# Important Information on Security Regarding Electronic Account Access and Regular Payment

Effective date: 1st March 2019

## Bank of Heritage Isle

**Contact Centre**
134 374

**Launceston Branch**
69 St John Street, Launceston 7250
(03) 6348 3400

**George Town Branch**
72 Macquarie Street, George Town 7253
(03) 6380 3400

**Beaconsfield Branch**
133 Weld Street, Beaconsfield 7270
(03) 6383 3588

**Email**
info@heritageisle.com.au

**Website**
www.heritageisle.com.au

Bank of Heritage Isle

Bank of Heritage Isle

## Contents

Bank of Heritage Isle

## Electronic Account Access

These guidelines are provided to assist you in maintaining security for accounts where transactions may be carried out through electronic access. Information is also provided regarding your liability for transactions on your accounts through electronic access.

## Summary of Security Guidelines

### Internet and Mobile Banking

The Bank employs the third-party verification (SSL certificate) to ensure uncompromised identity. Effectively, every time a user is connected to the Bank's Internet Banking facility, the SSL "handshake" occurs where a browser requires authentication from the Bank's server. If the information does not match or the certificate has expired, the browser displays an error message.

Using SSL technology also ensures that all information exchanged during your Internet Banking session is encrypted, scrambling the transmission and guaranteeing message privacy and integrity.

For Internet Banking, we have also implemented a second factor authentication function known as a *Captcha* test (Completely Automated Public Turing Test To Tell Computers and Humans Apart). Captcha is functionality that protects websites against unwarranted attacks from Trojans by generating text that humans can read easily but current computer programs cannot.

Security tokens are available to download onto most mobile phones, providing extra security without having to carry a token. To find out whether it is available on your mobile, or to download the software visit our website.

To activate your Mobile Phone Token or for more information please call the Contact Centre on 134 374.

### Redidial Telephone Banking

We employ a telephone banking system (Redidial) which only allows you to access your accounts after you have provided your access code electronically over the telephone.

### Cards

For EFTPOS and ATM transactions, (where you press savings or cheque account) we employ an electronic card access system which only allows access to your accounts after you have provided your personal identification number (PIN).

There may be no need for PIN authority for small transactions or PayWave transactions.

## What You Need to Do to Maintain Security

### PIN, Password and App Passcode Security

- Never record your PIN or password on your card or on anything that you usually keep with or near your card. We recommend you memorise your PIN and password. Also never use your PIN as a password or App passcode;
- Destroy any notification we send you containing PIN or passwords;
- When selecting a PIN, password or App passcode, do not choose numbers and letters that can be easily identified or associated with you (such as initials, phone numbers, date of birth etc);
- Try not to use the same PIN, password or App passcode for every service;
- Never disclose your PIN, password or App passcode to anyone. No employee from the Bank, the police or a merchant should ask for your PIN or password.

### Internet Banking, Mobile Banking App and Website Security

- Always log in directly by typing our site address www.heritageisle.com.au from your browser;
- When using internet banking, check for a locked padlock symbol. This indicates that it is secure to use;
- Never accept links or redirections from other websites or emails for the purpose of logging into internet banking. Never click on an email that asks for your personal banking information, and beware of phishing emails;
- Change your password regularly. Never write your password down, store it on your computer and/or mobile device;
- Install anti-virus, anti-spyware and firewall software on your computer. If you use our Mobile Banking Service we recommend you also install anti-virus software on your phone to reduce the risk of phone hacking. To get the most benefit from this software, make sure you always keep it updated;
- When performing financial transactions online, never leave your computer or mobile phone unattended while the session is still active;
- If you use Mobile Banking you should ensure you place a password/PIN on your phone in case you lose your phone, to secure against unauthorised access to your accounts.
- Be careful about using internet banking from other PC's (such as those at some Internet Cafés) which may not have up-to-date virus protection installed;
- Always log off when you are finished using internet or mobile banking to avoid others accessing your account details;
- Safeguard your account details if you save or print them. Keep this information in a secure place or destroy it once you have finished with it;
- You should clear your browser cache files at the end of a session;
- Beware of windows that "pop-up" during an Internet Banking session and be very suspicious if it directs you to another site which then requests your account details or password.

### Cards

- Report lost or stolen cards immediately to us on 134 374.
- Sign your card on the signature panel as soon as you receive it.
- Protect your cards as if they were cash, always keep them in a secure place.
- Ensure that you get your card back after every purchase.
- Always check sales vouchers for the correct purchase amount before you authorise them, and keep copies of your vouchers and ATM receipts.
- Always check your billing statement and verify the amounts of your purchases. Report any unauthorised transactions to the Bank immediately on 134 374.
- Destroy all old, cancelled or expired cards.
- When destroying your old card, be sure to cut vertically through the magnetic strip before disposing of it.
- Don't lend your card to anyone. You are responsible for all card transactions.
- If you are going overseas, tell us first, so we can better monitor your transactions.

## Summary of Liability Guidelines

### Liability for Use by an Authorised Person

Where you have provided the means to access your accounts electronically to another person by:

- Authorising that person to have a Visa Card and/or Redicard linked to your accounts; or
- Against our advice giving your access code details to that person, you are liable for transactions on your accounts carried out by that person.

### Liability for Loss through Unauthorised Use

Report any suspicious activity on your account immediately to our Contact Centre on 134 374.

Failure to report breaches to your account promptly may affect your liability for your loss.

Where there has been unauthorised use of your Visa Card, Redicard or access code, you are not liable for your loss if it is clear you have not contributed to your loss (and the transactions involved were carried out without your knowledge and consent).

However, if we establish you contributed to the unauthorised use, then you are liable for the lesser of:-

- The actual losses; or
- The amount you are able to withdraw from your account; or
- The total amount you would have been allowed to withdraw on the days that the unauthorised use occurred; or
- The balance in the account accessed, including if applicable, the amount available through an Overdraft or Credit Card facility. If you delay in notifying us, then in addition to the previously mentioned losses, you are liable for the losses incurred (because of that delay on the same terms as previously detailed); or
- The losses arising from unauthorised transactions that occur because your card has been left in an ATM, where the ATM incorporates reasonable safety standards that mitigate the risk of the card being left in the ATM.
- You are not liable where:-
- The losses are caused by the fraudulent or negligent conduct of our employees;
- The losses relate to any component of internet banking that is forged, faulty, expired or cancelled;
- The losses arise before we provide you with an access code or the losses are caused by the same transaction being incorrectly debited more than once to the same account;
- The unauthorised use takes place after you tell us that your access code has been misused, lost or stolen or has become known to an unauthorised person.
- In all other circumstances not covered above, you are liable for the lesser of:-
- $150.00; or
- The balance in the account accessed including, if applicable, the amount available through an Overdraft or Credit Card facility; or
- The actual loss at the time we are notified of the loss, theft and/or misuse.

### ePayments Code

These guidelines will always be read in conjunction with the ePayments Code (available by contacting 134 374). In the event of any discrepancy between these guidelines and the ePayments Code, your liability for loss (if any) will be determined under the ePayments Code.

## Regular Payment Arrangements

### What is a 'Regular' Payment?

Regular payments can be either a recurring payment or an instalment payment. A Regular Payment represents an agreement between you (the cardholder) and a merchant in which you preauthorise the merchant to bill your card account at predetermined intervals (e.g. monthly or quarterly) or at intervals as agreed by you. The amount may differ or be the same for each transaction.

For example: You may ask your local gymnasium to charge your monthly gym membership fee to your credit card each month; or,

You may have purchased a new television from your local appliance store and are being billed by the merchant in subsequent multiple periods.

### What are the benefits of Regular Payments?

There are many benefits for cardholders who set up regular payments including:

1. Ensures timely payments to the merchant.
2. Saves you time as the payment is processed automatically.
3. Saves you money as you do not have to pay for cheques, money transfers or postage, nor will you be liable for late fees.

Regular payment arrangements are an agreement between you (the cardholder) and the merchant. You should keep a record of all regular payment arrangements you have established with your merchant and store in a safe place. A template for recording your regular payment arrangements is available from APCA's website www.apca.com.au

You are responsible for notifying the merchant when your account details change, including a change in card number and/or change of card expiry date. Until you notify the merchant, your bank is required to process transactions from the merchant. Visit the Account Switching Service on our website www.heritageisle.com.au to generate a Change in account details letter to your merchant. We recommend you keep a copy of any Change in account details letter sent to your merchant and your earlier regular payment agreements. This correspondence will be required if your merchant does not comply to your request in a timely manner and you decide to dispute any incorrectly charged regular payments.

### Customer Rights to Dispute

Any issues with your regular payments, including the failure of the merchant to act on a change in account details advice, should be taken up directly with your merchant first.

Should further assistance be required to resolve an issue between yourself and a merchant, contact the Bank on 134 374 for more information.

To stop or alter a regular payment, you must provide either written instructions, phone us or visit a Service Centre. We will require full details of the regular payment at least (3) business days before the next payment is to be made.

Written instruction can be by using the Cancellation of Direct Debit/Regular Payment Form, letter, fax or email.

*Note: Cancellation of a regular payment does not cancel any contract arrangement between you and the supplier.*

Visit APCA's website www.apca.com.au to read FAQs on regular payments.

HDT13 V10 03/19