) ensure your mailbox can receive email notifications (e.g. it has sufficient storage space available); and

(e) arrange with the Biller to send you bills or statements by an alternative means if you no longer have an EFT Account with us.

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

19.1 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.

19.2 We will attempt to rectify any such matters in relation to your BPAY Payments in the way described in clauses 19.3 to 19.5. 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 30. Otherwise, except as set out in clauses 19.3 to 19.5 and clause 25 and subject to clause 31.3, we will not be liable for any loss or damage you suffer as a result of using the BPAY Scheme.

19.3 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.

19.4 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.

19.5 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 unless

some other person involved in the BPAY Scheme knew of the fraud or would have detected it with reasonable diligence, in which case we will attempt to obtain a refund for you of the fraud induced payment.

19.6 If a BPAY Payment you have made falls within the type described in clause 19.4 and also clause 19.3 or 19.5, then we will apply the principles stated in clause 19.4.

19.7 If a BPAY Payment you have made falls within both the types described in clauses 19.3 and 19.5, then we will apply the principles stated in clause 19.5.

19.8 Except where a BPAY Payment is a mistaken payment referred to in clause 19.3, an unauthorised payment referred to in clause 19.4, or a fraudulent payment referred to in clause 19.5, 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.

19.9 Your obligation under clauses 19.3 and 19.4 to pay us the amount of any mistaken or unauthorised payment (as applicable) is subject to any of your rights referred to in clause 25.

19.10 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.

19.11 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.

20. BPAY View billing errors

20.1 For the purposes of clauses 20.2 and 20.3, a BPAY View billing error means any of the following:

(a) if you have successfully registered with BPAY View:

(i) failure to give you a bill (other than because you failed to view an available bill);

(ii) failure to give you a bill on time (other than because you failed to view an available bill on time);

(iii) giving a bill to the wrong person;

(iv) giving a bill with incorrect details; or

(b) if your BPAY View deregistration has failed for any reason, giving you a bill if you have unsuccessfully attempted to deregister.

20.2 You agree that if a BPAY View billing error occurs:

(a) immediately upon becoming aware of the BPAY View billing error, you must take all reasonable steps to minimise any loss or damage caused by the billing error, including contacting the applicable Biller and obtaining a correct copy of the bill; and

(b) the party who caused the error is responsible for correcting it and paying any charges or interest which would ordinarily be payable to the applicable Biller due to any consequential late payment and as a result of the BPAY View billing error.

20.3 You agree that for the purposes of this clause you are responsible for a BPAY View billing error if the billing error occurs as a result of an act or omission by you or the malfunction, failure or incompatibility of computer equipment you are using at any time to participate in BPAY View.

21. 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.

22. 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.

23. 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.

24. 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.

25. Consequential damage

25.1 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.

25.2 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.

26. Privacy

26.1 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 personal information (for example your name, email address and the fact that you are our customer) as is necessary to facilitate your registration for or use of the BPAY Scheme;

(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 and your information necessary to process your use of BPAY View will be disclosed by BPAY Pty Ltd, through its agent, to the Biller. 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; and

(c) that an event in clause 18.3 (b), (c), (d), (e) or (f) has occurred.

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

26.3 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.

26.4 If your personal information detailed above is not disclosed to BPAY Pty Ltd or its agent, it will not be possible to process your requested BPAY Payment or for you to use BPAY View.

Section 5 – Alerts Services

27. Alerts Services

27.1 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.

27.2 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.

27.3 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.

27.4 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.

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

27.6 The Alerts Service may without notice to you be suspended or terminated for any reason including without limitation 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.

27.7 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

27.8 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

27.9 Fees may be charged for each Alert (as provided in the Fees and Charges Booklet for your applicable EFT Account).

Section 6 – Telegraphic Transfers

28. Telegraphic Transfer terms and conditions

28.1 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.

28.2 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.

28.3 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.

28.4 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.

28.5 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).

28.6 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.

28.7 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.

28.8 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).

28.9 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.

28.10 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.

Section 7 – General matters

29. Security of your Internet and Phone Banking Access Codes

29.1 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.

29.2 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 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 you fail to ensure the security of your Access Codes your liability for unauthorised transactions will be determined under clause 30.

Your obligations

You must:

(a) not record your Internet and Phone Banking Security Number or Internet Banking Password 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 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; and

(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.

(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?

29.3 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.

29.4 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 29.2, 29.3 and 29.4.

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

29.5 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.

29.6 If you do not notify us you may be liable for unauthorised use – see clause 30.

29.7 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.

29.8 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.

29.9 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.

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

30.1 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 29.5 (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 30.3 and 30.4 for details of those circumstances.

30.2 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 29.5; 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.

(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

30.3 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) you 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.

30.4 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.

30.5 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.

30.6 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.

30.7 You will not be liable under clauses 30.3 or 30.4 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 30.4 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 30.4.

31. Electronic banking system malfunction

31.1 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.

31.2 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.

31.3 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.

31.4 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).

32. Mistaken Internet Payments

32.1 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 6 of these terms for information about Telegraphic Transfers.

Reporting mistaken internet payments

32.2 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.

Dealing with mistaken internet payments

32.3 Mistaken internet payments will be dealt with by us in accordance with the ePayments Code, where that Code applies to the payment. Set out at clauses 32.4 to 32.6 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.

Notwithstanding anything set out below, where the unintended recipient of the mistaken internet payment is receiving income support payments

from Centrelink, the receiving institution must recover the funds from that recipient in accordance with the Code of Operation for Centrelink Direct Credit 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

32.4 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

32.5 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

32.6 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 32.4(b)(i),

we will, without your consent, 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 32.4 above.

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

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

Liability for losses arising from internet payments

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

33. Industry codes

33.1 If you are an individual or a Small Business, the relevant provisions of the Code of Banking Practice will apply to the Banking Services you use. Information is available from us about:

- account opening procedures;
- our obligations regarding the confidentiality of your information;
- complaint handling procedures;
- bank cheques;
- the advisability of you informing us promptly when you are in financial difficulty; and
- the advisability of you reading the terms and conditions applying to the relevant banking service.

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

34. Changes to the Terms and Conditions

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

34.2 We will give notice of any change to the Terms and Conditions in accordance with the times set out in the table in clause 34.3, and in the manner described in clause 35.

34.3

Type of change or event	Notification we will give you
A If we: (a) introduce a new fee or charge (other than a government fee or charge, see clause 35.4); (b) increase any fee or charge (other than a government fee or charge, see clause 35.4); (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	On or before the day the change takes effect.

35. Communications

35.1 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 35.5).

35.2 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.

35.3 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.

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

35.5 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.

35.6 We need not give any advance notice 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.

35.7 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.

36. Appropriate use of our services

36.1 You warrant that your use of the services we provide will not breach any law of Australia or any other country.

36.2 Where we consider it necessary for us to meet our regulatory and compliance obligations:

(a) you must provide us with any information we reasonably request;

(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 exercising our rights under this clause.

37. 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.

38. GST

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

38.2 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.

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

39. 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.

40. Assignment

You cannot assign your rights under the Terms and Conditions.

41. Problems and Disputes

41.1 If you believe an error has been made, please notify us by contacting any of our branches. We will correct any error that is found to be ours as soon as possible.

41.2 If you have a problem or complaint about a Banking Service, you should speak to our Customer Service personnel. You can do this by:

(a) contacting the branch where the problem arose; or

(b) calling the Customer Contact Centre phone number listed on the end of these Terms and Conditions.

41.3 To assist us in resolving your problem or complaint, you should:

(a) report it promptly;

(b) state clearly the nature of the problem or your particular grievance; and

(c) have available all documents and background information.

41.4 If the matter is not resolved to your immediate satisfaction, you can follow the dispute procedures set out below. Please also refer to our "Let Us Know What You Think" brochure for further information about disputes. It is available at any of our branches.

41.5 If you have a credit contract relating to the EFT Account, you may also have rights regarding disputes under the National Credit Code which are not referred to below. Further information about these rights may be obtained by:

(a) calling the Customer Contact Centre phone number at the end of these Terms and Conditions;

(b) referring to our brochure "Let Us Know What You Think"; or

(c) contacting a Government Consumer Agency.

41.6 You can lodge a complaint at any of our branches or telephone or write to the Senior Manager, Customer Relations at our head office in Sydney. The relevant details are set out at the end of these Terms and Conditions.

41.7 If we do not immediately resolve your complaint to your satisfaction, we will inform you in writing of our procedures for investigating and handling complaints. We will notify you of the name and contact number of the person who is investigating your complaint.

41.8 If it is unclear whether you have contributed to any loss, that is the subject of any complaint you make to us, we will consider all reasonable evidence, including all reasonable explanations for a transaction occurring. The fact that your EFT Account has been accessed with the correct Access Methods, while significant, will not be conclusive evidence that you have contributed to any loss.

41.9 We will not require you to raise complaints or disputes in relation to the processing of EFT Transactions with any other party to the shared EFT System (such as a retailer or a merchant). Where we have been notified by another party to the shared EFT System, or form the view, that a transaction has been debited or credited incorrectly to your EFT Account, we will investigate. We will make any corrections to your EFT Account we consider appropriate in the circumstances. Any correction will be included in your next statement. We will also notify you as soon as practicable, after reversing an incorrect credit.

41.10 If you request, we will provide you with further details about any correction shown on your account statement.

41.11 Normally, we will complete the investigation of your complaint and inform you of the results of our investigation within 21 days of receiving a complaint. Unless there are exceptional circumstances, we will complete our investigation within 45 days.

41.12 Where an investigation continues beyond 45 days, we will inform you of the reasons for the delay, give you monthly updates on the progress of the investigation and a date when a decision can reasonably be expected. We will not do this if we have requested a response from you and we are waiting for that response.

41.13 We will inform you in writing of our decision relating to an EFT Transaction dispute and, if the dispute is not resolved to your satisfaction, any further action you can take to resolve the dispute. We will inform you in writing of our decision relating to any other dispute, unless we agree with you that the notice can be given verbally.

41.14 The next available step is the Financial Ombudsman Service. This is a free, external and independent process for resolving disputes between banks and customers, provided the Ombudsman has the power to deal with your dispute. In addition, if your complaint relates to the way we handle your personal information, you have the right to complain to the Privacy Commissioner. Please refer to our brochure "Protecting Your Privacy". You can obtain a copy of the brochure by asking at any of our branches or by calling our Customer Contact Centre.

41.15 If, in relation to an EFT Transaction, we fail to observe these terms and conditions when we allocate liability or when conducting our complaint investigation and dispute resolution procedures and as a result there is an unreasonable delay or the outcome of our investigation is prejudiced, we will accept full liability for the amount that is the subject of the complaint.

41.16 If you have a complaint that relates to the BPAY Scheme and you are not an individual or Small Business, then we will resolve your dispute in accordance with dispute resolution procedures established under the BPAY Scheme. Please refer to Section 4 of these terms and conditions for further information.

41.17 There are other external avenues for dealing with disputes. Your State or Territory Government has a consumer rights protection agency such as the Department of Consumer Affairs.

42. 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; and

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

"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;

"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;

"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;

"Cardless Cash Account" means a St.George Banking Group eligible transaction account with a linked card in relation to which Cardless Cash is available for use from time to time. The list of these accounts can be found under the 'Cardless Cash' link within the Mobile Banking section of the website stgeorge.com.au.

Cardless Cash is only available on one of these accounts if the account is active and is not subject to an account block/restriction. An account may be subject to a block/restriction for a number of reasons including bankruptcy and account disputes. Phone the Customer Contact Centre phone number listed at the end of this document if you have any queries;

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

"cash code" means an identifier (within the meaning of the ePayments Code) which we issue to you on your request which is to be used to make Cardless Cash withdrawals at St.George Banking Group ATMs and Westpac-branded ATMs in Australia;

"Collection Code" means the code we create and send to the Pay to Mobile Recipient via SMS using the Australian mobile telephone number you provide;

"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;

"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;

"Fees and Charges Booklet" means the current fees and charges booklet setting out the current fees and charges payable by you when you perform a transaction using your EFT Account or a payment service;

"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;

"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 where the funds are paid into the account of an unintended recipient because the individual enters or selects a BSB number or other 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 number and/or identifier;

"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 St.George 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;

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

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

"Pay to Mobile Payment" means a transfer of value (including a request to transfer value) from an eligible EFT Account to an account held at an Australian financial institution (including us) by providing us with the recipient's Australian mobile telephone number. A payment cannot be made to an overseas mobile telephone number or an overseas financial institution;

"Pay to Mobile Recipient" means the intended recipient to receive a payment from you as payer by you providing us with their Australian mobile telephone number;

"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;

"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" means a business employing:

(a) less than 100 full-time (or equivalent) people, if the business is or includes the manufacture of goods; or

(b) in any other case, less than 20 full-time (or equivalent) people,

but does not include a business that obtains a Banking Service in connection with another business that does not meet the elements in (a) or (b) above;

"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;

"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 or a landline 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 **"St.George"** or **"St.George Bank"** or **"the Bank"** means St.George Bank – 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;

"you" means the user of Internet Banking or Phone 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.

BPAY is a registered trademark of BPAY Pty Ltd ABN 69 079 137 518

This page has been left blank intentionally.

This page has been left blank intentionally.

Important

If your Internet and Phone Banking Security Number or Internet Banking Password or any record of them is misused, lost or stolen, immediately notify us on **1300 555 203**, 24 hours a day, seven days.

Internet & Phone Banking Helpdesk

Call **1300 555 203** 24 hours a day, seven days.

Customer Contact Centre

Call **13 33 30** 24 hours a day, seven days.

Disputes

If your complaint is not immediately resolved to your satisfaction, contact:
Senior Manager, Customer Relations
Locked Bag 1, Kogarah NSW 1485
Telephone (Metro): **02 9553 5173**
Telephone (non-Metro): **1800 804 728**

st.george start something