ELECTRONIC BANKING AND CARD SECURITY

Heritage Bank

Important information to help you protect your account.

PIN/PAN/Password (Code) Security
It is important to treat any password, PIN or PAN that enables access to your account as top secret. To ensure its confidentiality, and to reduce the chance of suffering any loss, you should:

- Memorise the Code by choosing a Code that is meaningful **only to you**. You should not choose any code that may be easy for a third party to guess, e.g. '1234', 'AAAA' or codes related to personally identifiable information such as your postcode, date of birth or a recognisable part of your name
- Not record the Code in reverse order, or disguised as a phone number or date where no other phone numbers or dates exist
- Not record the Code in an easily understood format, eg A=1, B=2, C=3
- Not record the Code as a series of numbers with the actual numbers circled or highlighted in any way
- Not keep a record of your Code on, with, or near your card, passbook or devices
- Not tell anyone your Code, including friends, family and Heritage staff. Heritage will never contact you to ask you for this information
- Not allow another person to see you enter your Code.

If you do not treat your Code as top secret, you may be contributing to any losses which result from unauthorised transactions using your card, passbook, telephone banking or on-line banking and you could be liable for all or part of the losses.

Card Skimming
Card skimming is the criminal practice of copying information contained on the black magnetic strip found on the back of cards. A criminal can illegally attach a 'card reading' device to EFTPOS machines or ATMs that copies card data whenever a card is swiped or inserted. Data copied by a card reader can later be reproduced onto a 'fake card' so the criminal can fraudulently withdraw money or purchase goods. Card reading devices are usually small and difficult to detect. In ATMs, criminals can strategically attach a small camera to capture and record the Personal Identification Number (PIN) entered by the cardholder. Recording the PIN can allow a criminal to withdraw cash from a cardholder's account in conjunction with a fake card.

Since 2009, Heritage has integrated a special 'chip' into Visa cards. These cards are referred to as 'chip cards' and will help reduce the risk associated with card skimming.

What can you do to prevent card fraud?
To assist with the prevention of card fraud and in particular card skimming, Heritage encourages you to:

1. **Be observant** and study the ATM you are using BEFORE inserting your card. If the ATM appears as if it has been tampered with, do not use it and advise your concerns to the financial institution that owns the ATM. Be aware of who is watching you when you are using the ATM and always ensure that you cover the entry of your PIN with your other hand.
2. **Swipe your card yourself** for EFTPOS transactions and never allow the sales person to remove the card from your sight.
3. **Be aware of who you transact with** – only do business with reputable merchants or vendors and ignore unsolicited emails and phone calls seeking personal or account information.
4. **Be wary of providing credit card details over the internet** – while a number of sites are secure for credit card details, this is the most vulnerable type of transaction as you are not dealing with the vendor face-to-face.
5. **Maintain a minimum balance in your account accessed by your Visa debit card** – Your Visa debit card allows you to access your own funds anywhere at anytime. In order to minimise any risk in the event of your card being compromised it is recommended that you only keep minimal funds in accounts which are accessed by your Visa debit card. Your account can then be topped up utilising your internet banking facility, telephone banking or by contacting Heritage on 13 14 22.
6. **Monitor your account statements** and check all transactions, especially if you have recently returned from overseas travel. Notify your nearest Heritage branch if you detect anything unusual.
7. **Contact Heritage on 13 14 22** if you are planning to travel overseas and you will be using a Heritage Visa card. We can give you further tips on how to minimise your risk.
8. **Protect your cards** as if they were cash and always keep them in a secure place.
9. **Memorise your PIN** and never write it down.
10. **Report your lost or stolen Heritage cards immediately** by calling 1800 076 037, or if you are overseas call +61 7 4694 9139. You can also deactivate your card through Heritage on-line internet banking or the Mobile Banking app.

Liability for Unauthorised Transactions
Note: The details under this heading are written to reflect the provision of the ePayments code and apply to all ePayment accounts other than those designed primarily for use by a business and established primarily for business purposes. Except in relation to those business accounts, the determination of whether a transaction is authorised or not, and of your liability for an unauthorised ePayment transaction, will be made in accordance with the ePayments code.
An unauthorised transaction on an account is a transaction which is not authorised by an authorised user. Therefore, a transaction carried out by, or with the consent of an authorised user is not an unauthorised transaction. Heritage will treat any transaction carried out by any authorised user as authorised by the accountholder unless prior to the transaction, the accountholder has told Heritage to cancel that authorised user's card or device and the card or device issued to that authorised user is destroyed.

If you are an accountholder, your liability to Heritage for any unauthorised transaction shall not exceed the least of:

- The actual loss at the time of notification to us of the loss, theft or misuse of the card or other device;
- The balance of the account, including any pre-arranged credit;
- $150.

This does not apply in instances where the accountholder or an authorised user has contributed to the loss:

- Through the accountholder's or the authorised user's fraud or extreme carelessness;
- By voluntarily disclosing any code;
- By recording or indicating the code in any form on a related card or security token;
- By failing to reasonably disguise the code if recorded on any item kept with or near a related card or security token;
- By unreasonably delaying notification to us of the misuse, loss or theft of the card or security token, or that the security of a code had been breached;
- If the code was liable to loss or theft with a related card or security token;
- Through unauthorised transactions that occur because the user left their card in an ATM.

In those instances, the accountholder's liability shall not exceed the least of:

- The actual loss at the time of notification to us of the loss, theft or misuse of the card or security token;
- The balance of the account including any pre-arranged credit; and
- The maximum amount that the accountholder or authorised user would have been entitled to access over the relevant period prior to notification of the loss, theft or misuse of the card or security token, calculated by multiplying any daily transaction limit by the number of days on which there was unauthorised use.

The accountholder will not be liable for losses caused by the failure of any electronic funds transfer system or equipment to complete a transaction accepted by a terminal. However, where the accountholder or authorised user at the time of the transaction should have been aware that the system or equipment was unavailable for use or malfunctioning, our liability will be limited to correction of any errors in the account and the refund of any charges or fees imposed as a result.

Are your contact details up to date?

We will keep in touch with you via letters, account statements, email and other written material to you:

- at a postal, residential or business address that we have recorded for you or that we believe is then your current postal, residential or business address; or
- by fax to a fax number that you have given us to send faxes to you; or
- by electronic notification to any electronic address, electronic equipment or device you have provided the details of to Heritage or by being made available for retrieval from our website by electronic communication (if the use of this method is restricted by law or the ePayments Code, we will only use this method if we follow any applicable requirements)