NOTICE TO ALL SUNCORP BANK CUSTOMERS

Effective 20 March 2013, Suncorp Bank will subscribe to the ePayments Code which replaces the current Electronic Funds Transfer Code of Conduct. The ePayments Code regulates consumer electronic payments including ATM, EFTPOS, debit and credit card transactions, online payments, Internet banking and BPAY.

This document sets out the changes that have been made to the existing Suncorp Bank *Terms and Conditions for Suncorp Bank Accounts and for Continuing Credit Accounts* (Terms and Conditions) to reflect our obligations under the ePayments Code. The changes will apply on and from 20 March 2013.

Customers can obtain an updated copy of the Terms and Conditions at any Suncorp Bank branch, online at www.suncorpbank.com.au/product-information-documents or by contacting us on 13 11 75.

Global Changes

All relevant references to:

(a) "EFT Code" have been replaced by "ePayments Code";
(b) "EFT transaction" have been replaced by "ePayments Transaction";
(c) "Account" have been capitalised;
(d) "device" have been capitalised;
(e) "code" have been replaced by "Secret Code" in clause 20, clause 21, clause 22 and clause 23;
(f) "You" and "Your" have been capitalised in clause 20, clause 21, clause 22 and clause 23; and
(g) "Secret Access Code" have been replaced by "Secret Code".

Additional Changes

(a) The following definitions have been inserted in alphabetical order in 'Clause 1.3 Definitions and Interpretation':

"ADI" has the same meaning as authorised deposit-taking institution in the Banking Act 1959 (Cth) or any successor term adopted by the Australian Prudential Regulation Authority.

"Device" means a device given by us to You that is used to perform an ePayments transaction. Examples include:

• ATM or transaction card,
• debit card or credit card,
• prepaid card (including gift card), and
• security token issued by us that generates a security code.

"ePayments Code" means the ePayments Code issued by the Australian Securities & Investments Commission.

"ePayments Transaction" has the meaning provided for in clause 20.1.

"Identifier" means information that You know and must provide to perform an ePayments Transaction but which You are not required to keep secret (for example, an account number).
.

"Party to a Shared Electronic Payments Network" includes retailers, merchants, communications services providers and other organisations offering facilities, merchant acquirers and us.

"Receiving ADI" means an ADI which is a subscriber to the ePayments Code and whose customer has received an internet payment which You have reported as being a Mistaken Internet Payment.

"Sending ADI" means an ADI which is a subscriber to the ePayments Code and whose customer has made an internet payment which has been reported as being a Mistaken Internet Payment.

"Mistaken Internet Payment" means a payment using a 'pay anyone' internet banking facility (for example, an external funds transfer) processed by an ADI through direct entry where funds are paid into the account of an Unintended Recipient because the transferor entered or selected a BSB number and/or Identifier that does not belong to the named and/or intended recipient as a result of:

• the transferor's error, or

• the transferor being advised of the wrong BSB number and/or Identifier.

It does not include payments made using Bpay.

"Unintended Recipient" means the recipient of funds as a result of a Mistaken Internet Payment.

(b) The following definition has been deleted from 'Clause 1.3 Definitions and Interpretation':

"EFT Code" means the Electronic Funds Transfer Code of Conduct applying to electronic banking and being subscribed to by Suncorp.

(c) 'Clause 13 Lost or Stolen Cards, Passbooks, Cheques or Secret Access Codes etc' is renamed to 'Clause 13 Unauthorised Transactions and Lost or Stolen Cards, Passbooks, Cheques or Secret Codes etc.' and is deleted and replaced by:

"If You suspect an unauthorised transaction has been made on Your Account or Your card, passbook, cheque book, PIN, Telephone Access Code, Internet Banking Password, External Transfer Password or any password or secret code or any access method is stolen, lost or misused, or You suspect is being misused, contact us immediately by calling.

(a) the Hotline number, **1800 775 020**; or
(b) if overseas, **617 3362 2222**.

We may require You to confirm the details in writing.

We will give You a notification number or some other form of acknowledgment which You should retain as evidence of the date and time of Your report.

If You fail to notify us promptly when You become aware that Your card, passbook, cheque book, PIN, Telephone Access Code, Internet Banking Password, any password or Secret Code or any access method is stolen, lost or misused, or You suspect is stolen, lost or being misused then, subject to clause 20.5 and clause 20.14 to clause 20.16 (inclusive), You will be liable for any unauthorised transactions processed to Your Account.

Any items stolen must be reported to the police as the police report may be required by us if You wish to make a claim that a transaction on Your Account was not authorised by You."

(d) 'Clause 20.1 What is an EFT Transaction?' is renamed to 'Clause 20.1 What is an ePayments Transaction?'.

Delete the first and second paragraphs in Clause 20.1 and replace with the following:

"Where You are an individual, the ePayments Code applies to the following transactions provided by us, each of which is an ePayments Transaction:

(a) electronic card transactions, including ATM, EFTPOS, credit card and debit card transactions that are not intended to be authenticated by comparing a manual signature with a specimen signature,

(b) telephone banking and bill payment transactions,

(c) internet banking transactions, including by way of external transfer,

(d) online transactions performed using a card number and expiry date,

(e) online bill payments (including BPAY®),

(f) transactions using facilities with contactless features and prepaid cards, not intended to be authenticated by comparing a manual signature with a specimen signature,

(g) direct debits,

(h) transactions using mobile devices,

(i) mail order transactions not intended to be authenticated by comparing a manual signature with a specimen signature, and

(j) any other transaction specified by the Australian Securities & Investments Commission.

We will comply with the ePayments Code where it applies."

(e) 'Clause 20.2 Terms and Conditions' is deleted and replaced by:

"This clause 20 applies only to ePayments Transactions. If these provisions are inconsistent with or contrary to any other provision concerning ePayments Transactions in this document, this clause applies in precedence to those other provisions.

Clause 20 and the ePayments Code do not apply to:

(a) an Account that is designed primarily for use by a business, and established primarily for business purposes,
(b) a facility where You and Suncorp do not have a contractual relationship."

(f) 'Clause 20.6 Guidelines for Selecting Your Secret Code'. The second paragraph in Clause 20.6 is deleted.

(g) 'Clause 20.7 Guidelines for Recording Your Secret Code' is renamed to 'Clause 20.7 Secret Code Security Requirements'. The following paragraph is inserted at the beginning of Clause 20.7:

"You must not voluntarily disclose one or more of Your Secret Codes to anyone, including a family member or friend."

The fullstop at the end of paragraph (h) in Clause 20.7 is deleted and replaced with the following:

"unless You make a reasonable attempt to protect the security of the Secret Code; or"

The following new paragraph (i) is inserted in clause 20.7 following paragraph (h):

"(i) where a Device is not needed to perform an ePayments Transaction keep a written record of all Secret Codes required to perform ePayments Transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the Secret Code(s)."

The last paragraph in Clause 20.7 is deleted.

(h) 'Clause 20.9 EFT Transactions at Electronic Equipment' is renamed to 'ePayments Transactions using Electronic Equipment, Your Card or Other Approved Access Method'. Clause 20.9 is deleted and replaced by:

"We can limit the amount of Your ePayments Transactions using electronic equipment, Your card or any access method we provide in any single transaction or in any set period (a daily or weekly limit). The denomination of the notes You get is decided by the owner of the electronic equipment."

(i) 'Clause 20.11 Queries on EFT Transactions, Receipts and Sales Vouchers' is renamed to 'Clause 20.11 Queries on ePayments Transactions, Receipts and Sales Vouchers'.

The words 'or sales voucher' is inserted into the first sentence in Clause 20.11 after the words:

"If You have a question about the details on a transaction receipt or..."

The words 'transaction receipt or' is inserted into the second sentence in Clause 20.11 after the words:

"We may try to get a copy of the..."

(j) 'Clause 20.12 Electronic Equipment Faults' is renamed to 'Clause 20.12 Liability for Loss Caused by System or Equipment Malfunction'.

The words 'or system' are inserted into the first sentence in Clause 20.12 after the words "any electronic equipment".

The following paragraphs are inserted in Clause 20.12 after the existing paragraphs:

"You are not liable for loss caused by the failure of a system or equipment provided by any Party to a Shared Electronic Network to complete a transaction accepted by the system or equipment in accordance with Your instructions.

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 any Party to a Shared Electronic Payments Network, however caused. However, where You should reasonably have been aware that a system or equipment provided by any Party to a Shared Electronic Network was unavailable or malfunctioning, our liability may be limited to:

(a) correcting any errors, and

(b) refunding any fees or charges imposed on You."

Paragraph (a) and paragraph (f) have been deleted from Clause 20.12 and the remaining paragraphs have been renumbered accordingly.

(k) 'Clause 20.14 When You Are Not Liable for Any Losses' has been deleted and replaced by:

"An unauthorised transaction, that is a transaction You do not authorise, does not include any transaction carried out by You or by anyone performing a transaction with Your knowledge and consent. You will not be liable for losses resulting from unauthorised transactions where it is clear that You have not contributed to the loss.

Where You do not authorise a transaction, You will not be responsible for losses which:

(a) are caused by fraudulent or negligent conduct of our staff or agents of ours or third parties involved in networking arrangements or merchants or their agents or employees;

(b) are losses relating to an Identifier, Device or Secret Code which is forged, faulty, expired, or cancelled;

(c) arise from a transaction which required the use of any Device and / or Secret Code that occurred before You received any Device and / or Secret Code or reissued Device and / or Secret Code;

(d) are caused by the same transaction being incorrectly debited more than once to the same Account;

(e) arise from unauthorised transactions performed after we have been informed that the Device has been misused, lost or stolen or the security of the Secret Code has been breached;

(f) arise from unauthorised transactions that can be made using an Identifier without a Secret Code or Device or can be made using a Device, or a Device and an Identifier, but does not require a Secret Code, if You do not unreasonably delay reporting the loss or theft of the Device; and / or

(g) are losses which occur while our processes are unavailable, provided that a report is made within a reasonable time of the process again becoming generally available."

(l) 'Clause 20.15 When You are Liable for Losses' is deleted and replaced by:

"You will be liable for losses resulting from transactions which are carried out by You or by another person with Your knowledge and consent.

Where we can prove on the balance of probability that You have contributed to a loss through fraud, or breaching the Secret Code security requirements in clause 20.6, clause 20.7 and clause 20.16:

(a) You are liable in full for the actual losses that occur before the loss, theft or misuse of a Device or breach of Secret Code security is reported to us, but

(b) You are not liable for the portion of losses:

(i) incurred on any one day that exceeds any applicable daily transaction limit,
(ii) incurred in any period that exceeds any applicable periodic transaction limit,
(iii) that exceeds the balance on the Account, including any pre-arranged credit, or
(iv) incurred on any Account that we and You had not agreed could be accessed using the Device or Identifier and/or Secret Code used to perform the transaction.

Where:

(a) more than one Secret Code is required to perform a transaction, and

(b) we prove that You breached the Secret Code security requirements in clause 20.6, clause 20.7 and / or clause 20.16 for one or more of the required Secret Codes, but not all of the required Secret Codes,

You are liable as outlined above only if we prove on the balance of probability that the breach of the Secret Code security requirements under clause 20.6, clause 20.7 and / or clause 20.16 was more than 50% responsible for the losses, when assessed together with all the contributing causes.

You are liable for losses arising from unauthorised transactions that occur because You contributed to losses by leaving a card in an ATM, as long as the ATM incorporates reasonable safety standards that mitigate the risk of a card being left in the ATM.

Where we can prove, on the balance of probability, that You contributed to losses resulting from an unauthorised transaction by unreasonably delaying reporting the misuse, loss or theft of a Device, or that the security of all Secret Codes has been breached, You:

(a) are liable for the actual losses that occur between:

(i) when You became aware of the security compromise, or should reasonably have become aware in the case of a lost or stolen Device, and
(ii) when the security compromise was reported to us, but

(b) are not liable for any portion of the losses:

(i) incurred on any one day that exceeds any applicable daily transaction limit,
(ii) incurred in any period that exceeds any applicable periodic transaction limit,
(iii) that exceeds the balance on the Account, including any pre-arranged credit, or
(iv) incurred on any Account that we and You had not agreed could be accessed using the Device and/or Secret Code used to perform the transaction.

Where a Secret Code was required to perform the unauthorised transactions, and the other circumstances outlined in this clause above do not apply, You are liable for the least of:

(a) $150.00, or a lower figure determined by us;

(b) the balance of the Account or Accounts which we and You have agreed may be accessed using the Device and / or Secret Code, including any prearranged credit; or

(c) the actual loss at the time the misuse, loss or theft of a Device or breach of the Secret Code security is reported to us, excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction limit or any other periodic transaction limit.

We, or our external dispute resolution body, have a discretion to reduce Your liability in the circumstances set out in the ePayments Code.

If You report an unauthorised transaction on a debit card Account:

(a) we must not hold You liable for losses under this clause for an amount greater than the liability of You if we exercised any rights we had under the rules of the card scheme at the time the report was made, against other parties to the scheme (for example, charge-back rights), and

(b) this clause does not require us to exercise any rights we may have under the rules of the card scheme. However, we cannot hold You liable under this clause for a greater amount than would apply if we had exercised those rights."

(m) Insert a new clause 20.19 as follows, immediately following existing clause 20.18:

"20.19 Mistaken Internet Payments

When the ePayments Code applies to a transaction made through an internet banking facility, we are bound by and follow the rules of the ePayments Code in relation to Mistaken Internet Payments. Other ADIs who have subscribed to the ePayments Code are required to follow the same processes. These processes do not apply to transactions where the 'Pay Anyone' internet banking service used is a service designed primarily for use by a business and established primarily for business purposes.

This clause sets out how we will deal with Mistaken Internet Payments made by You and Mistaken Internet Payments received into Your Account. You agree to us dealing with Mistaken Internet Payments in this way.

Reporting a Mistaken Internet Payment

You must report a Mistaken Internet Payment as soon as possible. You can report a Mistaken Internet Payment by:

- contacting us on **13 11 75** within Australia;
- contacting us on **617 3362 2222**, if overseas; or
- visiting our branches.

You must give us full details of the transaction You are querying. We may require further information from You to investigate.

When You report a Mistaken Internet Payment 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.

When You Have Made a Mistaken Internet Payment

When You report a Mistaken Internet Payment to us, we as the Sending ADI, will investigate whether a Mistaken Internet Payment has occurred. We will require certain information to enable us to undertake that investigation, such as the BSB and Account number into which the Mistaken Internet Payment was made, the name of the party or the intended recipient and any further information You may have evidencing the mistake. We will contact You if we require further information.

If we are not satisfied that a Mistaken Internet Payment has occurred, we will not take any further action.

If we are satisfied that a Mistaken Internet Payment has occurred, we will send the Receiving ADI a request for the return of the funds. The Receiving ADI is required to acknowledge this request within 5 business days and advise us whether there are sufficient funds in the Account of the Unintended Recipient to cover the Mistaken Internet Payment.

The Receiving ADI will also investigate. If the Receiving ADI is not satisfied that a Mistaken Internet Payment has occurred, they will not return the funds.

We must inform You of the outcome of the reported Mistaken Internet Payment in writing and within 30 business days of the day on which You reported the Mistaken Internet Payment to us.

If the Receiving ADI returns the funds to us we will return the funds to You as soon as practicable. Usually, we will return funds to You by crediting the Account from which the Mistaken Internet Payment was made. If You no longer have an Account with us, or if it is

not practicable to credit the returned funds to that Account, we will return funds to You by some other means.

Where we and the Receiving ADI are satisfied that a Mistaken Internet Payment has occurred, but there are not sufficient credit funds available in the Account of the Unintended Recipient to the full value of the Mistaken Internet Payment, the Receiving ADI must use reasonable endeavours to retrieve the funds from the Unintended Recipient for return to You (for example, by facilitating repayment of the funds by the Unintended Recipient by instalments).

When a Mistaken Internet Payment Is Made Into Your Account

When a Sending ADI sends a request to us, as Receiving ADI, of a Mistaken Internet Payment having been made into Your Account, we will within 5 business days acknowledge that request and advise the Sending ADI whether there are sufficient funds in Your Account to cover the Mistaken Internet Payment.

We will investigate whether a Mistaken Internet Payment has occurred.

If we are not satisfied that a Mistaken Internet Payment has occurred, we are not required to take any further action but we may seek Your consent to return the funds.

If we are satisfied that a Mistaken Internet Payment has occurred, we will take action as follows:

(a) Process where funds are available and report is made within 10 business days

If a Mistaken Internet Payment is reported within **10 business days** after the payment is made, we are satisfied that a Mistaken Internet Payment has occurred, and there are sufficient funds in Your Account, we will withdraw the funds from Your Account and arrange for the return of the funds to the Sending ADI within 10 business days.

(b) Process where funds are available and report is made within 10 business days and 7 months

If a Mistaken Internet Payment is reported between **10 business days and 7 months** after the payment is made, we are satisfied that a Mistaken Internet Payment has occurred, and there are sufficient funds in Your Account, we will complete our investigation into the reported Mistaken Internet Payment within 10 business days of receiving the request. If we are satisfied that a Mistaken Internet Payment has occurred, we will place a hold on Your Account to prevent You from withdrawing the amount of the funds for a further 10 business days and notify You that we will withdraw the funds if You do not establish that You are entitled to the funds within that 10 business day period. If You fail to establish Your entitlement within 10 business days, we will return the funds to the sending ADI within 2 business days of the end of that period.

(c)Process where funds are available and report is made after 7 months

If a Mistaken Internet Payment is reported **more than 7 months** after the payment is made, there are sufficient funds in Your Account and we are satisfied that a Mistaken Internet Payment has occurred, we will ask You if You agree to the return of the funds to the sender. If You consent to the return of the funds we must return the funds to the sender.

(d)Process where funds are not available in Your Account

Where we and the Sending ADI are satisfied that a Mistaken Internet Payment has occurred, but there are not sufficient credit funds available in Your Account to the full value of the Mistaken Internet Payment, then we must use reasonable endeavours to

retrieve the funds from You for return to the sender (for example, by facilitating repayment of the funds by You by instalments).

In each case, if we are not satisfied that a Mistaken Internet Payment has occurred, we may (but are not obliged to) seek Your consent to return the funds.

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.

Centrelink Direct Credit Payments

Where the Unintended Recipient of a Mistaken Internet Payment is receiving income support payments from Centrelink, we will recover the funds from the Unintended Recipient in accordance with the Code of Operation for Centrelink Direct Credit Payments.

Complaints About Mistaken Internet Payments

If You report a Mistaken Internet Payment to us as Sending ADI and You are unhappy with our handling of the matter, You can make a complaint to us. Please refer to clause 1.7 in relation to making complaints. If a complaint is made to another ADI where we are the Receiving ADI, we must cooperate with the other ADI's dispute resolution scheme."

(n) 'Clause 22.7 Guidelines for Recording Your Secret Access Codes' is renamed to 'Clause 22.7 Secret Code Security Requirements'.

The following paragraph is inserted at the beginning of Clause 22.7:

"You must not voluntarily disclose one or more of Your Secret Codes to anyone, including a family member or friend."

The fullstop at the end of paragraph (h) in Clause 22.7 is deleted and replaced with the following:

"unless You make a reasonable attempt to protect the security of the Secret Code; or"

A new paragraph (i) is inserted in clause 22.7, immediately following paragraph (h):

"(i) where a Device is not needed to perform an ePayments Transaction keep a written record of all Secret Codes required to perform ePayments Transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the Secret Code(s)."

The last paragraph in Clause 22.7 is deleted.

(o) 'Clause 23.5 Electronic Funds Transfer Code of Conduct' is renamed to 'Clause 23.5 ePayments Code' and is deleted and replaced with:

"We agree to follow the rules of the ePayments Code for ePayments Transactions made in Australia and we give You a warranty that we will do so.

This does not apply to:

(a) an Account that is designed primarily for use by a business, and established primarily for business purposes, or
(b) a facility where You and Suncorp do not have a contractual relationship."

(p) 'Clause 23.6 You Secret Access Codes' is renamed to 'Clause 23.6 Your Secret Codes'.

The last paragraph in Clause 23.6 is deleted.

(q) 'Clause 23.7 Guidelines for Recording Your Secret Access Codes' is renamed to 'Clause 23.7 Secret Code Security Requirements'.

The following paragraph is inserted at the beginning of Clause 23.7:

"You must not voluntarily disclose one or more of Your Secret Codes to anyone, including a family member or friend."

The fullstop at the end of paragraph (h) in Clause 23.7 is deleted and replaced with the following:

"unless You make a reasonable attempt to protect the security of the Secret Code; or"

A new paragraph (i) is inserted in Clause 23.7, immediately following paragraph (h):

"(i) where a Device is not needed to perform an ePayments Transaction keep a written record of all Secret Codes required to perform ePayments Transactions on one or more articles liable to be lost or stolen simultaneously, without making a reasonable attempt to protect the security of the Secret Code(s)."

The last paragraph in Clause 23.7 is deleted.

(r) 'Clause 23.9 When You are Not Liable For Any Losses' is deleted and replaced with the following:

"An unauthorised transaction, that is a transaction You do not authorise, does not include any transaction carried out by You or by anyone performing a transaction with Your knowledge and consent. You will not be liable for losses resulting from unauthorised transactions where it is clear that You have not contributed to the loss.

Where You do not authorise a transaction, You will not be responsible for losses which:

(a) are caused by fraudulent or negligent conduct of our staff or agents of ours or third parties involved in networking arrangements or merchants or their agents or employees;

(b) losses relating to a Identifier, Device or Secret Code which is forged, faulty, expired, or cancelled;

(c) losses that arise from a transaction which required the use of any Device and / or Secret Code forming part of Your access method and that occurred before You received any Device and / or Secret Code or reissued Device and / or Secret Code;

(d) are caused by the same transaction being incorrectly debited more than once to the same Account;

(e) arise from unauthorised transactions performed after we have been informed that the Device has been misused, lost or stolen or the security of the Secret Code has been breached;

(f) arising from unauthorised transactions that can be made using an Identifier without a Secret Code or Device or can be made using a Device, or a Device and an Identifier, but does not require a Secret Code, if You do not unreasonably delay reporting the loss or theft of the Device; and / or

(g) are losses which occur while our processes are unavailable, provided that a report is made within a reasonable time of the process again becoming generally available."

(s) 'Clause 23.10 When You are Liable for Losses' is deleted and replaced with the following:

"You will be liable for losses resulting from transactions which are carried out by You or by another person with Your knowledge and consent.

Where we can prove on the balance of probability that You have contributed to a loss through fraud, or breaching the Secret Code security requirements in clause 23.6, clause 23.7 and clause 23.11:

(a) You are liable in full for the actual losses that occur before the loss, theft or misuse of a Device or breach of Secret Code security is reported to us, but

(b) You are not liable for the portion of losses:

(i) incurred on any one day that exceeds any applicable daily transaction limit,
(ii) incurred in any period that exceeds any applicable periodic transaction limit,
(iii) that exceeds the balance on the Account, including any pre-arranged credit, or
(iv) incurred on any Account that we and You had not agreed could be accessed using the Device or Identifier and/or Secret Code used to perform the transaction.

Where:

(a) more than one Secret Code is required to perform a transaction, and

(b) we prove that You breached the Secret Code security requirements in clause 23.6, clause 23.7 and clause 23.11 for one or more of the required Secret Codes, but not all of the required Secret Codes,

You are liable as outlined above only if we prove on the balance of probability that the breach of the Secret Code security requirements under clause 23.6, clause 23.7 and clause 23.11 was more than 50% responsible for the losses, when assessed together with all the contributing causes.

You are liable for losses arising from unauthorised transactions that occur because You contributed to losses by leaving a card in an ATM, as long as the ATM incorporates reasonable safety standards that mitigate the risk of a card being left in the ATM.

Where we can prove, on the balance of probability, that You contributed to losses resulting from an unauthorised transaction by unreasonably delaying reporting the misuse, loss or theft of a Device, or that the security of all Secret Codes has been breached, You:

(a) are liable for the actual losses that occur between:

(i) when You became aware of the security compromise, or should reasonably have become aware in the case of a lost or stolen Device, and
(ii) when the security compromise was reported to us, but

(b) are not liable for any portion of the losses:

(i) incurred on any one day that exceeds any applicable daily transaction limit,
(ii) incurred in any period that exceeds any applicable periodic transaction limit,
(iii) that exceeds the balance on the Account, including any pre-arranged credit, or
(iv) incurred on any Account that we and You had not agreed could be accessed using the Device and/or Secret Code used to perform the transaction.

Where a Secret Code was required to perform the unauthorised transactions, and the other circumstances outlined in this clause above do not apply, You are liable for the least of:

(a) $150.00, or a lower figure determined by us,

(b) the balance of the Account or Accounts which we and You have agreed may be accessed using the Device and / or Secret Code, including any prearranged credit, or

(c) the actual loss at the time the misuse, loss or theft of a Device or breach of the Secret Code security is reported to us, excluding that portion of the losses incurred on any one day which exceeds any relevant daily transaction limit or any other periodic transaction limit.

We, or our external dispute resolution body, have a discretion to reduce Your liability in the circumstances set out in the ePayments Code.

If You report an unauthorised transaction on a debit card Account:

(a) we must not hold You liable for losses under this clause for an amount greater than the liability of You if we exercised any rights we had under the rules of the card scheme at the time the report was made, against other parties to the scheme (for example, charge-back rights), and

(b) this clause does not require us to exercise any rights we may have under the rules of the card scheme. However, we cannot hold You liable under this clause for a greater amount than would apply if we had exercised those rights."

(t) Insert a new clause 23.20 as follows, immediately following existing clause 23.19:

"23.20 Mistaken Internet Payments

When the ePayments Code applies to a transaction made through an internet banking facility, we are bound by and follow the rules of the ePayments Code in relation to Mistaken Internet Payments. Other ADIs who have subscribed to the ePayments Code are required to follow the same processes. These processes do not apply to transactions where the 'Pay Anyone' internet banking service used is a service designed primarily for use by a business and established primarily for business purposes.

This clause sets out how we will deal with Mistaken Internet Payments made by You and Mistaken Internet Payments received into Your Account. You agree to us dealing with Mistaken Internet Payments in this way.

Reporting a Mistaken Internet Payment

You must report a Mistaken Internet Payment as soon as possible. You can report a Mistaken Internet Payment by:

- contacting us on **13 11 75** within Australia;
- contacting us on **617 3362 2222**, if overseas; or
- visiting our branches.

You must give us full details of the transaction You are querying. We may require further information from You to investigate.

When You report a Mistaken Internet Payment 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.

When You Have Made a Mistaken Internet Payment

When You report a Mistaken Internet Payment to us, we as the Sending ADI, will investigate whether a Mistaken Internet Payment has occurred. We will require certain information to enable us to undertake that investigation, such as the BSB and Account number into which the Mistaken Internet Payment was made, the name of the party or the intended recipient and any further information You may have evidencing the mistake. We will contact You if we require further information.

If we are not satisfied that a Mistaken Internet Payment has occurred, we will not take any further action.

If we are satisfied that a Mistaken Internet Payment has occurred, we will send the Receiving ADI a request for the return of the funds. The Receiving ADI is required to acknowledge this request within 5 business days and advise us whether there are sufficient funds in the Account of the Unintended Recipient to cover the Mistaken Internet Payment.

The Receiving ADI will also investigate. If the Receiving ADI is not satisfied that a Mistaken Internet Payment has occurred, they will not return the funds.

We must inform You of the outcome of the reported Mistaken Internet Payment in writing and within 30 business days of the day on which You reported the Mistaken Internet Payment to us.

If the Receiving ADI returns the funds to us we will return the funds to You as soon as practicable. Usually, we will return funds to You by crediting the Account from which the Mistaken Internet Payment was made. If You no longer have an Account with us, or if it is not practicable to credit the returned funds to that Account, we will return funds to You by some other means.

Where we and the Receiving ADI are satisfied that a Mistaken Internet Payment has occurred, but there are not sufficient credit funds available in the Account of the Unintended Recipient to the full value of the Mistaken Internet Payment, the Receiving ADI must use reasonable endeavours to retrieve the funds from the Unintended Recipient for return to You (for example, by facilitating repayment of the funds by the Unintended Recipient by instalments).

When a Mistaken Internet Payment Is Made Into Your Account

When a Sending ADI sends a request to us, as Receiving ADI, of a Mistaken Internet Payment having been made into Your Account, we will within 5 business days acknowledge that request and advise the Sending ADI whether there are sufficient funds in Your Account to cover the Mistaken Internet Payment.

We will investigate whether a Mistaken Internet Payment has occurred.

If we are not satisfied that a Mistaken Internet Payment has occurred, we are not required to take any further action but we may seek Your consent to return the funds.

If we are satisfied that a Mistaken Internet Payment has occurred, we will take action as follows:

(a) Process where funds are available and report is made within 10 business days

If a Mistaken Internet Payment is reported within **10 business days** after the payment is made, we are satisfied that a Mistaken Internet Payment has occurred, and there are sufficient funds in Your Account, we will withdraw the funds from Your Account and arrange for the return of the funds to the Sending ADI within 10 business days.

(b) Process where funds are available and report is made within 10 business days and 7 months

If a Mistaken Internet Payment is reported between **10 business days and 7 months** after the payment is made, we are satisfied that a Mistaken Internet Payment has occurred, and there are sufficient funds in Your Account, we will complete our investigation into the reported Mistaken Internet Payment within 10 business days of receiving the request. If we are satisfied that a Mistaken Internet Payment has occurred, we will place a hold on Your Account to prevent You from withdrawing the amount of the funds for a further 10 business days and notify You that we will withdraw the funds if You do not establish that You are entitled to the funds within that 10 business day period. If You fail to establish Your entitlement within 10 business days, we will return the funds to the sending ADI within 2 business days of the end of that period.

(c)Process where funds are available and report is made after 7 months

If a Mistaken Internet Payment is reported **more than 7 months** after the payment is made, there are sufficient funds in Your Account and we are satisfied that a Mistaken Internet Payment has occurred, we will ask You if You agree to the return of the funds to the sender. If You consent to the return of the funds we must return the funds to the sender.

(d)Process where funds are not available in Your Account

Where we and the Sending ADI are satisfied that a Mistaken Internet Payment has occurred, but there are not sufficient credit funds available in Your Account to the full value of the Mistaken Internet Payment, then we must use reasonable endeavours to retrieve the funds from You for return to the sender (for example, by facilitating repayment of the funds by You by instalments).

In each case, if we are not satisfied that a Mistaken Internet Payment has occurred, we may (but are not obliged to) seek Your consent to return the funds.

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.

Centrelink Direct Credit Payments

Where the Unintended Recipient of a Mistaken Internet Payment is receiving income support payments from Centrelink, we will recover the funds from the Unintended Recipient in accordance with the Code of Operation for Centrelink Direct Credit Payments.

Complaints About Mistaken Internet Payments

If You report a Mistaken Internet Payment to us as Sending ADI and You are unhappy with our handling of the matter, You can make a complaint to us. Please refer to clause 1.7 in relation to making complaints. If a complaint is made to another ADI where we are the Receiving ADI, we must cooperate with the other ADI's dispute resolution scheme."

(u) The following definitions have been inserted in alphabetical order in 'Clause 23.28 Definitions':

"ADI" has the same meaning as authorised deposit-taking institution in the Banking Act 1959 (Cth) or any successor term adopted by the Australian Prudential Regulation Authority.

"Device" means a device given by us to You that is used to perform an ePayments transaction. Examples include:

• ATM or transaction card,
• debit card or credit card,
• prepaid card (including gift card), and
• security token issued by us that generates a security code.

"ePayments Code" means the ePayments Code issued by the Australian Securities and Investments Commission.

"ePayments Transaction" has the meaning provided for in clause 20.1.

"Identifier" means information that You know and must provide to perform an ePayments Transaction but which You are not required to keep secret (for example, an account number).

.

"Party to a Shared Electronic Payments Network" includes retailers, merchants, communications services providers and other organisations offering facilities, merchant acquirers and us.

"Receiving ADI" means an ADI which is a subscriber to the ePayments Code and whose customer has received an internet payment which You have reported as being a Mistaken Internet Payment.

"Sending ADI" means an ADI which is a subscriber to the ePayments Code and whose customer has made an internet payment which has been reported as being a Mistaken Internet Payment.

"Mistaken Internet Payment" means a payment using a 'pay anyone' internet banking facility (for example, an external funds transfer) processed by an ADI through direct entry where funds are paid into the account of an Unintended Recipient because the transferor entered or selected a BSB number and/or Identifier that does not belong to the named and/or intended recipient as a result of:

• the transferor's error, or

• the transferor being advised of the wrong BSB number and/or Identifier.

It does not include payments made using Bpay.

"Unintended Recipient" means the recipient of funds as a result of a Mistaken Internet Payment.