Important changes to your current St.George Bank/Bank of Melbourne/BankSA Internet and Phone Banking Terms and Conditions and Important Information

Effective 20 March 2013, St.George Bank, Bank of Melbourne and BankSA will subscribe to the ePayments Code which replaces the current Electronic Funds Transfer Code of Conduct (***EFT Code***). The ePayments Code regulates consumer electronic payments including ATM, EFTPOS, debit and credit card transactions, online payments, internet banking and BPAY®.

As under the EFT Code, the ePayments Code will:

- require subscribers to provide customer disclosures in relation to fees, transaction limits and other terms and conditions;
- require subscribers to give receipts and statements in certain circumstances; and
- provide consumer protection in cases of fraud and unauthorised transactions.

For more information about the ePayments Code, please visit stgeorge.com.au/tandcchanges or bankofmelbourne.com.au/tandcchanges or banksa.com.au/tandcchanges.

To reflect our obligations under the ePayments Code, effective 20 March 2013, the following changes to your current St.George Bank/Bank of Melbourne/BankSA Internet and Phone Banking Terms and Conditions and Important Information will apply.

The Changes are:

Table A, insert the following text on the footnote
* Merchants or other providers of facilities may impose additional limits.

Table C, insert the following text on the footnote
* Merchants or other providers of facilities may impose additional limits.

Condition 4.4, is amended to read
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 phoning the General Customer Enquiries phone number on the back of this booklet.

Condition 5.4 is amended to read
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 5.2, 5.3 and 5.4

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

Condition 5.5, is amended to read
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 telephoning us on 1300 555 203 24 hours a day, seven days.

Condition 5.9, is amended to read
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.

Condition 6.1(c), is amended to read
the actual loss incurred before you notify us under clause 5.5 (excluding that portion of the loss incurred on any one day that exceeds the applicable daily transaction limit),

Condition 6.2 is amended to read
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 which occur after you have given us notice as required by clause 5.5; 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.

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

Condition 6.3 is amended to read
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;

(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, 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 has been breached or we are notified of the existence of unauthorized 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 unauthorized use occurs.

Condition 6.4 is amended to read

You will be liable if you have contributed to the unauthorised transactions because you unreasonably delayed in notifying us that any applicable 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.

Page 11, insert condition 6.6

If more than one Code is required to perform a 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.

Page 11, insert condition 6.7

You will not be liable under clauses 6.3 or 6.4 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. Your liability under clause 6.4 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 6.4.

Condition 7.3 is amended to read

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.

Condition 10A, heading and the following texts are inserted
10A Mistaken Internet Payments

10A.1 This clause 10A does not apply to BPAY® payments. See Section 2 of these terms for information about BPAY® payments.

Reporting mistaken internet payments

10A.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 a St George branch or by phoning us on 13 33 30 (St.George), 13 22 66 (Bank of Melbourne) or 13 13 76 (BankSA).

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

10A.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 10A.4 to 10A.5 is a summary of the processes in that Code.

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

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

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

Notwithstanding anything set out below, where the unintended recipient of the mistaken internet payment is

receiving income support payments from 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

10A.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:

Where the report is made within 10 Business Days of the payment:

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

Where the report is made between 10 Business Days and 7 months of the payment:

• the receiving institution will investigate the payment and complete the investigation within 10 Business Days of receiving a request.

• 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.

• if the unintended recipient does not establish they are entitled to the funds within that time, the receiving
institution will return the funds to the sending institution within 2 business days of that period (during
which time the recipient will be prevented from withdrawing the funds).

Where a report is made after 7 months of payment:

• 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

10A.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

10A.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 10A.4,

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 10A.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

10A.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.

Condition 17.2 is amended to read
We will attempt to rectify any such matters in relation to your BPAY® Payments in the way described in
clauses 17.3 to 17.5. 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 unauthorized BPAY® Payment will be determined in accordance with clause 6. Otherwise, except as set out in clauses 17.3 to 17.5 and clause 23 and subject to clause 7.3, we will not be liable for any loss or damage you suffer as a result of using the BPAY® Scheme.

Condition 27.2 is amended to read

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

New definitions inserted to Meaning of Words
"Code" means an Internet and Phone Banking Security Number, an Internet Banking Password, or any similar information which may be required in order to make EFT Transactions to and from an EFT Account and which you or the User is required to keep secret;

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

Definition deleted to Meaning of Words
"EFT Code"

New definitions inserted to Meaning of Words
"EFT Transaction" means a transfer of funds initiated by an instruction you give through Electronic Equipment to debit or credit an EFT Account;

"Identifier" means information that a User knows and must provide to perform an EFT Transaction but is not
required to keep secret;

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

"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;