HEARTLAND BANK

Heartland Bank Australia Limited Privacy Policy

Table of contents

Approved by:
Board Risk Committee

Approval date:
October 2025

Policy owner:
Chief Risk Officer

Review frequency:
Biennial

1. Background and Objectives

Heartland Bank Australia Limited (Heartland) is a locally incorporated Authorised Deposit-Taking Institution (ADI). This Privacy Policy (Policy) applies to all legal entities, divisions, support functions and employees that act for or on behalf of Heartland or its subsidiaries and related bodies corporate including ASF Custodians Pty Ltd. Heartland collects, holds, and uses information about its customers to provide them with the products and services that they obtain from us. In cases where administrative functions are outsourced by Heartland to third party providers, they are permitted to follow their respective privacy policies provided they meet the requirements set out under the APPs.

Much of this information will be private or personal to our customers, and they would have an expectation that we would treat this information as confidential, only disclosing it in certain circumstances. In respect of natural living persons, the Privacy Act 1988 (Privacy Act) establishes a set of Australian Privacy Principles (APPs) to govern how Personal Information is handled. Heartland may also be subject to regulatory obligations outside of Australia related to Privacy and Breach Management.

Heartland may also collect Personal Information from potential customers, employees, potential employees, contractors, suppliers, brokers or industry and professional contacts. Whilst the focus of this document is on Heartland's customers, the collection, use and disclosure of any Personal Information by Heartland's employees from any source is governed by this Policy. This Policy incorporates Heartland's internal procedures regarding its obligations under the APPs as well as obligations under its more general duty of confidentiality. Whilst this is a non-public document, Heartland publishes a customer-facing Privacy Policy on its public websites which sets out how it manages Personal Information in reference to the site in question. Website versions of our customer- facing Privacy Policies are provided as Appendix 1 (PRIVACY POLICY (WEB VERSION -- HEARTLAND) and Appendix 2 (PRIVACY POLICY (WEB VERSION -- STOCKCO).

This Policy should be read in conjunction with the Heartland's Document Governance Policy.

2. Scope

2.1. Foreign Jurisdictions

Heartland may have operations in jurisdictions other than Australia (including entities and divisions established outside of Australia) and must consider local laws, rules and regulations that may conflict or require stricter practices than those set out in this Policy. Where local requirements are more stringent than those outlined in this Policy, the local requirements will always prevail. If there is a direct conflict between local laws and the requirements under this Policy, management must notify the Policy Owner prior to implementation.

3. Application and Interpretation

The applicability of this Policy to relevant Heartland employees will be dependent on the scope and type of work undertaken at Heartland and whether the Personal Information being handled relates to information about other staff members, customers, prospective customers, or industry and professional contacts. Generally, the obligations contained in section 7 below relate only to Personal Information and Sensitive Information in respect of natural living persons whether they are customers, suppliers, or contractors etc. of Heartland or not.

4. References

This Policy should be read in conjunction with the obligations set out in the:

- Information Retention and Storage Policy;
- Information Security Policy;
- AML/CTF Program;
- Outsourcing Policy;
- Complaint and Dispute Resolution Policy;
- Consumer Data Right Policy;
- Data Breach Response Plan.

5. Key Terms

ADI	Authorised Deposit-Taking Institution
AML/CTF	Anti Money-Laundering and Counter-Terrorism Financing
APPs	Australian Privacy Principles
CDR	Consumer Data Right
Heartland	Heartland Bank Australia Limited (ACN 087 651 750)
OAIC	Office of the Australian Information Commissioner
Policy	Privacy Policy
Privacy Act	Privacy Act 1988
TFN	Tax File Number

6. Privacy Act Overview

6.1. What is the Privacy Act?

The Privacy Act was introduced to promote and protect the privacy of individuals and to regulate how handle personal information. The Privacy Act includes 13 APPs. The Privacy Act also regulates the privacy component of the consumer credit reporting system, tax file numbers, and health and medical research.

6.2. What is Personal Information?

Personal information includes a broad range of information,

or an opinion, which could identify an individual. What is personal information will vary, depending on whether a person can be identified or is reasonably identifiable in the circumstances. Personal information may include, but is not limited to:

- an individual's name, signature, address, email, phone number or date of birth;
- sensitive information;
- financial and credit information;
- employee record information;
- photographs;
- internet protocol (IP) addresses;
- voice print and facial recognition biometrics; and/or
- location information from a mobile device (because it can reveal user activity patterns and habits).

6.3. What is Sensitive Information?

Sensitive information is personal information that includes information or an opinion about an individual's:

- racial or ethnic origin;
- political opinions or associations;
- religious or philosophical beliefs;
- trade union membership or associations;
- sexual orientation or practices;
- criminal record;
- health or genetic information; and/or
- some aspects of biometric information.

Generally, sensitive information has a higher level of privacy protection than other personal information.

6.4. What are the APPs?

There are 13 APPs, and they govern standards, rights and obligations around:

- the collection, use and disclosure of personal information;
- an organisation or agency's governance and accountability;
- integrity and correction of personal information;
- the rights of individuals to access their personal information.

For more information, see Australian Privacy Principles.

7. Specific Obligations and Accountabilities

The following specific obligations and accountabilities are designed to satisfy both the obligations arising under the APPs in the Privacy Act in respect of individuals, as well as the general duties of confidentiality owed to customers (whether they are natural living persons or legal persons).

7.1. Collection of Personal Information

Heartland must only collect Personal Information that is reasonably necessary for one or more of its functions or activities. Heartland will primarily collect Personal Information for the purpose of providing a customer with a financial product or service (including where required to do so by law).

Heartland will also collect Personal Information to promote our products and services, and to provide updates and marketing material to individuals that expressed an interest in receiving further communications from Heartland. Where it is reasonable and practicable to do so, Heartland must collect the information directly from the individual. Whether information is collected directly or indirectly, Heartland must ensure there is disclosure including the following:

- Heartland's identity and contact details;
- The fact that it has collected the information (if the individual may be unaware);
- If the collection is required under Australian law or court order, the fact that it is so authorised (and name of relevant law);
- The fact that the individual can request access to their information;
- The purposes for which the information is collected;
- The consequences if the information is not provided;
- What disclosures of that information may be made, including the names (or types) of entities to which it may usually disclose Personal Information collected by it;
- That the Privacy Policy explains how individuals may access or seek to correct Personal Information;
- That the Privacy Policy explains how a complaint may be lodged and how it will be dealt with; and
- At or before the time of collection or as soon as possible afterwards, whether it is likely to disclose the Personal Information to overseas recipients, and if so, the countries in which those recipients are likely to be located (if practicable to list them).

Heartland's customer-facing Privacy Policy(s), listed in the Appendices, are available on its public websites and referenced in relevant documentation such as Product Offer Documents, contains information addressing each of the above matters. The following sub-sections describe the main avenues through which Heartland collects Personal Information.

7.1.2. Customers

Personal Information is collected from application forms completed by customers in connection with products or services provided. The Privacy Policy sets out how Personal Information collected will be used and disclosed, along with the other matters that need to be disclosed to the customer. Personal Information may also be collected from individuals who complete forms to request information or services.

It should be noted that for customers who are legal persons, for example a trust, Personal Information may still be collected about individuals connected with the customer,

e.g., names, addresses and dates of birth of the trustees of a trust will be Personal Information and subject to the Privacy Act.

7.1.3. Prospective Customers

Where an individual makes enquiries about our products or services, but is not yet a customer, the information that they provide may be Personal Information and thus subject to the Privacy Act. Prospective customers should be referred to the Privacy Policy to inform them of the matters required above. Heartland may also collect Personal Information directly from Prospective Customers through forms or tools. Where Personal Information is collected through these channels, disclosure must occur.

7.1.4. Industry and Professional Contacts

Heartland sales and marketing teams use contact databases and client relationship management systems that include records of Personal Information about financial advisers, mortgage brokers and other industry and professional contacts (who also may provide us with customer and prospective customer information). All contact information, including Personal Information must be recorded in these databases or systems as it has appropriate security levels, access restrictions and the facilities for recording 'opt-out' instructions. Industry and professional contacts should refer to the Privacy Act or Privacy Policy to inform them of Privacy obligations.

7.1.5. Conducting Market Research

Whenever Heartland and/or its suppliers conduct surveys on customers, industry participants for perceptions of service levels, purchase intentions or brand recognition, Heartland will typically preserve their anonymity. Where Personal Information is collected in these surveys, participants will be informed of how the Personal Information will be used and disclosed and their consent to participate will be obtained.

7.1.6. Telephone

Heartland does not usually monitor or record staff phone calls. The exception to this is customer-facing outbound and inbound calls, such as to the Contact Centre, Customer File Managers, Compliance Administrators and Client Operations Administration teams, which may be monitored and recorded for coaching and training purposes. Where this occurs, the recordings are retained as outlined in the Information Retention and Storage Policy. In these instances, the staff-member, the customer, and any other party to the call must be made aware that this may take place and be provided with the option to request that the call is not recorded.

7.2. Use and Disclosure of Personal Information

Generally, Heartland can only use or disclose Personal Information for the primary purpose for which it was collected. Use or disclosure for a secondary purpose can occur where:

- The individual has consented (examples of this are where an individual consents to us disclosing information to their financial adviser, or their loan was originated by a financial adviser, mortgage broker, or other professional contact, and where we submit information to credit reporting agencies in performing credit checks, or to electronic verification service providers in performing identity checks);
- The secondary purpose is related to the primary purpose and the individual would reasonably expect this use or disclosure (if it is Sensitive Information, then the secondary purpose must be directly related to the primary purpose); or
- The secondary purpose is direct marketing, but only under certain circumstances as defined in APP 7.2.

Additionally, Heartland may use or disclose Personal Information in certain circumstances detailed in APP 6 such as where it is required or authorised by or under law, or for a permitted general situation such as where Heartland has reason to suspect that unlawful activity or serious misconduct that relates to Heartland's functions has been, is being, or may be engaged in (refer to the Heartland AML/CTF program for information regarding

suspicious matter reporting) or where reasonably necessary for a confidential alternative dispute resolution process (refer Heartland Complaint and Dispute Resolution Policy).

Requests for use or disclosure of personal information in circumstances that are not encountered in the ordinary course of business should be forwarded to the Privacy Officer to assess and document the need for disclosure.

To assist in ensuring that the above requirements are met, each business division must restrict access to the Personal Information that it holds so that it is only available to staff who need to use it to perform their work. Heartland staff must not attempt to access Personal Information where there is no requirement to do so.

Certain Heartland group entities may be considered 'Data Holders' under the Consumer Data Right ('CDR') as the regime is progressively rolled out. Where a Heartland entity is a Data Holder, they must be subject to a CDR Policy, and at the request of a consumer, transfer consumer data to an 'Accredited Data Recipient' under the CDR regime. The Data Holder must have the authorisation of the consumer prior to disclosing consumer data to an 'Accredited Data Recipient.' Further information is provided in the CDR Policy.

7.2.1. Direct Marketing

Heartland may use or disclose Personal Information for the purpose of direct marketing, only if;

- it collected the information from the individual (or their adviser) and the individual would reasonably expect it to use or disclose the information for that purpose; and
- it has provided a simple means by which the individual

can 'opt-out' of direct marketing; and
- the individual has not made such a request.

If an individual would not have a reasonable expectation that Heartland will use or disclose their Personal Information for the purpose of direct marketing, or where Heartland collected the Personal Information from someone other than the individual, then Heartland may only use or disclose the information for that purpose where it has (in addition to the above requirements) the relevant authority to do so. Heartland must provide a simple means for the individual to opt-out of receiving direct marketing communications and in each of these direct marketing communications must make the customer aware that they can opt-out.

Heartland may use personal information, such as email address or mobile number etc, to deliver marketing messages to through digital advertising platforms. This may include sharing hashed versions of information with third-party platforms for the purposes of audience targeting, remarketing, and measuring the effectiveness of our advertising campaigns.

Heartland use advertising technologies including cookies and pixels to help show relevant advertisements to individuals who have interacted with Heartland services or may be interested in Heartland services. These technologies may collect information about browsing activity on the Heartland website and mobile apps.

Cookies and similar technologies may be placed on devices to:

- Deliver advertisements that are more relevant;
- Build audiences for targeted advertising;
- Measure the performance of Heartland marketing efforts.

A cookie is a small data file sent from a website to a browser and stored on the computer to identify a unique user and store information about the session. Cookie preferences can be managed through browser settings, and individuals may opt out of personalised advertising by managing settings within the platforms.

If Heartland proposes to conduct marketing campaigns to persons that are not currently prospective (provided their information to us with disclosure) or actual customers of Heartland, the Privacy Officer and Legal should be consulted and care taken with respect to the requirements of the Spam Act 2003 and the Do Not Call Register Act 2006. Where an individual has indicated that they no longer wish to receive direct marketing from Heartland, this request must be actioned within five (5) business days.

7.3. CDR

Certain Heartland entities may be considered Data Holders under the CDR as the regime is progressively rolled out. Where a Heartland entity is a Data Holder, they must be subject to a CDR Policy, and at the request of a consumer, transfer consumer data to an Accredited Data Recipient under the CDR regime. The Data Holder must have the authorisation of the consumer prior to disclosing consumer data to an Accredited Data Recipient. Refer CDR Policy. Under the CDR Regime, an entity that is a Data Holder is required to respond to a request by a consumer to correct CDR data. The Data Holder must take correct the CDR data, include a qualifying statement, or provide reasons why a correction or statement is unnecessary or inappropriate. The Data Holder must provide notice to the consumer where a correction or qualifying statement is made in response to a correction request.

7.4. Data Quality

Heartland must take reasonable steps to ensure that the Personal Information it collects is accurate, up-to-date, and complete. When disclosing Personal Information, Heartland must ensure that, having regard to the purpose of using or disclosing the information, it is accurate, up-to-date, complete, and relevant. Customers are provided with the facility to update their details (for example via the call centre or by submitting forms) and these changes must be acted on promptly.

7.5. Data Security

Heartland must take reasonable steps to keep Personal Information secure from misuse, interference, or loss and from unauthorised access, modification, or disclosure. The Information Security Policy and the employee access control system are integral components in Heartland's approach to data security. The Information Security Policy applies to all employees and formally documents and communicates Heartland's framework for managing and protecting information.

7.6. Privacy Breach Management

Breaches will be managed in accordance with Data Breach Response Plan which considers guidance published by the OAIC in relation to the assessment and reporting of notifiable data breaches in accordance with the Privacy Act 1988 (as amended by the Privacy Amendment (Notifiable Data Breaches) Act 2017). See Data Breach Response Plan.

7.7. Openness

Heartland must set out in a document its policies on its management of Personal Information and must make this document available to anyone who asks for it. Heartland achieves this through the publication of its external Privacy Policy(s) on its public websites. If a person requests a copy and does not have access to the internet, a hardcopy version of the relevant Privacy Policy must be provided to them.

Where a person requests details from Heartland about generally what sort of Personal Information it holds, for what purposes, and how it collects, holds, uses, and discloses that information, Heartland must take reasonable steps to

provide that general information. Typically, a response to this sort of query should be satisfied by reference to the Privacy Policy available on the relevant public website.

7.8. Access and Correction

If an individual requests access to their Personal Information, Heartland must provide access within a reasonable period and in the manner requested by the individual (if reasonable and practicable to do so) unless an exception applies, such as where:

- it would be unlawful to provide the information; or
- providing access would be likely to prejudice an investigation of possible unlawful activity, or enforcement activities conducted by, or on behalf of, an enforcement body; or
- the information is relevant to legal proceedings and would not be accessible in the normal discovery process; or
- it would pose a serious and imminent threat to the life or health of any individual; or
- the request is frivolous or vexatious; or
- giving access would have an unreasonable impact on the privacy of other individuals; or
- giving access would divulge a commercially sensitive decision-making process.

If Heartland refuses to grant access (or grant access using the method requested) it will notify the individual in writing the reasons for refusal and a mechanism for them to complain about the refusal. All access requests should be sent to the Privacy Officer.

If Heartland is satisfied that the Personal Information it holds about an individual is inaccurate, out-of-date, incomplete, misleading, or irrelevant (to the purpose for which it is held), or it receives a request from an individual to correct their information, then it will take reasonable steps to correct it. Changes to account details should not be actioned based on an email request from an individual solely.

Some changes may be made over the phone (after security checks have been undertaken) or alternatively the appropriate form should be used. Policy specific information should not be provided through email, unless the client has requested this.

Aside from receiving customer requests, Heartland may also become aware that information requires correction by way of the procedure for handling returned mail. If Heartland and the individual disagree about the accuracy, completeness, or currency of our records, then the individual has the right to request that we note their disagreement on those records.

7.9. Identifiers

Heartland must not adopt government-issued identifiers for use as its own identifier. Government-issued identifiers include Medicare numbers and Drivers Licence numbers. Each business division must ensure that its databases for storing customer and other lists assign a unique identifier, and that they do not use government- issued identifiers to identify individuals on those databases.

7.9.1. Tax File Numbers

Heartland can only collect, use, or disclose TFNs for the purpose of carrying out responsibilities in accordance with relevant laws. Tax File Numbers are specifically subject to further protection under the Tax File Number Guidelines 2011 which were issued under section 17 of the Privacy Act. When collecting a Tax File Number (TFN), Heartland must ensure that the customer is informed:

- of the legal basis for the collections;
- that declining to provide a TFN is not an offence; and
- of the consequences of not providing their TFN, for example, they may be charged the highest marginal tax rate (plus levies) on income earnt.

Heartland must ensure TFN records are securely maintained to prevent loss or unauthorised access. Unauthorised use or disclosure of a TFN is an offence under the Tax Administration Act 1953.

7.10. Anonymity or Use of a Pseudonym

Heartland is required by law to identify its customers when entering into a designated product or service (see for example the requirements of the AML/CTF Act set out in the AML/CTF Program) and so is unable to provide the option of transacting anonymously or through the use of a pseudonym. Access to Heartland's public website does not require persons to identify themselves, and so information provided there may be done on the basis of anonymity. In addition, a customer may request information be sent to them without revealing their identity.

7.11. Overseas Disclosures

Heartland may share personal information with recipients located overseas, including some of our related bodies corporate or service providers. The countries in which these recipients are located include New Zealand. Information may also be held by data storage providers, including cloud-based data storage providers in Australia, New Zealand or elsewhere.

7.12. Sensitive Information

Heartland must not collect Sensitive Information about an individual unless the individual has consented, or the collection is required by law. Where Heartland collects Sensitive Information, it must be reasonably necessary for the performance of one or more of its functions or activities. For example, carrying out background checks on potential new employees may involve the handling of Sensitive Information.

7.13. The Data Life Cycle and Change Management

Heartland must consider the security of Personal Information before it purchases or develops information

systems. Privacy impact assessments and data security assessments help to ensure that the concept of 'privacy by design' is applied in relation to system development, assisting Heartland to identify security risks and implement appropriate controls to protect Personal Information over time, and ensure reasonable measures are taken to comply with any relevant requirements of the Privacy Act and APPs.

In this context, the term 'Project' should be interpreted broadly to include any business initiative, marketing campaign, product development or system change which could impact or alter the handling of Personal Information, which must be referred to the Privacy Officer, who will help to determine whether existing privacy controls and processes are adequate, and, if not, propose actions to address gaps. Possible actions may include updating policies, procedures, product disclosure statements, forms, third party agreements, training materials or delivering role-specific training. Enhancements to data access, storage and security controls may be required.

7.14. Privacy Management for Third Party Providers

Where Heartland engages a third party to provide services that involve that third party holding Personal Information on Heartland's behalf, or otherwise having access to such information, Heartland's privacy obligations continue to apply. Heartland has several controls in place to manage privacy risk arising through outsourcing arrangements. The Outsourcing Policy sets out due diligence considerations and contractual requirements that apply to new contracts carrying material privacy risk that involve the outsourcing of a Heartland business activity.

7.15. Complaints Management

Any complaints that relate to the Privacy Act must be documented, resolved or escalated promptly. The Privacy Officer must be notified of the complaint and kept always informed. While a complaint relating to privacy laws may be received through various channels (i.e., call centre, email, mail etc.) and reported under Heartland's existing Complaints procedure, the matter must be immediately referred to the Privacy Officer for consideration.

If there is a Privacy Breach, this must be reported to the Privacy Officer to arrange a privacy breach assessment to be undertaken.

If an individual making the complaint is not satisfied with our response, they may approach the OAIC to instigate an investigation. The customer-facing Privacy Policy (website) outlines how a complaint may be made and how it will be dealt with. Complaints may also be made to the Australian Financial Complaints Authority (AFCA), the external dispute resolution (EDR) scheme handling complaints about financial products and services. Where necessary, the Privacy Officer may also be consulted on an ad-hoc basis for specific advice or expertise on issues generally relating to privacy or confidential information.

8. Reporting Requirements

Eligible Data Breaches must be reported under the Privacy Act 1988 to both the OAIC and any affected individuals as soon as Heartland forms a reasonable belief that such a breach has occurred. Complaints relating to potential, actual or perceived breaches of privacy will be documented in either the Complaints Register and/or incidents register and/or issues register in Protecht.

9. Point of Contact

The Policy Owner is the point of contact for matters arising in relation to this Policy. In instances of uncertainty or need for clarification, a staff-member should speak initially to their people leader. If necessary, both the individual and leader can escalate matters, as necessary to the Privacy Officer.

This Privacy Policy will be reviewed at least every two years or as required if there are material changes in either the regulatory framework or Heartland business activities.

Appendix 1 – Privacy Policy (Web Version – Heartland)

1. What is our privacy policy?

At Heartland, we realise the importance of protecting your personal information whether it comes from you or through other sources. This Privacy Policy describes how we collect, store, and handle personal information, the types of personal information we collect, the purposes for which we use this information, to whom this information is disclosed and how you can communicate with us about your personal information.

In this policy, "we" or "us" refers to Heartland Bank Australia Limited ABN 54 087 651 750, and its related bodies corporate (as that term is defined in the Corporations Act 2001 (Cth)) including ASF Custodians Pty Ltd. We may change our Privacy Policy from time to time at our discretion. At any time, the latest version of our Privacy Policy is available from our website at https://www.heartlandbank.com.au/privacy-policy

2. What types of personal information do we collect?

Personal information is information about you that identifies you or from which your identity is apparent or can reasonably be worked out. It can include an opinion and does not necessarily need to include your name.

One kind of information that we regularly collect is credit information. Credit information is that part of your

information that we use to assess your eligibility for the credit products that we make available.

This can include details of any finance that you have available, your history in repaying credit and other information that credit providers use to assess eligibility. Section 6 below contains further information about credit information.

The kinds of personal information we are allowed to obtain about you, and the manner in which we collect, maintain and protect your personal information, are primarily governed by the Privacy Act and the Australian Privacy Principles (APPs) under that Act.

In addition, before we are able to provide you with financial products or services, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) ("AML/CTF Act") requires us to collect information about you in order to verify your identity. This information may also be provided to a credit reporting body for verification, or to third parties for the purposes of fraud prevention, Anti-Money Laundering and Counter-Terrorism Financing checks as required by law and identity verification. Section 7 below contains further information about the collection and verification of identification information.

The types of personal information we collect about you depend on the circumstances in which the information is collected. Such information may include:

- contact details (such as your name, address, email address and phone numbers);
- photographs of you;
- date of birth and gender;
- current occupation and employment history;
- education, qualifications and training;
- relationship status;
- details of individuals you are (or may be) connected to;
- financial information, such as information about your assets, finances, income, expenses and debit and credit history (including information obtained from credit reporting bodies);
- your tax file number; and/or
- information concerning your use of our products and services.

We also have access to information about your account(s) and transactions. This means we can see how and where you use your account(s). We may use this information to form a view on our other products and services that may benefit you.

We generally do not collect sensitive information about you unless required by applicable laws or rules. Sensitive information includes information in relation to:

- political or religious beliefs;
- race or ethnic origin;
- memberships of unions, trade or professional associations;
- criminal records; and/or
- health information.

If you do provide sensitive information to us for any reason, you consent to us collecting that information and to us using and disclosing that information for the purpose for which you disclosed it to us and as permitted by the Privacy Act and other relevant laws.

In addition to the types of personal information identified above, we may collect personal information as otherwise permitted or required by law.

We will only obtain, use or disclose government generated identifiers (for example, your tax file number) in circumstances where we are legally permitted or obliged to do so.

The scope of your personal information may include many records and documents. Should you require it, we would be happy to explain in greater detail what this information includes. Should you require it, you may also see the personal information we keep about you, subject to certain limitations set out in the Australian Privacy Principles. Please contact us if you require us to give you a further explanation.

3. How do we collect your personal information?

We collect personal information in a number of ways. The most common ways we collect your personal information are:

- directly from you, including when you request or use any of our products or services;
- from publicly available sources;
- from market research bodies who may have records about you from surveys and questionnaires you may have engaged in;
- from your personal representatives, including your solicitor, accountant and financial adviser;
- from distributors, agents and brokers, including insurance brokers or mortgage brokers you may have had contact with;
- from other credit providers you may have had contact with and credit reporting bodies;
- from Federal, State or Territory government departments and regulatory bodies; and/or
- from other third parties.

We may also collect information about how you use our website and mobile apps. For example, this may include your identity, date and time of your visits, number of visits, the type of products and services you view and how you use our website and mobile apps. We obtain information via our website through 'cookies' and related technologies. The use of cookies helps us monitor the effectiveness of our website and mobile apps.

A 'cookie' is a packet of information placed on a user's computer by a website which is used for record keeping. Cookies are used to monitor traffic on our website, but generally we do not collect personal information from you using cookies.

You can configure your browser to accept or reject cookies, or notify you when cookies are sent. If you disable the use of cookies on your web browser or reject cookies from us then you may not be able to gain access to all of the content or facilities that we offer.

Throughout our website and mobile apps we use the Google Universal Analytics system, Google Play Console and App Store Connect (as applicable) to measure anonymous website and mobile app activity. These services provide us with information about the use, functionality and effectiveness of our website and mobile apps, helping us to understand and optimise user experiences and to also optimise our advertising on, and outside of, our website and mobile apps. We may also use other third party data analytic software in the future and you may request a list of all data analytic software providers that we use from us at any time.

The information we collect from your general use of our websites and mobile apps does not identify you. It is general data regarding the number of visitors/users of our website and mobile apps, and statistics regarding their usage.

However, where you access functions of our website and mobile apps that require you to verify your identity by entering your log-on details and/or a password we will keep a record of that access to monitor and record transactional information within the secure parts of our website and mobile apps. We may store this information for a period of up to 7 years unless we reasonably need to store it for a longer period for example to resolve a complaint that you have made.

We may also monitor and/or record telephone discussions between you and our staff for training purposes and to check the accuracy of our records.

4. For what purposes do we collect, use and disclose your personal information?

The purposes for which we use and disclose your personal information will depend on the circumstances in which we collect it. Generally, we collect, use and disclose your personal information so that we can:

- establish who you are and assess your creditworthiness;
- assess applications for products and services;
- administer and monitor products or services;
- develop and run our business generally;
- comply with legal obligations and assist government departments and regulatory bodies; and/or
- tell you about other products or services that we think may be of interest to you.

We may also collect, use and disclose your information in other ways where permitted by law.

If you do not agree to give us certain types of personal information, we may be unable to provide you with the products or services you have asked for.

5. To whom may we give your personal information?

We may disclose your personal information to third parties in connection with the purposes described above. This generally includes disclosure to the following types of third parties:

- our related bodies corporate;
- other persons named in your application for a product or service with us;
- our service providers and contractors, including data storage providers in Australia or overseas;
- other financial and insurance institutions;
- identity verification agencies;
- debt collecting agencies;
- credit reporting bodies;
- government departments & regulatory bodies and issuers or official record holders of identity documents;
- your agents, advisers, referees, executors, administrators, trustees, guardians, beneficiaries (if you are a trustee) or attorneys;
- anyone to whom we consider assigning or transferring any of our rights or obligations; and/or
- other persons where this is permitted by law or to whom you have directed or otherwise permitted us to disclose your personal information to.

Where we disclose your personal information to third parties we will use reasonable endeavours to ensure that such third parties only use your personal information as reasonably required for the purpose we disclosed it to them and in a manner consistent with the Privacy Act. Third parties who access your personal information are required to adhere to appropriate security standards to protect your information from unauthorised access, destruction or loss.

6. Credit reports

When you apply to us for credit, we may request a credit report about you from a credit reporting body. A credit report contains information about your credit history which assists credit providers to assess your application, verify your identity and manage your accounts. Credit reporting bodies collect and exchange this information with credit providers.

The Privacy Act limits the information that credit providers can disclose about you to credit reporting bodies, as well as the ways in which credit providers can use credit reports. The information we may disclose includes your identification details, any applications for credit you have

made, the type and amount of credit you have, any failure to make repayments or defaults and whether you have committed a serious credit infringement (such as fraud). This is information we have collected through your use of our products and services. We may also ask credit reporting bodies to provide us with an overall assessment score of your creditworthiness.

The credit reporting bodies we may share information with are:

- Equifax (equifax.com.au);
- Illion (creditcheck.illion.com.au/) and/or
- Experian (experian.com.au).

Contact details and copies of their privacy policies are available on their websites.

We use information from credit reporting bodies to confirm your identity, assess applications for credit, manage our relationship with you and otherwise in order to comply with laws, regulations and codes of practice. This includes sharing your credit information with the entities listed in Section 5. We may combine the information from a credit reporting body with other information. Credit providers can ask credit reporting bodies to use your credit-related information to pre-screen you for direct marketing. You can ask a credit reporting body not to do this. You can also ask a credit reporting body to not use or disclose your credit information if you believe you have been, or are likely to be, a victim of fraud. To do this, contact the credit reporting body directly.

Sections 12 and 13 contain details about how you can access or correct any information we hold about you, how you can make a complaint about a data breach and how we will deal with any complaint.

7. Identity verification

Before we can provide you with financial products or services, we are required to collect information from you to verify your identity. This requirement applies to Australian financial institutions such as Heartland under the AML/CTF Act.

There are two methods we can use to verify your identity: electronic verification or a manual alternate method. Heartland may choose to use either electronic verification or a manual alternate method (or both) depending on the product you are applying for and the identification you have provided to us.

Electronic Verification

Under the AML/CTF Act, we can disclose your name, residential address and date of birth to a credit reporting body to assist in verifying your identity. The credit reporting body will then assess whether this information matches (in whole or part) information held in their records and in the records of government departments, an issuer or official record holder of identity documents, or other third parties (if any).

For us to complete electronic verification, you need to:

- be 18 years or over;
- have an Australian residential address;
- hold an acceptable form of identification; and
- consent to your identity being verified in this way.

Manual Alternate Method

If you cannot or choose not to be electronically verified, we must identify you using a manual alternate method for example by requesting originally certified copies of identifying documents such as your driver's licence, passport or other documents that verify your identity if you do not have a driver's licence or passport, or your name has been changed.

8. Does personal information leave Australia?

We may share your information with recipients located overseas, including some of our related bodies corporate or service providers. The countries in which these recipients are located include New Zealand. We take reasonable steps to ensure that these recipients protect your information in the same way that we do (although they may not be subject to Australian laws).

Your information may also be held on our behalf by data storage providers, including cloud-based data storage providers in Australia, New Zealand or elsewhere.

9. How do we protect your personal information?

We keep hard copy documents in our offices which are protected by building security and other office security measures. The electronic records that we keep are in computer systems that have firewalls, intrusion detection and virus scanning tools to protect against unauthorised access. We also maintain and monitor our online security systems.

Our staff are trained in the proper handling of personal information so that they are aware of the things they must do to protect your personal information. We also seek to ensure that appropriate data handling and security arrangements are in place when we send information overseas or use third parties that handle or store data.

However, the internet is not a secure environment and although care is taken, we cannot guarantee the security of information provided to us or stored or transferred via electronic means. You can help us protect your privacy by observing our security requirements and contacting us immediately if your contact details change. You should keep any usernames, passwords and pin codes secure and

confidential at all times, and not disclose them to any other person. Please contact us immediately using the details in Section 14 below if you believe that your username or password may have been disclosed to another person.

10. Direct marketing

We may use your information to inform you of other products and services that could be of interest to you, including through direct marketing. We may contact you from time to time to tell you about these products and services. If you don't want to receive direct marketing, you can ask us not to contact you and not to disclose your information to others for that purpose. If you would like to opt out of receiving our marketing, please contact us using the information provided below in Section 14.

We may use your personal information, such as your email address or mobile number etc, to deliver marketing messages to you through digital advertising platforms. This may include sharing hashed versions of your information with third-party platforms for the purposes of audience targeting, remarketing, and measuring the effectiveness of our advertising campaigns.

We use advertising technologies including cookies and pixels to help us show relevant advertisements to individuals who have interacted with our services or may be interested in our services. These technologies may collect information about your browsing activity on our website and mobile apps.

Cookies and similar technologies may be placed on your device to:

- Deliver advertisements that are more relevant to you;
- Build audiences for targeted advertising;
- Measure the performance of our marketing efforts.

You can manage your cookie preferences through your browser settings, and you may opt out of personalised advertising by managing your settings within the platforms.

We will not use or disclose sensitive information about you for direct marketing purposes unless you have consented to such use or disclosure.

11. Unsolicited information

Sometimes we receive personal information that we have not asked for, which can include sensitive information. If we receive such information, we will examine whether we are permitted to collect such information and, if we are, we will review the information and handle it in accordance with this Privacy Policy. If we are not able to collect such information and it is not in a government record, then we will destroy or de-identify the information as soon as possible, if it is lawful to do that.

There are occasions where it is difficult to separate sensitive information from other personal information and we may need to store information for future use including for regulatory reasons. Where this is the case, we will still keep the information in accordance with this Privacy Policy.

12. How can you access and correct your personal information?

If you wish to access the personal information we hold about you, you can contact us using the details in Section 14. We may require that the person requesting access provides suitable identification.

We will provide access to that information in accordance with the Privacy Act, subject to certain exemptions which may apply. Access may not be provided where the information would disclose personal information about someone else, would disclose commercially sensitive matters (including our business operations and decision making processes) or is protected from disclosure by law. If you have requested to see your information and we are not able to disclose it to you, then we will tell you and give you reasons.

We will usually provide your personal information free of charge. However, in some cases we may need to charge you an administration fee (such as when your request requires us to obtain information that is not readily available).

If you think that any personal information we hold is incorrect or out of date, then you can ask us to correct or update it. If your request relates to credit related information provided by others, we may need to consult with credit reporting bodies or other credit providers before being able to correct or update the information. If we disagree that the information should be corrected, then we will tell you and give you reasons.

13. What can you do if you have a privacy issue?

If you have any questions, concerns or complaints about our collection, use or disclosure of personal information, or if you believe that we have not complied with this Privacy Policy or the Privacy Act, you can contact the Privacy Officer using the details in Section 14.

Please provide as much detail as possible in relation to your question, concern or complaint. We take any privacy complaint seriously and it will be assessed by a Privacy Officer with the aim of resolving any issue in a timely and efficient manner. We request that you cooperate with us during this process and provide us with any relevant information that we may need. If your complaint concerns credit related information, then we may need to consult with other organisations, including credit reporting bodies or credit providers.

If you are not satisfied with the outcome of our assessment of your complaint, you may wish to contact the Office of the Australian Information Commissioner (click here for information) or the Australian Financial Complaints

Authority (click here for information).

14. Contact us

The Privacy Officer
Heartland Bank Australia Limited
PO Box 18134
Collins Street East VIC 8003
By Phone – 1300 889 338

Appendix 2 – Privacy Policy (Web Version – StockCo)

1. What is our privacy policy?

At StockCo, we realise the importance of protecting your personal information whether it comes from you or through other sources. This Privacy Policy describes how we collect, store, and handle personal information, the types of personal information we collect, the purposes for which we use this information, to whom this information is disclosed and how you can communicate with us about your personal information.

In this policy, "we","us","StockCo" or "StockCo Group" refers to Heartland Bank Australia Limited ABN 54 087 651 750, and its related bodies corporate (as that term is defined in the Corporations Act 2001 (Cth)). We may change our Privacy Policy from time to time at our discretion. At any time, the latest version of our Privacy Policy is available from our website at https://stockco.com.au/resources/policies/.

2. What types of personal information do we collect?

Personal information is information about you that identifies you or from which your identity is apparent or can reasonably be worked out. It can include an opinion and does not necessarily need to include your name.

One kind of information that we regularly collect is credit information. Credit information is that part of your information that we use to assess your eligibility for the credit products that we make available.

This can include details of any finance that you have available, your history in repaying credit and other information that credit providers use to assess eligibility. Section 6 below contains further information about credit information.

The kinds of personal information we are allowed to obtain about you, and the manner in which we collect, maintain and protect your personal information, are primarily governed by the Privacy Act and the Australian Privacy Principles (APPs) under that Act.

In addition, before we are able to provide you with financial products or services, the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth) ("AML/CTF Act") requires us to collect information about you in order to verify your identity. This information may also be provided to a credit reporting body for verification, or to third parties for the purposes of fraud prevention, Anti-Money Laundering and Counter-Terrorism Financing checks as required by law and identify verification. Section 7 below contains further information about the collection and verification of identification information.

The types of personal information we collect about you depends on the circumstances in which the information is collected. Such information may include:

- contact details (such as your name, address, email address and phone numbers);
- photographs of you;
- date of birth and gender;
- current occupation and employment history;
- education, qualifications and training;
- relationship status;
- details of individuals you are (or may be) connected to;
- financial information, such as information about your assets, finances, income, expenses and debit and credit history (including information obtained from credit reporting bodies);
- your tax file number; and/or
- information concerning your use of our products and services.

We also have access to information about your account(s) and transactions. This means we can see how and where you use your account(s). We may use this information to form a view on our other products and services that may benefit you.

We generally do not collect sensitive information about you unless required by applicable laws or rules. Sensitive information includes information in relation to:

- political or religious beliefs;
- race or ethnic origin;
- memberships of unions, trade or professional associations;
- criminal records; and/or
- health information.

If you do provide sensitive information to us for any reason, you consent to us collecting that information and to us using and disclosing that information for the purpose for which you disclosed it to us and as permitted by the Privacy Act and other relevant laws.

In addition to the types of personal information identified above, we may collect personal information as otherwise permitted or required by law.

We will only obtain, use or disclose government generated identifiers (for example, your tax file number) in circumstances where we are legally permitted or obliged to

do so.

The scope of your personal information may include many records and documents. Should you require it, we would be happy to explain in greater detail what this information includes. Should you require it, you may also see the personal information we keep about you, subject to certain limitations set out in the Australian Privacy Principles. Please contact us if you require us to give you a further explanation.

3. How do we collect your personal information?

We collect personal information in a number of ways. The most common ways we collect your personal information are:

- directly from you, including when you request or use any of our products or services;
- from publicly available sources;
- from market research bodies who may have records about you from surveys and questionnaires you may have engaged in;
- from your personal representatives, including your solicitor, accountant and financial adviser;
- from distributors, agents and brokers, including insurance brokers or mortgage brokers you may have had contact with;
- from other credit providers you may have had contact with and credit reporting bodies;
- from Federal, State or Territory government departments and regulatory bodies; and/or
- from other third parties.

We may also collect information about how you use our website and mobile apps. For example, this may include your identity, date and time of your visits, number of visits, the type of products and services you view and how you use our website and mobile apps. We obtain information via our website through 'cookies' and related technologies. The use of cookies helps us monitor the effectiveness of our website and mobile apps.

A 'cookie' is a packet of information placed on a user's computer by a website which is used for record keeping. Cookies are used to monitor traffic on our website, but generally we do not collect personal information from you using cookies.

You can configure your browser to accept or reject cookies, or notify you when cookies are sent. If you disable the use of cookies on your web browser or reject cookies from us then you may not be able to gain access to all of the content or facilities that we offer.

Throughout our website and mobile apps we use the Google Universal Analytics system, Google Play Console and App Store Connect (as applicable) to measure anonymous website and mobile app activity. These services provide us with information about the use, functionality and effectiveness of our website and mobile apps, helping us to understand and optimise user experiences and to also optimise our advertising on, and outside of, our website and mobile apps. We may also use other third party data analytic software in the future and you may request a list of all data analytic software providers that we use from us at any time.

The information we collect from your general use of our websites and mobile apps does not identify you. It is general data regarding the number of visitors/users of our website and mobile apps, and statistics regarding their usage.

However, where you access functions of our website and mobile apps that require you to verify your identity by entering your log-on details and/or a password we will keep a record of that access to monitor and record transactional information within the secure parts of our website and mobile apps. We may store this information for a period of up to 7 years unless we reasonably need to store it for a longer period for example to resolve a complaint that you have made.

We may also monitor and/or record telephone discussions between you and our staff for training purposes and to check the accuracy of our records.

4. For what purposes do we collect, use and disclose your personal information?

The purposes for which we use and disclose your personal information will depend on the circumstances in which we collect it. Generally, we collect, use and disclose your personal information so that we can:

- establish who you are and assess your creditworthiness;
- assess applications for products and services;
- administer and monitor products or services;
- develop and run our business generally;
- comply with legal obligations and assist government departments and regulatory bodies; and/or
- tell you about other products or services that we think may be of interest to you.

We may also collect, use and disclose your information in other ways where permitted by law.

If you do not agree to give us certain types of personal information, we may be unable to provide you with the products or services you have asked for.

5. To whom may we give your personal information?

We may disclose your personal information to third parties in connection with the purposes described above. This generally includes disclosure to the following types of third parties:

- our related bodies corporate;

- other persons named in your application for a product or service with us;
- our service providers and contractors, including data storage providers in Australia or overseas;
- other financial and insurance institutions;
- identity verification agencies;
- debt collecting agencies;
- credit reporting bodies;
- government departments & regulatory bodies and issuers or official record holders of identity documents;
- your agents, advisers, referees, executors, administrators, trustees, guardians, beneficiaries (if you are a trustee) or attorneys;
- anyone to whom we consider assigning or transferring any of our rights or obligations; and/or
- other persons where this is permitted by law or to whom you have directed or otherwise permitted us to disclose your personal information to.

Where we disclose your personal information to third parties we will use reasonable endeavours to ensure that such third parties only use your personal information as reasonably required for the purpose we disclosed it to them and in a manner consistent with the Privacy Act. Third parties who access your personal information are required to adhere to appropriate security standards to protect your information from unauthorised access, destruction or loss.

6. Credit reports

When you apply to us for credit, we may request a credit report about you from a credit reporting body. A credit report contains information about your credit history which assists credit providers to assess your application, verify your identity and manage your accounts. Credit reporting bodies collect and exchange this information with credit providers.

The Privacy Act limits the information that credit providers can disclose about you to credit reporting bodies, as well as the ways in which credit providers can use credit reports. The information we may disclose includes your identification details, any applications for credit you have made, the type and amount of credit you have, any failure to make repayments or defaults and whether you have committed a serious credit infringement (such as fraud). This is information we have collected through your use of our products and services. We may also ask credit reporting bodies to provide us with an overall assessment score of your creditworthiness.

The credit reporting bodies we may share information are:

- Equifax (equifax.com.au);
- Illion (creditcheck.illion.com.au/); and/or
- Experian (experian.com.au).

Contact details and copies of their privacy policies are available on their websites.

We use information from credit reporting bodies to confirm your identity, assess applications for credit, manage our relationship with you and otherwise in order to comply with laws, regulations and codes of practice. This includes sharing your credit information with the entities listed in Section 5. We may combine the information from a credit reporting body with other information. Credit providers can ask credit reporting bodies to use your credit-related information to pre-screen you for direct marketing. You can ask a credit reporting body not to do this. You can also ask a credit reporting body to not use or disclose your credit information if you believe you have been, or are likely to be, a victim of fraud. To do this, contact the credit reporting body directly.

Sections 12 and 13 contain details about how you can access or correct any information we hold about you, how you can make a complaint about a data breach and how we will deal with any complaint.

7. Identity verification

Before we can provide you with financial products or services, we are required to collect information from you to verify your identity. This requirement applies to Australian financial institutions such as Heartland under the AML/CTF Act.

There are two methods we can use to verify your identity: electronic verification or a manual alternate method. Heartland may choose to use either electronic verification or a manual alternate method (or both) depending on the product you are applying for and the identification you have provided to us.

Electronic Verification

Under the AML/CTF Act, we can disclose your name, residential address and date of birth to a credit reporting body to assist in verifying your identity. The credit reporting body will then assess whether this information matches (in whole or part) information held in their records and in the records of government departments, an issuer or official record holder of identity documents, or other third parties (if any).

For us to complete electronic verification, you need to:

- be 18 years or over;
- have an Australian residential address;
- hold an acceptable form of identification; and
- consent to your identity being verified in this way.

Manual Alternate Method

If you cannot or choose not to be electronically verified, we must identify you using a manual alternate method for example by requesting originally certified copies of identifying documents such as your driver's licence, passport or other documents that verify your identity if you do not have a driver's licence or passport, or your name has been changed.

8. Does personal information leave Australia?

We may share your information with recipients located overseas, including some of our related bodies corporate or service providers. The countries in which these recipients are located include New Zealand. We take reasonable steps to ensure that these recipients protect your information in the same way that we do (although they may not be subject to Australian laws).

Your information may also be held on our behalf by data storage providers, including cloud-based data storage providers in Australia, New Zealand or elsewhere.

9. How do we protect your personal information?

We keep hard copy documents in our offices which are protected by building security and other office security measures. The electronic records that we keep are in computer systems that have firewalls, intrusion detection and virus scanning tools to protect against unauthorised access. We also maintain and monitor our online security systems.

Our staff are trained in the proper handling of personal information so that they are aware of the things they must do to protect your personal information. We also seek to ensure that appropriate data handling and security arrangements are in place when we send information overseas or use third parties that handle or store data.

However, the internet is not a secure environment and although care is taken, we cannot guarantee the security of information provided to us or stored or transferred via electronic means. You can help us protect your privacy by observing our security requirements and contacting us immediately if your contact details change. You should keep any usernames, passwords and pin codes secure and confidential at all times, and not disclose them to any other person. Please contact us immediately using the details in Section 14 below if you believe that your username or password may have been disclosed to another person.

10. Direct marketing

We may use your information to inform you of other products and services that could be of interest to you, including through direct marketing. We may contact you from time to time to tell you about these products and services. If you don't want to receive direct marketing, you can ask us not to contact you and not to disclose your information to others for that purpose. If you would like to opt out of receiving our marketing, please contact us using the information provided below in Section 14.

We may use your personal information, such as your email address or mobile number etc, to deliver marketing messages to you through digital advertising platforms. This may include sharing hashed versions of your information with third-party platforms for the purposes of audience targeting, remarketing, and measuring the effectiveness of our advertising campaigns.

We use advertising technologies including cookies and pixels to help us show relevant advertisements to individuals who have interacted with our services or may be interested in our services. These technologies may collect information about your browsing activity on our website and mobile apps.

Cookies and similar technologies may be placed on your device to:

- Deliver advertisements that are more relevant to you;
- Build audiences for targeted advertising;
- Measure the performance of our marketing efforts.

You can manage your cookie preferences through your browser settings, and you may opt out of personalised advertising by managing your settings within the platforms.

We will not use or disclose sensitive information about you for direct marketing purposes unless you have consented to such use or disclosure.

11. Unsolicited information

Sometimes we receive personal information that we have not asked for, which can include sensitive information. If we receive such information, we will examine whether we are permitted to collect such information and, if we are, we will review the information and handle it in accordance with this Privacy Policy. If we are not able to collect such information and it is not in a government record, then we will destroy or de-identify the information as soon as possible, if it is lawful to do that.

There are occasions where it is difficult to separate sensitive information from other personal information and we may need to store information for future use including for regulatory reasons. Where this is the case, we will still keep the information in accordance with this Privacy Policy.

12. How can you access and correct your personal information?

If you wish to access the personal information we hold about you, you can contact us using the details in Section 14. We may require that the person requesting access provides suitable identification.

We will provide access to that information in accordance with the Privacy Act, subject to certain exemptions which may apply. Access may not be provided where the information would disclose personal information about someone else, would disclose commercially sensitive matters (including our business operations and decision

making processes) or is protected from disclosure by law. If you have requested to see your information and we are not able to disclose it to you, then we will tell you and give you reasons.

We will usually provide your personal information free of charge. However, in some cases we may need to charge you an administration fee (such as when your request requires us to obtain information that is not readily available).

If you think that any personal information we hold is incorrect or out of date, then you can ask us to correct or update it. If your request relates to credit related information provided by others, we may need to consult with credit reporting bodies or other credit providers before being able to correct or update the information. If we disagree that the information should be corrected, then we will tell you and give you reasons.

13. What can you do if you have a privacy issue?

If you have any questions, concerns or complaints about our collection, use or disclosure of personal information, or if you believe that we have not complied with this Privacy Policy or the Privacy Act, you can contact the Privacy Officer using the details in Section 14.

Please provide as much detail as possible in relation to your question, concern or complaint. We take any privacy complaint seriously and it will be assessed by a Privacy Officer with the aim of resolving any issue in a timely and efficient manner. We request that you cooperate with us during this process and provide us with any relevant information that we may need. If your complaint concerns credit related information, then we may need to consult with other organisations, including credit reporting bodies or credit providers.

If you are not satisfied with the outcome of our assessment of your complaint, you may wish to contact the Office of the Australian Information Commissioner (**click here** for information) or the Australian Financial Complaints Authority (**click here** for information).

14. Contact us

The Privacy Officer
Heartland Bank Australia Limited
PO Box 18134
Collins Street East VIC 8003
By Phone – 1300 889 338