ANZ Electronic Banking Conditions

(Cook Islands, Fiji, Kiribati, Samoa, Solomon Islands, Tonga and Vanuatu)

Effective 8 April 2024

Contents

1. What you need to know about these conditions

These conditions set out some specific information about the following services (collectively referred to as the **electronic banking services**):

- ANZ Internet Banking
- ANZ Pacific App

These conditions also have information about your responsibilities, access to electronic banking services and how we tell you about changes.

It is important that you read and understand these conditions before using any of our electronic banking services. By using our electronic banking services, you agree that these conditions apply to you and you'll comply with them.

Other terms and conditions will also apply to your use of our services, such as specific account terms and conditions. Copies of these other terms and conditions are available on our website or at any branch.

If a particular term in those other terms and conditions is not consistent with a term in these conditions, these conditions will apply for any transactions using the electronic banking services.

2. How to contact us

Via our websites.

Or contact us by phoning the telephone numbers listed below:

- Cook Islands: +682 21750 or +682 25750 after hours
- Fiji: 132 411 (local), +679 321 3000 (overseas or after hours)
- Kiribati: +686 21095 or +679 3316644 after hours
- Samoa: +685 74021095 or +685 800199 after hours
- Solomon Islands: +677 21111 or +679 3316644 after hours
- Tonga: +676 20500 or +676 27931 after hours
- Vanuatu: +678 26355 or +678 27213 after hours

3. A glossary of the terms we use

ATM

ATM means automated teller machine.

Bank Mail

Bank Mail is the electronic messaging service that allows us to communicate with you by email within our secure Internet Banking system.

Biometric identification

Biometric identification means verifying identity using a person's unique physical and other traits, such as Voice ID, facial recognition or fingerprint log-on using fingerprint identity sensor.

Business day

Business day is any day except Saturday, Sunday or a public holiday in the country where your account is held.

Cleared funds

Cleared funds are funds in your account, available for you to use, and which won't be reversed or dishonoured, unless the transaction is considered fraudulent.

EFTPOS

EFTPOS means electronic funds transfer at point of sale.

Electronic payment

Electronic payments are payments you make using Internet Banking or the Pacific App, or payments we make for you electronically, including scheduled payments, bill payments, tax payments, payroll payments and funds transfers including international transfers and telegraphic transfers.

Internet Banking

Internet Banking means ANZ Internet Banking, our service that lets you do things like check your account balances and make electronic payments, using a computer or other device connected to the internet.

Mobile device

Mobile device is a mobile phone or other mobile telecommunication device that allows you to communicate with us through text message or internet connection.

Our websites

Our websites are:

- Cook Islands: anz.com/cookislands
- Fiji: anz.com/fiji
- Kiribati: anz.com/kiribati
- Samoa: anz.com/samoa
- Solomon Islands: anz.com/solomonislands
- Tonga: anz.com/tonga
- Vanuatu: anz.com/vanuatu

ANZ Electronic Banking Conditions

(Cook Islands, Fiji, Kiribati, Samoa, Solomon Islands, Tonga and Vanuatu)

Pacific App

Pacific App means ANZ Pacific App, our mobile banking app for iPhone, iPad and Android devices. The Pacific App lets you do things like check your account balances and make electronic payments, using your mobile device through an internet connection.

Password

Password is a series of between 8 and 32 characters containing at least one letter and one number that you choose and then use to access certain electronic banking services.

PIN

PIN is a number of between 4 and 8 digits (depending on the electronic banking service) that you choose and then use to access certain electronic banking services.

Push notification

Push notification is a message that can display on your mobile device without you having to open the Pacific App.

Responsibility or responsible

Responsibility or responsible means each of the following:

- the responsibility or liability someone has for debts they owe, or someone else owes;
- the responsibility or liability for someone else's losses or costs; and
- the responsibility someone has to do something, or not do something.

Scheduled payment

These are regular future-dated payments for a set amount to someone else or to another one of your accounts with us.

Security code

Your security code is the 6 to 14 character long identification code you have advised to us in writing. This is not your ANZ Internet Banking password.

Security questions

Security questions are questions that only you know the answer to.

Site key

Site key is a picture or image and its associated phrase that only you know.

Uncleared funds

Uncleared funds are funds in your account we may allow you to use, but which could be dishonoured, for any reason. For example, if a person who has deposited money into your account doesn't have enough money in their account to make that deposit, and their bank dishonours their payment to you. The money is then debited from your account.

ANZ Electronic Banking Conditions

(Cook Islands, Fiji, Kiribati, Samoa, Solomon Islands, Tonga and Vanuatu)

User ID

User ID is the number we give you to identify you when you access your account using an electronic banking service.

Voice ID

Voice ID is our system that lets you verify your identity using the unique biometric characteristics in your voice.

We, us, and our

We, us, and our means:

(a) the branch of Australia and New Zealand Banking Group Limited ABN 11 005 357 operating in the country where your account(s) is held, namely either in Cook Islands, Fiji, Solomon Islands or Tonga;

(b) ANZ Bank (Kiribati) Limited, if your account(s) is held in Kiribati;

(c) ANZ Bank (Samoa) Limited, if your account(s) is held in Samoa; or

(d) ANZ Bank (Vanuatu) Limited, if your account(s) is held in Vanuatu.

You

You means the person we've provided any accounts, products, or services to. If more than one person:

- 'you' means each person individually, and any two or more of those people;
- each person must comply with these conditions; and
- each person must pay any amounts we're owed, by themselves or with the others who are responsible for those amounts.

4. General information about these conditions and the services we provide you

We can change these conditions

We can change these conditions or our fees at any time. We'll let you know what's happening at least 30 days before we make any changes in any one of the following ways:

- Writing to you, sending you an email or a fax, or calling you by telephone.
- Posting messages in the electronic banking services.
- Putting up information in our branches or on our website.
- Advertising the changes, for example in newspapers or on radio or television.

We can charge you fees relating to electronic banking services

See our fees and charges brochure in your branch or visit our websites for the fees and charges that apply to our electronic banking services in the country where your account is held.

You agree we can take our fees and charges from your account. You are responsible for all charges charged by an internet service provider, mobile or telephone operator when you access any electronic banking service.

How to contact us for support

Please visit our website in the country where your account is held for information on how to contact us for support. If you are registered for Internet Banking, you can contact us through Bank Mail.

We will not give you advice on your mobile device, or data connections, or on the network charges to your mobile device and/or its associated accounts.

How you can give us your feedback, and what to do if there is a problem

Tell us immediately if either of the following apply:

- you think there is an error on your bank statement or online account information; or
- you have any questions or complaints.

You will need to give us the following information:

- your name;
- your account number and User ID; and
- any details you can about the suspected mistake, or the nature of your question, including the amount of money involved.

We may ask for more information from you to help us in our enquiries. We will make every effort to answer your questions or resolve your complaints quickly and fairly. Where we find that an error occurred, we will promptly correct the error (to the extent possible) and repay any interest or fees we may have charged you as a result of the error.

We will correct any errors made on your statement or online account information.

Please call us on the relevant telephone number set out in 'How to contact us' on page 1 of these conditions or talk to a staff member at any branch if you don't think your enquiry has been properly dealt with.

When terms in these conditions may be invalid

If a court in the country in which your account(s) is held, decides that any of the terms in these conditions are unlawful, we will remove the term(s) in question and the remaining terms will be enforceable.

We reserve our right to exercise our rights

Even if we don't immediately exercise a right we have under these conditions, we can still exercise that right in future.

Governing law

These conditions are governed by the law in force in the country in which your account(s) is held. You and we agree to submit to the non-exclusive jurisdiction of the courts of that country.

5. How you use your accounts with us

Your access to accounts and availability of electronic banking services

You can access and operate all your selected accounts through the electronic banking services where either:

- you are the only account holder and signatory;
- you have the authority to operate the account alone where there is more than one signatory to the account; or
- you are making a payment on an account that needs more than one authorised user. To complete that payment all required authorised users must approve the payment.

Our electronic banking services are generally available 24 hours a day, 365 days a year, except for downtime to allow for maintenance of the system. As we also rely on third parties to make the electronic banking services available (like software providers, network service providers, and internet service providers), there may be other times when the electronic banking services, including push notifications, are limited or unavailable.

We can suspend or terminate your access to electronic banking services or any functionality within our electronic banking services, at any time without telling you.

You can stop using any electronic banking service at any time by letting us know that you no longer wish to use the service.

How we act on instructions

You accept that our authority to process instructions on your accounts comes from the use of your User ID, password, PIN, security code, security questions, site key, Voice ID, or successful log-on to the Pacific App using fingerprint, face or other biometric identification or another security feature that might apply. Our authority also comes from a transmission of a contactless transaction. You agree that we have that authority whether or not you have actually given authority for the instruction. You agree that we may do any of the following things:

- act on an instruction received through the electronic banking services without checking your identity;
- delay acting on an instruction; and
- ask you for more information before acting on an instruction.

You agree that you will only use our electronic banking services to carry out your banking transactions and enquiries available through the electronic banking service.

You may not be able to cancel or change instructions once issued. Please contact us on the relevant telephone number set out in 'How to contact us' on page 1 of these conditions, or ask at any of our branches if you have any queries about cancelling or changing instructions.

ANZ Electronic Banking Conditions

(Cook Islands, Fiji, Kiribati, Samoa, Solomon Islands, Tonga and Vanuatu)

How to help protect yourself and your information

Your card, password(s), PIN(s), security code, security questions, site key, User ID, Voice ID and any biometric identification stored on your mobile device to log-on to the Pacific App, are the key to accessing your accounts electronically (including by phone or mobile device).

The security of your card, password(s), PIN(s), security code, security questions, site key, mobile device, User ID, Voice ID and any biometric identification is very important. You must memorise your password, PIN(s), security code, security questions and site key.

If you enable fingerprint, face or other biometric identification access to log-on to the Pacific App, anyone whose fingerprint, face or other biometric identification is stored on your mobile device will be able to access the Pacific App.

You must not have fingerprint, face or other biometric identification access enabled in the Pacific App settings if someone else's fingerprint, face or other biometric identification is stored on your mobile device.

You must not record your voice identification phrases used for Voice ID, such as your passphrase. You must not let someone else record their voiceprint against your customer profile. You agree that you will be responsible for actions on your accounts following successful identification using Voice ID, in accordance with these conditions.

For more information and advice on how to protect yourself and your information when using electronic banking services, see our website.

How to help protect your passwords, PIN(s), security code, security questions, site key and biometric identification

You must follow our advice to help protect your passwords, PIN(s), security code, security questions, site key and biometric identification:

- Tell us immediately if you suspect that your password, PIN, security code, security questions or site key has become known to anyone.
- Change your password, PIN, security code, security questions and site key regularly and immediately when we ask you to.
- Change your password, PIN, security code, security questions and site key after any spyware or viruses have been removed from the computer you use.
- Keep your password, PIN, security code, security questions and site key memorised and not written down (even if disguised).
- Keep your password, PIN, security code, security questions and site key for our electronic banking services different from your other password, PIN, security code, security questions and site key and don't use the same PIN, passwords, security questions and site key for more than one electronic banking service.
- Don't tell anyone your password, PIN, security code, security questions or site key. This includes family members or anyone who appears to be in a position of authority, including our staff or the police.
- Don't let anyone see your password, PIN, security code, security questions or site key – for example, when you enter your PIN or password into a computer, mobile phone, EFTPOS or an ATM.
- Keep your password, PIN, security code, security questions hard to guess – don't choose a PIN or password or security code or security questions based on information about you that's easy to find, like your birth date or telephone number and don't choose a PIN, security code, security questions or password that's easy to work out, like 1111 or 3456.
- Never enter your password, PIN, security code or security questions on a third party website or mobile application or a webpage accessed by a link from an email, even if the email appears to be from us.
- Never have fingerprint, face or other biometric identification access enabled in the Pacific App settings if someone else's fingerprint, face or other biometric identification is stored on your mobile device.
- Never record your voice identification phrases used for Voice ID, such as your passphrase.
- Never let someone else record their voiceprint against your customer profile.

ANZ Electronic Banking Conditions

(Cook Islands, Fiji, Kiribati, Samoa, Solomon Islands, Tonga and Vanuatu)

How you can help stop unauthorised use of your accounts

You must immediately change your password, PIN, security code, security questions or site key and call us on the relevant telephone number set out in 'How to contact us' on page 1 of these conditions if:

- Someone might know your password, PIN, security code, security questions or site key.
- You think someone has accessed your information and accounts without your authority.
- Your mobile device or SIM card has been lost or stolen.

Please visit our website for how to contact us if your card has been lost or stolen or you think someone has been using your card.

When we will reimburse you

We will reimburse you for direct losses you incur that are caused by any of the following:

- our employees or agents acting fraudulently or negligently;
- any forged, faulty, expired or cancelled part of an electronic banking service; or
- an unauthorised transaction where it is clear you have not contributed to the loss.

When we will not reimburse you

We will not reimburse you for any losses you incur that are caused by any of the following:

- Any loss or damage to your mobile device resulting from your access or use, or attempted access or use, of Internet Banking or the Pacific App (including downloading any applications).
- Any loss or damage resulting from an inability of your mobile device to access Internet Banking or the Pacific App.
- Any information, content or data you give us.
- Any loss caused by the disclosure of any of your passwords, PINs, security code, security questions or site key as a result of your use of a mobile device.
- Any loss or damage you or any other person may suffer because of action we have taken or not taken on any Bank Mail message from you.
- Any loss you suffer in connection with any failed or declined transactions.
- We will not reimburse you for any loss or damage you or any other person may suffer in connection with situations outside of our control, including:
- Where you can't use our electronic banking services because of a power or communication failure.
- Failure to connect to the internet.
- A malfunction of any equipment (including telecommunications equipment) that supports our electronic banking services.
- Loss caused by any third party products or services.

We will do our best to make sure you have continuous access to the electronic banking services. However, we are not responsible for any loss you suffer because you cannot use the electronic banking services, or due to delays or errors in processing your instructions caused by a third party.

ANZ Electronic Banking Conditions

(Cook Islands, Fiji, Kiribati, Samoa, Solomon Islands, Tonga and Vanuatu)

Your responsibility for unauthorised use of our electronic banking services

The table below explains what losses you'll be responsible for if someone accesses your accounts using our electronic banking services without your authority:

What's happened	Your responsibility before you tell us	Your responsibility after you tell us
You become aware of a breach of security or unauthorised access to your accounts. You tell us as soon as you become aware of the problem and you haven't either: • Acted fraudulently or negligently. • Contributed to the unauthorised transactions.	No responsibility	No responsibility
You breached our conditions. For example: • You selected a PIN, password, security code, security questions or site key we believe is unsuitable. • You didn't reasonably safeguard your PIN, password, security code, security questions or site key. • You kept your PIN, password, security code, security questions or site key written down. • You have given someone else access to your accounts using our electronic banking services. • You have left a computer unattended when logged on to Internet Banking. • You have used a computer or device that doesn't have an up-to-date operating system installed for Internet Banking or the Pacific App; or that doesn't have up-to-date anti-virus software installed for Internet Banking or the Pacific App. • You didn't promptly tell us that someone else has accessed your accounts using our electronic banking services. • You have enabled fingerprint, face or other biometric identification access to the Pacific App on your mobile device, and someone else's fingerprint, face or other biometric identification was stored on your mobile device and used to access the Pacific App. • You have recorded your voice identification phrases, such as your passphrase, or let someone else record their voiceprint against your customer profile.	You're responsible for the lower of: • the actual loss at the time you told us; and • the balance that would have been available to withdraw (including any credit facility) between the time the unauthorised transactions were made and the time you told us.	No responsibility
You've allowed your account to be used fraudulently or to process unauthorised transactions.	You may be responsible for some or all of the losses, regardless of the balance available in your account.	You may be responsible for some or all of the losses, regardless of the balance available in your account.
You've acted fraudulently or negligently.	You're responsible for all losses, regardless of the balance available in your account.	You're responsible for all losses, regardless of the balance available in your account.

Your responsibility for any misuse or failure to stop unauthorised use of electronic banking services

You promise to reimburse us for any amount we pay to our customers or third parties as damages for loss they suffer from your misuse of the electronic banking services, or your failure to stop unauthorised use of the electronic banking services.

6. How to find information about making electronic payments

You can set electronic payments to go on the same date, a future date or recurring (scheduled payments).

See also the fees and charges booklet in your branch or on our website for information on the fees we charge for making electronic payments.

Check before confirming an electronic payment

You must check all payment details before confirming your electronic payments. Our systems are generally automated, so we don't check details for you. If you pay the wrong person or amount, you may have trouble getting the money back. See 'What happens if you have a problem with your electronic payment' below.

As soon as we start the process of making an electronic payment, we're unable to stop it, regardless of whether the person you're paying banks with us or another bank. If you make a mistake when you make a payment, for example, you pay the wrong account or amount, we can't stop the payment being sent.

What happens when you confirm an electronic payment

By confirming an electronic payment, you agree to let us take an amount from your account and pay it to someone else for you on the payment date selected or allowed. You also agree to let us take any fees for making that payment from your account — see our fees and charges booklet in your branch or on our website.

If you're paying someone at another bank, they won't get the payment until their bank deposits it to their bank account.

Here's an example. At 10am on Saturday, you confirm an electronic payment in Internet Banking for $20 to go to an account at another bank. We withdraw the $20 from your account immediately, but send it to the other bank early Monday morning.

ANZ Electronic Banking Conditions

(Cook Islands, Fiji, Kiribati, Samoa, Solomon Islands, Tonga and Vanuatu)

How and when we'll make your electronic payment

Electronic payment type	Who you're paying	How and when we'll make your electronic payment
Same-day electronic payment	Paying another account with us	We take the money from your account after you have confirmed the payment and send it immediately to the other account.
	Paying an account at another bank	We take the money from your account immediately after you have confirmed the payment and send it to the other bank throughout the day on business days between 9am and 2pm. If you set up the payment after 12am or on a non-business day, we'll send the payment in the morning of the next business day.
Future-dated electronic payment including scheduled payments	Paying another account with us	We take the money from your account, if there's enough money in there, from 5am on the payment date. We send the payment immediately to the other account. If you don't have enough money in your account, the payment will skip to the next payment date. See 'Don't have enough money for an electronic payment?'.
	Paying an account at another bank	We take the money from your account, if there's enough money in there, from 5am on the payment date. We send the payment immediately to the other account. If the payment date isn't a business day, we'll take the money from your account from 5am the next business day instead. If you don't have enough money in your account, the payment will skip to the next payment date. See 'Don't have enough money for an electronic payment?'.

For scheduled payments, you can only make your first payment after the day you set it up. All scheduled payments will be made as early as 5am on the scheduled payment date.

Don't have enough money for an electronic payment?

Always make sure you have enough money in your account to cover electronic payments. Here's what happens if you don't have enough money in your account for an electronic payment.

Electronic payment type	What happens if you don't have enough money
Same-day electronic payment	You won't be able to confirm the payment. There's no fee if this happens.
Future-dated electronic payment including scheduled payments	The payment will not happen and will skip to the next payment date.

You'll see failed payments in your transaction history.

Stopping electronic payments

Electronic payment type	Stopping that electronic payment
Same-day electronic payments	You can't stop, cancel, or change same-day electronic payments, even if set up and confirmed on a non-business day, because we start the process to send the payment immediately.
Future-dated electronic payments including scheduled payments	You can: • delete future-dated payments until 5am on the payment date or • skip any scheduled payments until 5am on the scheduled payment date.

What happens if you have a problem with your electronic payment?

If you make a mistake, contact us immediately. We may be able to help by contacting the other customer (if they bank with us) or the other bank and asking them to return the money. We can't guarantee you'll be able to recover the payment.

We don't have to get involved in disputes between you and anyone receiving your electronic payment.

If we make a mistake processing your electronic payment, we'll try to put it right and we'll refund any fees you've paid for the electronic payment. However, we're not responsible for any losses or costs you or anyone else incur if we:

- make an electronic payment using information you've given us that's wrong, or
- take any of the actions for any of the reasons set out under 'We can delay or cancel your electronic payments'.

We can delay or cancel your electronic payments

We can delay, refuse, or cancel your electronic payment, or reduce the amount paid, without telling you first. We can only do this if:

- you don't have enough money in your account for that or any other payment, or the money isn't cleared funds;
- we have a transaction limit for your account, and the electronic payment is over that limit;
- we can't process the electronic payment because of a technical failure in our system or systems used by the banking industry or you've given incorrect or incomplete information;
- we believe the electronic payment involves fraud, money laundering, or other criminal conduct by you, an authorised signatory, or someone else;
- we believe the electronic payment involves inappropriate messages that are abusive, threatening and sent for the purposes of causing harm to someone else. For example, using reference fields for messaging purposes other than for financial purposes;
- we believe the electronic payment is to someone we restrict payments to or from — we call those parties 'sanctioned parties'; or
- we've received a court order stopping us processing the electronic payment or we must stop the electronic payment under the laws of the country in which you're located or overseas law.

If we refuse or cancel an electronic payment or reduce the amount paid, you'll have to arrange to pay that money another way.

When we can make changes to your scheduled payment

From time to time, we may need to make changes to your scheduled payment.

We may use our discretion to cancel, reduce the amount, change the reference information, or change the recipient account without telling you.

7. How you use Internet Banking

Your eligibility to register for Internet Banking

To register for Internet Banking, you must be at least 18 years old (unless we agree otherwise) and hold an eligible account with us in Cook Islands, Fiji, Kiribati, Samoa, Solomon Islands, Tonga or Vanuatu at the time you register.

How to register and access your accounts

To access your accounts using Internet Banking, you need to complete an Internet Banking registration form and submit it to a branch. Internet Banking registration forms are available on our websites and at our branches. Once registered you can access your accounts and your bank statements, using Internet Banking.

If you are a personal customer, you need to choose the primary account you want to access using Internet Banking and link all or some of your other accounts to Internet Banking with different access levels (value or non-value), all of which will be subject to a daily Internet Banking limit as set out in the Internet Banking registration form.

If you are not a personal customer, you need to choose the accounts that you would like to access using Internet Banking. You also need to register your authorised users and set their function levels and access levels and authorisation limits to determine how you and those authorised users complete transactions on those accounts. Where making a payment on an account requires more than one authorised user, all required authorised users must approve the payment in order to complete the payment.

We may restrict the accounts you can select for use with Internet Banking. We may also restrict your use of Internet Banking on your account.

We will set daily transaction limits on electronic payments from your accounts using Internet Banking. These limits are specified in the Internet Banking registration forms. Contact us if you would like to change any of these limits. We may make changes to these limits at any time. We will let you know if we do so.

How you can help stop unauthorised access to your accounts through Internet Banking

You must follow our advice about processes and safeguards when using Internet Banking, to help prevent unauthorised access to your account(s).

Don't let unauthorised people or systems access your information

- Don't let anyone see you enter your User ID, password, security code, security questions or site key.
- Don't change your security details in a public place.
- Ensure your browser is set so that it does not save your User ID, password, security code, security questions, details or autocomplete your login.
- Take all reasonable steps to prevent unauthorised use of your computer and always log off your Internet Banking session when you have finished or before you leave your computer unattended.
- Don't let anyone else access your accounts through our electronic banking services.
- Keep information we send you private.
- Let us know immediately if you change your mobile number.

See 'How to help protect your passwords, PIN(s), security code, security questions, site key and biometric identification' on page 7 for steps you must take.

Make sure you can trust the computer you use and the links you follow

- Don't click on links in emails; instead, enter our websites directly into your browser address bar.
- Ensure there is a security symbol in your browser.
- Don't enter your login details onto a third party website or mobile application.
- Don't use public computers, like those in internet cafes, for Internet Banking, as these computers may not be safe or unsecured public Wi-Fi hotspots that don't require a password for your Internet Banking.
- Ensure your computer has anti-virus software installed and regularly updated and that the operating system on your computer is regularly updated.

Granting third parties access to Internet Banking

Sometimes, other companies or organisations request access to your Internet Banking. This could be to provide you services like paying a fine or an airfare. Or, it could be an easy way for them to get access to your account information for credit approval.

You must not give anyone else access to your Internet Banking. This includes not logging in to Internet Banking from other websites or mobile applications.

See 'Your responsibility for unauthorised use of our electronic banking services' for information about what losses you'll be responsible for if you allow someone to access your accounts using our electronic banking services.

How you can use Bank Mail

You can use Bank Mail to make general account or other enquiries or to request services from us in Internet Banking or the Pacific App. You must make sure the information in your Bank Mail messages is correct. We may send you information about other facilities, products and services using Bank Mail, unless you tell us not to.

We are not responsible for third party software

We are not responsible for third party software used in conjunction with Internet Banking or the Pacific App.

We are not responsible for any Internet Banking module included in accounting software used to access Internet Banking. If you access Internet Banking through accounting software that includes an Internet Banking module, you agree that the Internet Banking module in the accounting software has been acquired by you for your business purposes.

You must make sure the information you send to Internet Banking using an Internet Banking module is correct.

8. How you use the ANZ Pacific App

Your eligibility to register for the Pacific App

To register for the Pacific App, you must:

- be at least 18 years old (unless we agree otherwise);
- be our customer with an account in Cook Island, Fiji, Kiribati, Samoa, Solomon Islands, Tonga or Vanuatu;
- be registered for Internet Banking (and have a valid Internet Banking password and User ID);
- have a mobile device that is enabled for cellular or wireless internet connection, running a minimum iOS software version or Android software version as required; and
- be authorised to use and incur charges on your mobile device account in relation to the Pacific App.

How to register and access your accounts on the Pacific App

You can register for the Pacific App by downloading the Pacific App from the App Store (for iOS) or the Google Play Store (for Android), setting up a four digit PIN and entering your activation code when you receive it from us. You can use either your Pacific App PIN or your Internet Banking logon details to access the Pacific App.

If you have a mobile device with fingerprint, face or other biometric identification capability, you can enable fingerprint, face or other biometric identification access in the Pacific App settings and use your fingerprint or face to access the Pacific App on your mobile device. A fingerprint or face access option will only appear in the Pacific App settings if you have a compatible mobile device and minimum software version.

If you enable fingerprint, face or other biometric identification access in the Pacific App settings, any person whose fingerprint, face or other biometric identification is stored on your mobile device will be able to access your Pacific App account. You must not have fingerprint, face or other biometric identification access enabled in Pacific App settings if someone else's fingerprint, face or other biometric identification is stored on your mobile device.

You agree that you will be responsible for actions on your accounts following successful fingerprint, face or other biometric identification logon to the Pacific App, in accordance with these conditions.

Your access to accounts and availability of the Pacific App

You can access your accounts and your bank statements using the Pacific App. We can limit the type of account you can access.

We will set daily transaction limits on electronic payments from your account using the Pacific App. These limits are specified in the Internet Banking registration forms. Contact us if you would like to discuss changing any of these limits. We may also make changes to these limits at any time. We will let you know if we do so.

As we rely on third parties to make the Pacific App available (like software providers, network service providers and internet service providers) there may be times when access to the Pacific App is limited or unavailable.

At any time, we may suspend or terminate your use of the Pacific App (including any features within the Pacific App). You may be unable to use the Pacific App, if your mobile device hasn't recently been connected to the internet.

How you can help stop unauthorised access to your accounts through the Pacific App

You must call us immediately on the relevant telephone number set out in 'How to contact us' on page 1 of these conditions if:

- your mobile device or the SIM card for your mobile is lost or stolen; or
- you suspect a security breach of your mobile device. This includes if the mobile service on your mobile device is suddenly disconnected without your permission.

To help prevent unauthorised access to your account(s), you must follow our advice about processes and safeguards when using the Pacific App. You must also protect your mobile device.

Don't let unauthorised people or systems access your information

Protect the security of your mobile device:

- Take all reasonable steps to prevent unauthorised use of your mobile device such as keeping your mobile device secure and not leaving it unattended, locking your mobile device when it's not in use, and not leaving your mobile device logged on to our electronic banking services.
- Notify us immediately if either your mobile device or its SIM card is lost or stolen.
- Don't have fingerprint, face or other biometric identification access enabled on your mobile device or in your Pacific App settings if someone else's fingerprint, face or other biometric identification is stored on your mobile device.

Protect the security of your information:

- Don't let anyone see you enter your User ID, password, PIN, security code, security questions or any information about your accounts.
- Don't change your security details in a public place.
- Keep information we send you private.
- Ensure the operating system on your mobile device is regularly updated.
- Don't let anyone else access your accounts through our electronic banking services.
- Don't let anyone else register for the Pacific App using your User ID and Internet Banking password.

See 'How to help protect your passwords, PIN(s), security code, security questions, site key and biometric identification' on page 7 for steps you must take.

Make sure you can trust the mobile device you use and the links you follow

- Only install applications on your mobile device from either the Apple App Store or the Google Play Store.
- Only use the Pacific App to carry out your banking.
- Don't do anything fraudulent or malicious to the Pacific App application or software (for example, don't copy, modify, adversely affect, reverse engineer, hack into or insert malicious codes into the Pacific App application or software).
- Don't override the software lockdown on your mobile device.
- Don't enable or allow jailbreaking (for iPhone) or rooting (for Android) on your mobile device.
- Avoid public Wi-Fi hotspots that are unsecured and don't require a password.

You may be charged fees for using the Pacific App

You may incur charges from your mobile service provider for downloading, updating and using the Pacific App. Your mobile service provider may charge additional fees to access the internet on your mobile device overseas. You're responsible for any fees your mobile service provider charges you. If you have any concerns about a fee you've been charged by your mobile service provider, you should speak with them directly.

ANZ Electronic Banking Conditions

(Cook Islands, Fiji, Kiribati, Samoa, Solomon Islands, Tonga and Vanuatu)

How the Apple Inc. software licence applies to your use of the Pacific App (for iPhone users)

You acknowledge that these conditions are between us and you, and not Apple Inc. You are given a non-transferable license to use the Pacific App on your mobile device in accordance with these conditions and the Apple Usage Rules in the Apple Store Terms of Service.

Subject to these conditions, we are solely responsible for the Pacific App, and Apple Inc. is not responsible for the Pacific App in any way. To the maximum extent permitted by law, Apple has no warranty obligations whatsoever with respect to the Pacific App. You agree that we, and not Apple Inc., are responsible for the following things:

- addressing any claims by you or a third party in relation to the Pacific App, including but not limited to product liability claims, claims that the Pacific App fails to conform to legal or regulatory requirements or consumer protection claims;
- investigating any claim that the Pacific App breaches third party intellectual property rights, and for defending, settling or discharging such claim; and
- maintenance and support services for the Pacific App.

You warrant that you are not located in a country that is subject to a US Government embargo or is designated by the US Government as a 'terrorist supporting' country, and you are not listed on any US Government list of prohibited or restricted parties.

You must comply with all third party service providers' terms of use (for example, software providers and network service providers) when using the Pacific App.

You agree that Apple Inc. and its subsidiaries are third party beneficiaries of these conditions and that Apple Inc. has the right to (and will be deemed to have accepted the right) to enforce these conditions against you as a third party beneficiary.

iPhone and iPad are trademarks of Apple Inc., registered in the U.S. and other countries. Apple Pay is a trademark of Apple Inc. The App Store is a service mark of Apple Inc.

How the Google Inc. software licence applies to your use of the Pacific App (for Android users)

You acknowledge that these conditions are between us and you, and not Google Inc. You are given a non-transferable license to use the Pacific App on your mobile device in accordance with these conditions, subject to the terms of service and policies applicable to your use of Google Play.

You warrant that you are not located in a country that is subject to a US Government embargo or is designated by the US Government as a 'terrorist supporting' country, and you are not listed on any US Government list of prohibited or restricted parties.

You must comply with all third party service providers' terms of use (for example, software providers and network service providers) when using the Pacific App.

9. Content of electronic banking services

We've made every effort to ensure that the information contained in our electronic banking services is complete, accurate and as up-to-date as possible. However, all information contained in our electronic banking services is subject to change.

Our electronic banking services contain some information provided to us by third parties. We are not responsible for the accuracy of information from third parties.

To check that information is up to date, please call us on the relevant telephone number set out in 'How to contact us' on page 1 of these conditions or visit any branch.

By using our electronic banking services, you acknowledge that our electronic banking services contain proprietary content, information and material owned by Australia and New Zealand Banking Group Limited and its licensors, which is protected by applicable intellectual property and other laws. By using our electronic banking services, you agree that you will not make any unauthorised use of any of our proprietary content, information or material provided or made available through our electronic banking services.

Inconsistency

In the event of any inconsistency between the English language and any other language into which this document is translated, the English version shall prevail.

Assignment

Our right to transfer these conditions

We can assign or transfer any of our rights and obligations under these conditions or under any related document to anyone we choose and you agree not to object if we do this. If we choose to assign or transfer any of our rights and obligations under these conditions:

- you agree we don't have to tell you unless we have to under any laws;
- the person we've assigned or transferred these conditions to can use our rights under these conditions; and
- you agree we can share information we have about you, these conditions, and your other agreements with us to allow the assignment or transfer to happen.

You can't transfer these conditions

You must not transfer or assign any of your rights or obligations under these conditions or under any related document unless we've agreed first in writing.

APS 222 Disclosure

You acknowledge that where we are a subsidiary of Australia and New Zealand Banking Group Limited:

(a) we are a separate entity to Australia and New Zealand Banking Group Limited and our obligations under this Agreement do not constitute deposits or other liabilities of Australia and New Zealand Banking Group Limited; and

(b) we are not an authorised deposit taking institution within the meaning of the laws of Australia, and Australia and New Zealand Banking Group Limited does not guarantee our obligations.