more than money

nab

NAB eCOMMERCE MERCHANT SOLUTIONS

Getting Started Guide and Application Form

Welcome to NAB eCommerce

The following guide will help you navigate through the establishment of your NAB eCommerce Merchant Account. Read it carefully to get a thorough understanding of the application process and the benefits and responsibilities that come with your eCommerce merchant account.

We wish you well as you establish your eCommerce business and look forward to helping you grow into the future.

What you need to know about the application process

Your application for a merchant account needs to contain as much relevant information as possible. This will help us to quickly assess your application, allowing your account to be up and running sooner.

To help make the application process easier for you, we've highlighted the most critical aspects of the application process. Be as specific as possible as this will make it easier for us to assess your application.

What will we be checking?
Your detailed completion of the application form helps us to understand your business, and what you might require from us. It also helps us to check things such as:

- Legal entity, owners and directors
- Trading names
- Settlement accounts
- Location, contact and industry
- Anticipated transaction types, volume and values
- Your website

If you are replacing a merchant facility at another bank, we will also require recent merchant statements.

How does your business operate?
Before we can approve your NAB eCommerce Merchant Account, we need to accurately assess the potential exposures for both your business and ours. To help us do this, we need to be able to clearly understand the following:

- What does a cardholder buy from you? Identify the type of goods or services you sell.
- How do you engage with your customers? Is your business purely online or do you have a physical presence as well? Do you sell goods or services as a one-off transaction or by subscription?
- When does the cardholder receive the goods or services in full after payment? For example, 5 business days for delivery; or initial membership day one that is then valid for 12 months.

Remember, the more information you can provide, the easier it is for us to quickly process your application.

What happens next?
Once your application has been through the initial assessment you will receive either:

1. Confirmation of approval (eg. Merchant number or NAB Transact and/or NAB Gateway details emailed to you); or
2. Communication regarding necessary website changes; and/or
3. Advice that we must undertake a more detailed credit assessment together with your relationship banking team.

Understanding your NAB eCommerce Merchant Account

You can use your eCommerce merchant account for accepting 'card-not-present' payments including:

- eCommerce: These transactions are used for taking one off customer payments that are initiated in real time. This is generally through a web site, but can also be integrated with other business applications.
- MOTO (Mail Order/Telephone Order): For mail orders, written authorisation is provided by the cardholder to charge their credit card. For telephone orders, you or your employees accept a verbal authorisation from the cardholder. Payment details are then submitted for processing.
- Recurring transactions: Involve charging a customer's credit card on a regular basis (eg. subscriptions, or automatic bill payments). To do this, you must establish a recurring authority with the cardholder.
- Mobile payments: Available through a version of NAB Transact specially formatted for mobile devices. Other payment gateways may also be able to provide this feature.

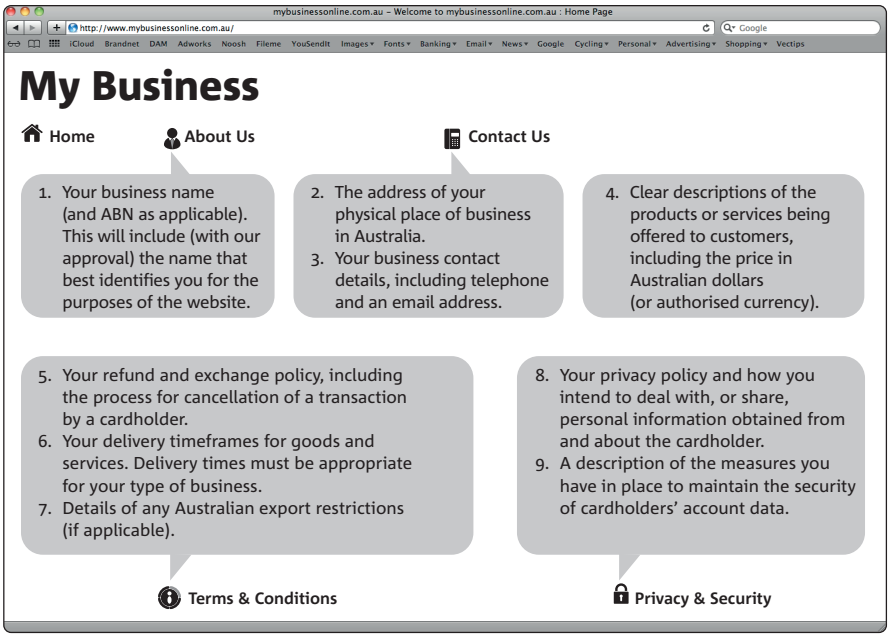
To process transactions with your NAB eCommerce Merchant Account you will need a payment gateway. NAB supports multiple solutions:

1. NAB Transact and NAB Gateway: NAB's own payment gateways that provide a range of hosted and fully integrated payment processing options.
2. Other payment gateway: You can use your NAB eCommerce Merchant ID with one of our accredited third party payment gateways. By providing the merchant account details to your chosen payment gateway, you can use their payment integration and processing integration services. This is referred to as 'Bureau Services' in your Merchant Agreement.

- When using a third party gateway you will enter into a direct relationship with them for the processing and reporting of your transactions.
- You will be responsible for the fees and charges of your third party gateway in addition to NAB fees that relate to your NAB eCommerce Merchant Account.

Requirements for your website

The most important aspect of our eCommerce relationship is your website – it is, after all, your business shopfront. In addition to any Australian legal requirements, your website must include all of the information shown below. The format below is for illustrative purposes – you should work with your web designer on a layout that suits your business.



Your privacy policy

It's essential that your customers know through your privacy policy what you're doing with the personal information collected during their transaction. This statement could cover the following:

- What customer data is collected and tracked (including if you use cookies).
- For what purposes the information will be used (be specific and advise if it will be used for marketing purposes).
- Who the information is shared with (name the types of third parties).
- The processes of you use to keep data secure (eg. policies, restricted access for employees, etc).
- The process for customers to access or correct their information (provide a contact email address or telephone number).

For tools and examples, you may wish to try a web search for 'website policy templates for Australia' or refer to the website of the Federal Privacy Commissioner **www.privacy.gov.au**

Your refund policy

Your refund and exchange policy must be clearly spelled out and comply with the Australian Consumer Law (ACL).

It is important to note that the consumer guarantees provisions of the ACL mean that businesses dealing with defective goods must provide a repair, replacement or refund. Where there is a major failure with an item, the consumer has the right to chose the remedy, including requesting a refund.

Goods and services bought online must meet the same statutory conditions and warranties as for other kinds of sales. Consumers' statutory rights are also the same.

The ACCC has published a recommended refund policy on their website:

Example refund policy

We are not required to provide a refund or replacement if you change your mind.

But you can choose a refund or exchange if an item has a major problem. This is when the item:

- has a problem that would have stopped someone from buying the item if they had known about it;
- is unsafe;
- is significantly different from the sample or description; or
- doesn't do what we said it would, or what you asked for and can't be easily fixed.

Alternatively, you can choose to keep the item and we will compensate you for any drop in value.

If the problem is not major, we will repair the item within a reasonable time. If it is not repaired in a reasonable time you can choose a refund or replacement.

Please keep your proof of purchase – eg. your receipt.

Making eCommerce safer

Fraud is one of the greatest threats to merchants who trade over the internet and through mail or telephone order. As they are at the frontline, it is the responsibility of these merchants to verify—to the greatest extent possible—the cardholder's identity and the validity of the transaction.

Basic fraud control actions are listed below. It should be remembered that none of these tools should be used exclusively to determine the validity of the customer or to accept or reject an order. They should be used as indicators of risk, and in combination with other fraud detectors.

Many of these tests can be conducted automatically. However, this will depend on the flexibility of your technical infrastructure or your ability to connect with fraud prevention service providers. Instead of manually reviewing each order, it is typically more cost effective to perform automated internal screening or to engage a third-party tool to screen for questionable transactions.

Basic steps you can take to combat fraud

1. Obtain the three or four-digit card verification number from the cardholder (often referred to as CVV). The card verification number is a code printed on all Visa, Mastercard and American Express cards.
    - From 1 April 2012, all eCommerce transactions must include the card verification number. An eCommerce transaction is defined as a payment accepted over the internet where the cardholder is entering the card details themselves.
    - To maintain the security of the card, it's important that this number is not stored in your system – therefore it's optional for mail/telephone orders.
    - The purpose of the card verification number is to attempt to verify that the person placing the order has the actual card in his or her possession.
    - Requesting the card verification number can add a measure of security to the transaction.
2. Effectively leverage your own customer history data.
    - If you have had a fraud event associated with a customer, the details of that transaction should be added to internal 'negative lists'. Any subsequent order that shares the same characteristics should be considered suspicious.

The warning signs: 10 indicators of potential fraud

Be alert for the following indicators and remember – any of these factors could pose a high risk.

1. First-time shopper: Criminals are always looking for new merchants to steal from.
2. Larger-than-normal orders: Because stolen cards or account numbers have a limited life span, criminals need to maximize the size of their purchase.
3. Orders that include several varieties of the same item: Having multiples of the same item increases a criminal's profits.
4. 'Rush' or 'overnight' shipping: Criminals want their fraudulently obtained items as soon as possible for the quickest possible resale and aren't concerned about extra delivery charges.
5. Multiple transactions on one card over a very short period of time: This could be an attempt to 'run a card' until the account is closed.
6. Inconsistencies: Information in the order details such as a mismatch in the billing and shipping address, telephone area codes that aren't aligned with postal area codes, email addresses that don't look legitimate, and orders placed at unusual times of the day.
7. Shipping to a single address, but transactions placed on multiple cards: This could involve account numbers generated using special software, or even a batch of stolen cards.
8. Multiple transactions on one card or a similar card with a single billing address, but multiple shipping addresses: This could represent organised activity, rather than one individual at work.
9. Multiple cards used from a single IP address: More than one or two cards could indicate a fraud scheme.
10. Orders from internet addresses that make use of free e-mail services: As these e-mail services involve no billing relationships, there is often neither an audit trail nor any means to verify that a legitimate cardholder has opened the account.

Using EMV 3-D Secure services for cardholder authentication

For internet (eCommerce) transactions, we recommend that you use EMV 3-D Secure services to authenticate the cardholder's identity, utilising Visa Secure (previously called Verified by Visa) and Mastercard Identity Check (previously called Mastercard Securecode).

- By utilising EMV 3-D Secure technology, a cardholder is presented with an authentication page provided by the card issuer as part of the purchase process.
- Visa Secure and Mastercard Identity Check offer chargeback protection for enrolled merchants on consumer (but not business and pre-paid) card products.
- Transactions are not processed if the cardholder fails the authentication process.

Shifting the balance
In most instances, the use of EMV 3-D Secure authentication will make the card issuer responsible for the chargeback liability on any fraudulent transactions. However, merchants will still remain liable for chargebacks related to the goods or services provided (eg. not as specified, goods not received, etc). It is important that you read through the terms and conditions around chargeback liability – particularly regarding which cards are covered by EMV 3-D Secure (for instance, commercial and pre-paid cards are generally not covered).

EMV 3-D Secure should not be considered a substitute for your own risk management practices – you should continue to monitor high risk or suspicious sales. We recommend that you cancel and refund any order that seems suspicious.

How it works
The system runs off software known as a Merchant Plug-in (MPI), which must be connected to the web server that handles your payments. Alternatively, you can use the hosted services of your payment gateway or a specialist service provider. The EMV 3-D Secure MPI provides transaction information to the card schemes and enables an authentication page that is hosted by the card issuer. This is presented within your website's payment page as part of your checkout process.

Cardholders use a password for authentication through EMV 3-D Secure. The card issuer can also link the authentication process with their SMS security for internet banking. To complete the transaction, the cardholder must enter their password or code to verify their identity.

If you're using NAB Transact and/or NAB Gateway Direct Post or Hosted Payment Page, you can access our hosted EMV 3-D Secure MPI. If you use another payment gateway service, discuss options for EMV 3-D Secure authentication with them.

When completing your merchant application, let us know whether you wish to be registered with Visa and Mastercard for EMV 3-D Secure authentication.

Data security

Looking after cardholder data
Card data ranks amongst an individual's most important personal information. For this reason, your customers must be certain that their personal card data is secure at all times.

In today's environment, there are a number of ways that cardholder data is transmitted, processed and stored. On the flipside, there are an equal number of ways for fraudsters to gain access to this information.

Payment account data security is mandated globally by the Payment Card Industry Data Security Standards (PCI DSS, or just "PCI"). This is governed by the PCI Security Standards Council.

It's your responsibility as a merchant to keep cardholder data secure. Because a united front is the best way to minimise the chances of cardholder data getting into the wrong hands, we're more than happy to assist you with all matters relating to your PCI compliance.

Making your obligations simple
The easiest way to reduce your responsibilities with PCI is not to transmit, process or store card data through your systems. Most payment gateways will be able to provide you with solutions that transmit card data directly from your customer's computer to the payment gateway. These solutions may be hosted payment pages or integrated solutions that use an iFrame or a transparent redirect such as NAB Transact Direct Post. If you offer recurring billing, your payment gateway you can store card details with the gateway and use a token to replace the card numbers in your system.

If you are using an integrated API (Application Programming Interface) to submit transactions to your payment gateway, your systems are still within scope of the PCI standards. The reason for this is that an API connects with your web server, not the web page directly, so card data is decrypted and re-encrypted by your server as it is transmitted to the payment gateway. You will be required to validate that no residual card data is retained in your system's memory or log files.

How you benefit from good data security
PCI DSS protects cardholders and minimises the risk to your business. Among the many benefits of adhering to the PCI DSS requirements are:

- Protect customer data.
- Provide a complete 'health check' for any business that stores or transmits customer information.
- Lower exposure to financial losses and remediation costs.
- Maintain customer trust and safeguard the reputation of their brand.

For more information, please refer to our PCI DSS brochure which is available on **nab.com.au**

eCommerce Merchant Application Form

Please note: ALL SECTIONS of this form need to be completed. If a box or section does not apply, please place N/A or NOT APPLICABLE in that box rather than leaving it blank. **ANY AREAS THAT ARE LEFT BLANK MAY DELAY YOUR APPLICATION.**

NAB contact name: – Phone number Fax

Please use blue or black pen and write in BLOCK LETTERS

Where did you hear about us?

☐ NAB branch ☐ nab.com.au ☐ Advertising ☐ Other

Business details

Full legal name

Trading name

ABN ACN

Merchant Name that you would prefer to appear on customer's credit card statement (subject to approval) (up to 20 characters)

Business address

Location address

State Postcode

Mailing address

State Postcode

Contact details

Contact name

Telephone ( )

Mobile number

Fax number ( )

Email address

Business website address

Preferred contact time

☐ Morning ☐ Afternoon

Preferred contact method

☐ Phone ☐ Email

Proprietors/Directors

Surname First name

Middle name(s) DOB / /

Surname First name

Middle name(s) DOB / /

Surname First name

Middle name(s) DOB / /

*If your business has more than 3 directors/proprietors, please provide details on a separate sheet.

Business account details

	BSB number	Account number	Account name
Credit funds to	___		
Debit fees from	___		

Both nominated accounts must be BUSINESS ACCOUNTS. Personal accounts cannot be used. (You will need to complete a Direct Debit Request for non-NAB accounts).

☐ I would like to open a new NAB business account

Merchant facility history

Are you a current merchant account holder with NAB? ☐ Yes ☐ No If yes, provide your Merchant Number

Do you have merchant facilities at another financial institution? ☐ Yes ☐ No If Yes, please provide the three most recent merchant statements.

Have you ever had a merchant facility terminated by a financial institution for any reason?

☐ Yes ☐ No If Yes, provide details

Full description of business and sales processes

It is important that your description answers the following questions. What does a cardholder purchase from you? How do you engage with your customers? When and/or how will the cardholder receive their goods or service from you?

Nature of transactions

	Historic	Projected		Source
Average number of credit card sales per month			Face-to-Face	%
Average credit card sale amount	$	$	Mail/Telephone	%
Total annual business turnover (includes cash, cheques, cards, etc)	$	$	Internet	%
			Recurring	%
			Total	**100%**

Provide the percentage split of credit card sales in the following categories:

Supply of goods/services	%	What are the average number of days taken for delivery?	
Memberships/subscriptions	%	How frequently are members/customers billed?	eg. monthly/yearly
		Are all members/customers billed at the same time?	☐ Yes ☐ No
Sale of gift certificates/coupons	%	What is the expiry period?	eg. 12 months
Other	%	Please specify	
Total	**100%**		

What payment gateway or service provider will you be using for processing card payments?

☐ NAB Transact

☐ NAB Gateway

☐ Other payment gateway or service provider _____(insert name)

How will you be submitting your card payments for processing? (refer to Data Security section on page 5)

☐ Virtual terminal or batched payments using tokenisation – you are not storing card details in your own systems.

☐ Hosted payment page or transparent redirect – card details are not transmitted via your systems (eg. NAB Transact/NAB Gateway Direct Post or Hosted Payment Page).

☐ API or batched payments – you store and/or transmit card details via your own systems.

Additional features

☐ Please register me for EMV 3-D Secure authentication.
☐ Visa Secure and Mastercard Identity Check.

NAB Transact

☐ I wish to accept American Express cards, using my existing Amex merchant number _____

☐ I wish to accept American Express cards and would like to establish a new American Express merchant facility.

☐ I wish to accept Diners Club cards using my existing Diners Club merchant number _____. If you do not have an existing Diners Club facility and wish to accept these cards, you must contact Diners Club directly to establish a new merchant facility. You can add your Diners Club merchant number to your NAB Transact service at any time.

NAB Gateway

☐ I wish to accept American Express cards, using my existing Amex merchant number _____

☐ I wish to accept American Express cards and would like to establish a new American Express merchant facility.

☐ I wish to accept Diners Club cards using my existing Diners Club merchant number _____. If you do not have an existing Diners Club facility and wish to accept these cards, you must contact Diners Club directly to establish a new merchant facility. You can add your Diners Club merchant number to your NAB Gateway service at any time.

Website details

What is the address (URL) of the website that you will be using for accepting payments?

URL

Please provide test URL and login details if required.

URL

User ID

Password

Website content

Please confirm that your website includes the following information:

☐ Your business name (and ABN as applicable); and
☐ The address of your place of business in Australia (not a PO Box); and
☐ Your business contact details, including telephone and an email address; and
☐ Clear descriptions of the products and/or services being offered to customers, including price in relevant currency; and
☐ Your refund and exchange policy, including the process for cancellation of a transaction by a cardholder; and
☐ Your delivery timeframe for goods and services; and
☐ Details of any Australian export restrictions (if applicable); and
☐ Your privacy policy and how you intend to deal with, or share, personal information obtained from and about the cardholder; and
☐ A description of the measures you have in place to maintain the security of cardholders' account data.

Security

Please refer to **www.pcisecuritystandards.org/smb** for payment data security guidelines. Larger businesses processing over 20,000 transactions per annum should refer to **www.pcisecuritystandards.org/merchants** for more detailed information.

If requested by NAB, you will need to provide proof of compliance with the global Payment Card Industry Data Security Standards (PCI DSS) by completing a Self Assessment Questionnaire (SAQ) which can be downloaded from the PCI DSS websites shown above. If you use an external hosting or processing service provider they must also be compliant and you should ask to view their certification so that you can complete your SAQ.

Application confirmation

Before signing and/or submitting this form by email, please complete all sections of this application and read all of the important information on this form, including the Privacy and Collection of Information statement and the Authority and Declaration. By submitting this form to NAB, the Applicant acknowledges and declares that:

- The information submitted is true and correct;
- The Applicant has read the section headed "Privacy and Collection of Information" and makes the Declaration set out on the following page.

Signature

If submitting for a company, print full name and capacity for signing (eg. Director)

Date

/ /

Privacy Notification

This notification covers National Australia Bank Ltd ABN 12 004 044 937 and its related companies (the 'Group'). It includes all the banking, financing, funds management, financial planning, superannuation, insurance, broking and ecommerce organisations in the Group. We are grateful for the trust and confidence you have in us to safeguard your privacy. The notification tells you how we collect your information, what we use it for and who we share it with. It also points out some key features of our Privacy Policy available at www.nab.com.au/privacy. By providing personal information to us, you consent to the collection, use and disclosure of your information in accordance with this Notification and any other arrangements that apply between us.

How we collect information from you

We'll collect your personal information from you directly whenever we can, for example when you fill out a form with us, when you've given us a call, used our websites (including via cookies) or mobile applications or dropped into one of our branches. (See our Cookies Policy www.nab.com.au/cookies for more information). Sometimes we collect your personal information from third parties. You may not be aware that we have done so. If we collect information that can be used to identify you, we will take reasonable steps to notify you of that collection.

How we collect your information from other sources

Sometimes we collect information about you from other sources. We may collect information about you that is publicly available (for example from public registers or social media), or made available by third parties. We do this where:

- we distribute or arrange products on behalf of others, including our business partners;
- we can't get hold of you and need to update your contact details;
- we need information from third parties about an application you make through us;
- we need information for fraud prevention purposes;
- we are checking the security you are offering;
- we can learn insight about your financial needs, such as through property information;
- you have consented to third parties sharing it with us, such as organisations we have loyalty programs with or we sponsor;
- at your request, we exchange information with your legal or financial advisers or other representatives.

We may use or disclose information about you in order to combine the information that we hold with information collected from or held by external sources.

When the law authorises or requires us to collect information

We may collect information about you because we are required or authorised by law to collect it. There are laws that affect financial institutions, including company and tax law, which require us to collect personal information. For example, we require personal information to verify your identity under Commonwealth Anti-Money Laundering law.

NAB believes that by applying for this account, you're not a US citizen or tax resident. If you are a US citizen or tax resident, you'll need to advise NAB by calling 1300 550 316 between 9am and 5pm (AEST/ADST) Monday to Friday.

How we use your information

We use your information to provide you with the product or service you asked for, and for other purposes including:

- giving you information about a product or service including financial help, guidance and advice;
- considering whether you are eligible for a product or service, including identifying or verifying you or your authority to act on behalf of a customer;
- processing your application and providing you with a product or service;
- administering the product or service we provide you, which includes answering your requests and complaints, varying products and services, conducting market research, and managing our relevant product portfolios;
- telling you about other products or services that may be of interest to you, or running competitions and other promotions (this can be via email, telephone, SMS, iM, mail, or any other electronic means including via social networking forums), unless you tell us not to;
- identifying opportunities to improve our service to you and improving our service to you;
- determining whether a beneficiary will be paid a benefit;
- assisting in arrangements with other organisations (such as loyalty program partners) in relation to a product or service we make available to you;
- allowing us to run our business and perform administrative and operational tasks (such as training staff, risk management; developing and marketing products and services, undertaking planning, research and statistical analysis; and systems development and testing)
- preventing or investigating any fraud or crime, or any suspected fraud or crime;
- as required by law, regulation or codes binding us; and
- for any purpose for which you have given your consent.

You can let us know at any time if you no longer wish to receive direct marketing offers from the Group. We will process your request as soon as practicable. Where you have subscribed to something specific (like to hear from one of our sponsored organisations) then these subscriptions will be managed separately. If you no longer wish to receive these emails click the unsubscribe link included in the footer of our emails.

How we use your credit information

In addition to the ways for using personal information mentioned above, we may also use your credit information to:

- enable a mortgage insurer or title insurer to assess the risk of providing insurance to us or to address our contractual arrangements with the insurer;
- assess whether to accept a guarantor or the risk of a guarantor being unable to meet their obligations;
- consider hardship requests; and
- assess whether to securitise loans and to arrange the securitising of loans.

What happens if you don't provide your information to us?

If you don't provide your information to us, we may not be able to:

- provide you with the product or service you want;
- manage or administer your product or service;
- personalise your experience with us;
- verify your identity or protect against fraud; or
- let you know about other products or services from our Group that might better meet your financial, ecommerce and lifestyle needs.

Sharing your information

We may share your information with other organisations for any purposes for which we use your information.

Sharing with the Group

We may share your personal information with other Group members. This could depend on the product or service you have applied for and the Group member you are dealing with. Where appropriate we integrate the information we hold across the Group to provide us with a complete understanding of you and your needs, including giving you access to the Group or related products you hold via Internet Banking.

Sharing with MLC Limited

NAB acts for MLC Limited ABN 90 000 000 402 (described as MLC Life Insurance) in distributing their life insurance products. MLC Limited is no longer part of the NAB Group of companies. We may exchange personal information with MLC Limited or their service providers in order to administer and manage your life insurance products that are issued by them. We may also need to share information so as to ensure:

- your insurance premium is calculated correctly (balance information may be required to be shared so your insurance can be calculated) and where authorised, make payments on your behalf to MLC Limited;
- insurance claims and benefits are paid;
- NAB and MLC Limited can both tell you about our respective marketing and products offers (including ensuring customers who hold MLC Limited products are excluded from NAB Group campaigns marketing MLC Limited products);
- a smooth customer experience when you contact us, including:
- we can transfer you to the right service centre;
- where appropriate, NAB and MLC Limited can cooperate in order to handle your complaint;
- being able to provide assistance should you wish to speak about your MLC Limited products held (for example, where possible, we may assist by updating contact details on request).

Some of the information exchanged will be stored and visible within NAB Group customer databases; with some of these databases being accessible to MLC Limited for a transition period. All information stored in these databases is subject to this privacy policy as well as NAB Group's security procedures and controls.

Sharing at your request

We may need to share your personal information with your representative or any person acting on your behalf (for example, financial advisers, lawyers, settlement agents, accountants, executors, administrators, trustees, guardians, brokers or auditors) and your referee such as your employer (to confirm details about you).

Sharing with Credit Reporting bodies

When we're checking your credit worthiness and at other times, we might share information about you with credit reporting bodies. When we give your information to a credit reporting body, it may be included in reports that the credit reporting body gives other organisations (such as other lenders) to help them assess your credit worthiness.

Some of the information that we give to credit reporting bodies may reflect adversely on your credit worthiness, for example, if you fail to make payments or if you commit a serious credit infringement (like obtaining credit by fraud). That sort of information may affect your ability to get credit from other lenders.

With your consent, personal information may also be shared with credit reporting bodies or other approved third parties who are authorised to assess the validity of identification information. These checks help us verify whether your identity is real and are not a credit check.

Sharing with third parties

We may disclose your personal information to third parties outside of the Group, including:

- those involved in providing, managing or administering your product or service;
- authorised representatives of the NAB Group who sell products or services on our behalf;
- credit reporting bodies or other approved third parties who are authorised to assess the validity of identification information;
- insurance, investment, superannuation and managed funds organisations, and their advisers and service provider;
- medical professionals, medical facilities or health authorities who verify any health information you may provide;
- real estate agents, valuers and insurers (including lenders' mortgage insurers and title insurers) , re-insurers, claim assessors and investigators;
- brokers or referrers who refer your application or business to us;
- other financial institutions, such as banks, as well as guarantors and prospective guarantors of your facility;
- organisations involved in debt collecting, including purchasers of debt;
- fraud reporting agencies (including organisations that assist with fraud investigations and organisations established to identify, investigate and/or prevent any fraud, suspected fraud, crime, suspected crime, or misconduct of a serious nature);
- organisations involved in surveying or registering a security property or which otherwise have an interest in such property;
- organisations we sponsor and loyalty program partners, including organisations the NAB Group has an arrangement with to jointly offer products or has an alliance with to share information for marketing purposes;
- companies we arrange or distribute products for, such as insurance products;
- rating agencies to the extent necessary to allow the rating agency to rate particular investments;
- any party involved in securitising your facility, including the Reserve Bank of Australia (sometimes this information is de-identified), re-insurers and underwriters, loan servicers, trust managers, trustees and security trustees;
- service providers that maintain, review and develop our business systems, procedures and technology infrastructure, including testing or upgrading our computer systems;
- payments systems organisations including merchants, payment organisations and organisations that produce cards, cheque books or statements for us;
- our joint venture partners that conduct business with us;
- organisations involved in a corporate re-organisation or transfer of NAB Group assets or business;
- organisations that assist with our product planning, analytics, research and development;
- mailing houses and telemarketing agencies and media organisations who assist us to communicate with you, including media or social networking sites;
- other organisations involved in our normal business practices, including our agents and contractors, as well as our accountants, auditors or lawyers and other external advisers (eg. consultants and any independent customer advocates);
- government or regulatory bodies (including the Australian Securities and Investment Commission and the Australian Tax Office) as required or authorised by law (in some instances these bodies may share it with relevant foreign authorities); and
- where you've given your consent or at your request, including to your representatives, or advisors.

Sharing outside of Australia

We run our business in Australia and overseas. We may need to share some of your information (including credit information) with organisations outside Australia. Sometimes, we may need to ask you before this happens. You can view a list of the countries in which those overseas organisations are located at www.nab.com.au/privacy/overseas-countries-list/

We may store your information in cloud or other types of networked or electronic storage. As electronic or networked storage can be accessed from various countries via an internet connection, it's not always practicable to know in which country your information may be held. If your information is stored in this way, disclosures may occur in countries other than those listed.

Overseas organisations may be required to disclose information we share with them under a foreign law. In those instances, we will not be responsible for that disclosure.

We will not share any of your credit information with a credit reporting body, unless it has a business operation in Australia. We are not likely to share credit eligibility information (that is, credit information we obtain about you from a credit reporting body or that we derive from that information) with organisations unless they have business operations in Australia. However in the event NAB seeks assistance from a related company to manage defaulting loans, we may need, as a consequence, to disclose credit eligibility information to the Bank of New Zealand, located in New Zealand. We are likely to share other credit information about you with organisations outside Australia. A list of countries in which those overseas organisations are located is set out above.

Accessing your information

You can ask us to access information that we hold about you. You have special rights to access credit information we obtain about you from a credit reporting body or that we derive from that information. You can find out how to access your information (including your credit eligibility information) by reading our Privacy Policy, available at www.nab.com.au/privacy or by calling 13 22 65 and asking us for a copy.

Correcting your information

You can ask us to correct information we hold about you. You have special rights to correct your credit information. You can find out how to correct your information (including your credit information) by reading our Privacy Policy, available at www.nab.com.au/privacy or by calling 13 22 65 and asking us for a copy.

Complaints

If you have a complaint about a privacy issue, please tell us about it. You can find out how to make a complaint (including special rights for credit information complaints) and how we will deal with these complaints, by reading our Privacy Policy, available at www.nab.com.au/privacy or by calling 13 22 65 and asking us for a copy.

Contact us

We care about your privacy. Please contact us if you have any questions or comments about our privacy policies and procedures. We welcome your feedback.

You can contact us by:

- submitting an online Compliments, Suggestions or Complaints form via www.nab.com.au
- calling our contact centre on 13 22 65 (Hearing impaired customers can call TTY 13 36 77)
- speaking to us in person at a branch

Contact details for credit reporting bodies

When we're checking your credit worthiness and at other times, we might share information about you with credit reporting bodies. The contact details of those credit reporting bodies are set out below. Each credit reporting body has a credit reporting policy about how they handle your information. You can obtain copies of these policies at their websites.

illion
https://www.illion.com.au
Illion's credit reporting policy is set out at https://www.illion.com.au/legal/illion-credit-reporting-policy-australia/
Phone: 1300 734 806
Email: pac.austral@illion.com.au

Experian Australia
http://www.experian.com.au
Experian's credit reporting policy is set out at www.experian.com.au/privacy-policy
Phone: 1300 783 684
Mail: Consumer Support Experian Australia PO Box 1969 North Sydney NSW 2060

Equifax Australia Information Services and Solutions Pty Limited
http://www.mycreditfile.com.au
Equifax's credit reporting policy is set out at https://www.equifax.com.au/credit-reporting-policy
Mail: Equifax Public Access, PO Box 964, NORTH SYDNEY NSW 2059

Contact credit reporting bodies if you think you have been the victim of a fraud

If you believe that you have been or are likely to be the victim of fraud (including identity fraud), you can request a credit reporting body not to use or disclose the information they hold about you. If you do this, the credit reporting body mustn't use or disclose the information during an initial 21 day period without your consent (unless the use or disclosure is required by law). This is known as a ban period.

If, after the initial 21 day ban period, the credit reporting body believes on reasonable grounds that you continue to be or are likely to be the victim of fraud, the credit reporting body must extend the ban period as they think reasonable in the circumstances. The credit reporting body must give you a written notice of the extension.

Contact credit reporting bodies if you don't want your information used by them for direct marketing/pre-screening purposes

Credit reporting bodies can use the personal information about you that they collect for a pre-screening assessment at the request of a credit provider unless you ask them not to. A pre-screening assessment is an assessment of individuals to see if they satisfy particular eligibility requirements of a credit provider to receive direct marketing. You have the right to contact a credit reporting body to say that you don't want your information used in pre-screening assessments. If you do this, the credit reporting body must not use your information for that purpose.

Authority and Declaration

Authority

[where NAB requires further information] I/We authorise NAB to seek any additional information it may require (including any information required to verify my/our identity) from my/our accountant, solicitor, adviser, bank, other financial institutions or contact person named in this Application, and I/we authorise my/our accountant, solicitor, adviser, bank, other financial institution or contact person to supply such information.

Declaration

[Personal information about an individual]I/We declare that where I/we have provided personal information about an individual (such as an employer, relative, spouse/partner, solicitor or contact person), I/we have made or will immediately make the individual, aware of that fact and:

- That their personal information has been collected by NAB for the purpose of providing me/us with the product or service which is the subject of this Application (including assessing my/our Application) and managing and administering the product or service and protecting against fraud;
- That their personal information may be disclosed to other organisations involved in the provision, management or administration of my/our product or service as required by law or with their consent;
- that I/we may not be able to obtain the product or service the subject of this Application if that individual's personal information is not provided;
- that the individual can gain access to their personal information by contacting NAB; and
- give the individual NAB's contact details.

[Insolvent, bankruptcy]I/We declare that I/we have never been insolvent nor committed any act of bankruptcy or entered into any assignment, composition or arrangement for the benefit of creditors and that there is no unsatisfied judgement in any court against me/us.

[Content of the Application Form] I/We declare that I/we have read the particulars which have been completed in this Application and declare that those particulars and the information in the accompanying documents are true, correct and complete. I/We acknowledge that the representations made in this Application have been made to NAB to induce NAB to grant financial accommodation to the Applicant(s) named in the Application and to enable NAB to determine whether or not to grant such financial accommodation.