Industrial and Commercial Bank of China (New Zealand) Limited

and

Industrial and Commercial Bank of China Limited, Auckland Branch

Terms and Conditions for Electronic Banking Services

Effective 26 May 2023

1. INTRODUCTION

1.1 Overview

This document contains the terms and conditions ("**Terms and Conditions**") for the Electronic Banking Services provided by us. These Terms and Conditions should be read in conjunction with our General Terms and Conditions, which can be obtained at www.icbcnz.com.

These terms and conditions are the terms and conditions of an agreement between us and you. By using our Electronic Banking, you're agreeing to be bound by these terms and conditions, which we can amend from time to time. Please take the time to read this document carefully.

1.2 Changes to these Terms and Conditions

These Terms will continue to apply until we give you notice of any changes to them. We can change any of our Terms at any time. Notice of any changes to our Terms will be given to you at least 14 days before the changes become effective or as required under a specific law. We can choose to contact you either at your most recent address as shown on our records, by public notice, press release, on our website, or by display in our branches, or such other method as we see fit. At times, we may also need to change these Terms and Conditions because of a change in law or a practice that affects everyone who provides the same type of account, product or service, or that we are making to protect the security of your accounts or our systems. We will try and tell you about these changes before they happen but it might not always be possible for us to do.

We can also add to, modify or withdraw any or all of the services provided by us.

1.3 Interpretation

Words in this document that are capitalised are words with specific meanings, as set out under the "Definitions" section below. In addition:

- "**you**" means each person named as an account holder and includes, where the context requires, an Authorised Person. If there is more than one, it means each person jointly and individually (unless the context requires otherwise), and includes their successors and permitted assignees. "**Your**" has a corresponding meaning;
- "**we**" or "**ICBCNZ**" means Industrial and Commercial Bank of China (New Zealand) Limited, Auckland Branch and our successors, assignees and authorised agents. "**Our**" and "**us**" have corresponding meanings;
- a reference to any document (including these Terms and Conditions) includes that document as amended, supplemented or replaced from time to time;
- except where the context requires otherwise (for example, where we refer to protecting your electronic devices from loss or theft), reference to "**loss**" or "**losses**" includes any costs, loss (whether direct or indirect) of profits, business, opportunity or anticipated savings or any indirect or consequential loss however incurred, by you or any other person;
- a reference to "**person**" includes any individual, company, partnership, limited partnership, corporation, trust, joint venture, organisation or governmental agency (in each case whether having separate legal personality);
- a reference to us giving you notice means public notice, press release, notices in our branches or on our website (www.icbcnz.com), mail to the address you have advised to us, or such other method as we see fit;

and

- a reference to our website means www.icbcnz.com.

1.4 Definitions

In this document (unless the context requires otherwise):

"**Account**" means an account you have with us that we have determined is accessible by one or more of the Electronic Banking Services.

"**Alerts**" means the optional alerts service we provide that enables you to receive predetermined Account information electronically (including, but not limited to email, SMS or other electronic messaging services).

"**Authorised Person**" means a specific person or specific persons, or a range or class of persons that you let access and operate your accounts by nominating them as an "Authorised Person".

"**Biometric Identification**" means any means of verifying identity and accessing Electronic Banking Services by using a person's unique physical and other biological traits such as fingerprint identification (for example 'Apple Touch ID' and 'Android Fingerprint Login'), facial recognition technology (for example 'Apple Face ID') or any other biometric identification methods that device manufacturers may provide from time to time, and to the extent we allow you to use those methods to access and use Mobile Banking and other Electronic Banking Services.

"**Business Day**" means any day other than a Saturday or Sunday or public holiday on which banks are open for normal banking business in Auckland.

"**Daily Limit**" means the aggregate maximum amount per day that may be debited to all Accounts pursuant to any one or more transactions.

"**Electronic Banking Services**" means Online Banking, Phone Banking and Mobile Banking.

"**General Terms**" means our General Terms and Conditions (as changed, updated or replaced from time to time), which are available at our branches and on our website. The form of General Terms that will apply will depend on whether the relevant Account is provided by Industrial and Commercial Bank of China (New Zealand) Limited or Industrial and Commercial Bank of China Limited, Auckland Branch - if you're not sure, you can check your statements, ask us at one of our branches or call us on 09 379 5588.

"**Login Details**" means passwords, online banking username, PIN, details relating to your Password Token Device, Biometric Identification, OTP and SMS and /or any other authentication process or identifier offered by us in relation to accessing Electronic Banking Services.

"**Mobile Banking**" means the mode of electronically accessing your Account via a software application and/or web application that has been created to suit small screen and/or portable electronic devices (including, but not limited to, mobile phones).

"**Online Banking**" means the mode of electronically accessing your Account through the Internet other than through Mobile Banking.

"**OTP**" means the 'one-time password' which is sent to your registered portable electronic devices.

"**Password Token Device**" means any device or software we provide to offer an additional layer of protection when logging in and making payments.

"**Phone Banking**" means the service that lets you use your telephone to do things like enquiry..

"**Specific Terms**" means terms and conditions applying to specific accounts, products and services we offer.

"**Transaction Limit**" means the maximum amount that may be debited from an Account pursuant to any one transaction.

"**Unauthorised Transactions**" means transactions made via Electronic Banking Services on your Account without your consent.

1.5 Deemed acceptance

By operating any of your Accounts with us, or by using or receiving any Electronic Banking Services, you acknowledge that you accept these Terms and Conditions.

1.6 Permission to contact you

By registering for Electronic Banking Services you agree that we can contact you by telephone, SMS, email or other electronic messaging services at the contact details you have (or any Authorised Person has) provided to us. (To opt out of receiving marketing and promotional material, you can call us on 09 374 7266.)

2. ELECTRONIC BANKING SERVICES (WHERE AVAILABLE)

2.1 How to apply

You can register for Electronic Banking Services by visiting any of our branches. You can also register for Online Banking on our website, but restrictions will apply to the accounts you can access and/or the transactions you can carry out.

Electronic Banking Services are only available on Accounts that you have nominated and that can be operated by:

(a) you as the sole signatory; or

(b) you alone where only one signatory is required to operate the Account(s).

Once you are registered you may immediately use the relevant service under these Terms and Conditions, any applicable Specific Terms, our General Terms, and as directed by us from time to time.

2.2 Restrictions may apply to your use of Electronic Banking Services

Restrictions may apply to the Accounts you can access and/or the transactions you can carry out using Electronic Banking Services. For example, we may at any time in our absolute discretion set Transaction Limits and Daily Limits that restrict your ability to confirm payment instructions to a specific dollar value. If a payment you submit for processing means you would exceed these limits, you will be notified by display on Electronic Banking Services or, in the case of future-dated payments, the payment will be declined at the time the payment is due to be made. To find out about these limits, or to request a change to your limits, please contact us.

2.3 Availability of Electronic Banking Services

Electronic Banking Services are generally available 24 hours a day, 365 days a year. We will endeavour to provide you with uninterrupted access to Electronic Banking Services subject always to any necessary downtime that may

be required for system maintenance, repairs and updating, or loss of access resulting from matters beyond our reasonable control (such as a failure to connect to the internet or a malfunction of any equipment that supports our Electronic Banking Services).

2.4 The purpose for using Electronic Banking Service

You agree that you will not use Electronic Banking Services for any purpose other than carrying out lawful banking transactions and enquiries on your Account.

2.5 How you can cancel your access to Electronic Banking Services

You can cancel your access to Phone Banking at any time by calling 09 379 5588 or visiting our branches. Other Electronic Banking Services can be cancelled online or by visiting our branches.

2.6 When we can suspend or cancel access to Electronic Banking Services

We can suspend or end your access to Electronic Banking Services at any time. Where appropriate, we will give notice to you under clause 1.2. However, there may be circumstances where we will suspend or end Electronic Banking Services without prior notice to you. We will not be responsible for any loss you may incur as a result of the suspension or ending of your access to Electronic Banking Services unless we have done so in error.

If you do not use Electronic Banking Services for a reasonably long period, we can end your access to Electronic Banking Services without notifying you.

2.7 Fees and charges

A list of the fees and charges we may charge for the use of Electronic Banking Services (which may change from time to time) is set out in our Fees and Charges Brochures, copies of which are available at our branches and on our website. All fees and charges with the use of Electronic Banking Services will be in addition to standard account, transaction and other customer fees.

2.8 Charges for using Phone Banking

You can access Phone Banking in New Zealand free of charge by calling 0800 995588.

You can access Phone Banking out of New Zealand by calling 0064 9 379 5588. You may be charged international tolls if you do so.

2.9 Our responsibility

Subject to our obligations under the Consumer Guarantees Act 1993 (where that applies), we will not be responsible for any loss to you caused by circumstances outside our reasonable control, which includes loss caused by your inability to access Electronic Banking Services, whether through a fault in our system, yours, or somebody else's.

We are also not responsible for any issues concerning your equipment, including security issues. You must take reasonable care to ensure that your system has appropriate anti-virus protection, that the software is up to date,

and that unauthorised persons can't access it (for example, by using your computer or portable electronic device while it is unattended).

3. SECURITY

3.1 Password Token Device

Unless otherwise permitted by us, you must have a Password Token Device to access Online Banking. A Password Token Device is an additional layer of internet security and does not replace or alter your existing access number or Login Details.

3.2 Keep your PINs and passwords hard to guess

You must not choose a PIN or password based on information about you that's easy to find and guess, like your birth date, telephone number, any other number associated with you (such as your driver licence number), parts of number printed on your debit or credit cards, your address street name, your family or pet names. Do not choose a PIN or password that's easy to work out such as repeated or sequential numbers or letters, like 1111, aaaa, 3456 or abcd.

3.3 Protecting your Login Details

You are responsible for keeping your Login Details secure. Where applicable, you must:

(a) memorise your Login Details— do not write them down anywhere or store them on your mobile phone or any other electronic device;
(b) not disclose your Login Details to anybody including family members or those in apparent authority, including bank staff;
(c) make sure your Authorised Persons follow these same security rules;
(d) make sure no one can see you enter your Login Details; and
(e) tell us about any possible disclosure of your Login Details as soon as possible.

3.4 Registering and using Biometric Identification

If you enable biometric identification access to log on to Mobile Banking, anyone whose biometric identification is stored on your device will be able to access your Mobile Banking. You must not have biometric identification access enabled in Mobile Banking Settings if someone else's biometric identification is stored on your device.

You are responsible for keeping your Biometric Identification safe. You must:

(a) never have Biometric Identification enabled for Mobile Banking if someone else's Biometric Identification is stored on your device;
(b) not allow someone else's Biometric Identification to be to be recorded against your account number;
(c) not allow any other person to access or open your device using Biometric Identification; and
(d) make sure any Authorised Person does not allow any other person to be able to access or open your (or the Authorised Person's) device using Biometric Identification.

3.5 Login Details compromised

If you believe someone may have learned your Login Details or that someone else (other than an Authorised

Person) has access to your Accounts (including by way of Biometric Identification), you need to immediately change your Login Details and tell us straight away. Our contact number is 09 379 5588.

3.6 Keeping your banking secure

You must take reasonable care when accessing your Accounts to ensure that your Login Details are not disclosed to any other person. In particular, ensure that you are not observed while entering your Login Details on your computer, telephone or portable electronic device.

You must take reasonable care to keep your Accounts secure, which includes:

(a) taking reasonable care to protect your Password Token Device from loss or theft;

(b) taking reasonable care to protect your computer, mobile phone, or other portable electronic device that you use to access your Accounts, from loss or theft; and

(c) checking your Account records carefully for errors or discrepancies or Unauthorised Transactions, and immediately inform us if you notice any; and

(d) letting us know as soon as any of your contact details (or those of any Authorised Person) including the mobile phone numbers you have provided to us change.

You must not:

(a) permit any other person to use your Login Details;

(b) leave your Password Token Device or mobile phone or other portable electronic devices that you use to access Electronic Banking Services in a location where it can be accessed by other people; or

(c) leave your computer, mobile phone, or other portable electronic devices unattended when logged into Electronic Banking Services.

3.7 Your responsibility for Unauthorised Transactions

You will not be liable for any loss caused by Unauthorised Transactions (unless you have acted negligently or fraudulently, or have contributed to the loss by not following our advice or by not complying with these Terms and Conditions) if you advise us as soon as reasonably possible that you suspect or know that:

(a) your Account has been accessed by someone else;

(b) your Login Details have become known to anyone other than you;

(c) your Password Token Device is lost or stolen;

(d) someone other than you has accessed, or is capable of accessing or opening, your mobile phone, computer or other portable electronic device that is registered for Biometric Identification; or

(e) your mobile phone or other portable electronic devices that you use to access Mobile Banking is lost or stolen.

You will be liable for all loss caused by Unauthorised Transactions if:

(a) you act negligently or fraudulently;

(b) you contribute to the loss by not following our advice or by not complying with these Terms and Conditions;

(c) you did not advise us as soon as reasonably possible once you knew or suspected that someone other than you has accessed or is capable of accessing your Electronic Banking Services, or as soon as reasonably possible after knowing or suspecting that any of the other circumstances listed at the start of 3.7 above applied;

(d) you have left a computer or other portable electronic device unattended when logged on to Online

Banking or Mobile Banking;

(e) you did not reasonably safeguard your Login Details or have kept your Login Details written down;

(f) you have given someone else access to your Accounts using our Electronic Banking Services; or

(g) you have enabled Biometric Identification to access Electronic Banking Services on your device, and someone else's Biometric Identification was stored on your device and was used to access any Electronic Banking Service.

3.8 Instructions

We may carry out any transactions initiated by any means using your Login Details, any of your other security details, or by any other means that we have agreed with you, whether or not you have authorised the transaction, and without making further enquiries. Anyone instructing us using these methods may be able to effect transactions on your behalf. We have the authority to carry out these instructions even if you have specific operating authorities for any of your accounts.

We can refuse to follow an instruction if we suspect that it is made by someone other than you or an Authorised Person, or if we consider we have a good reason to do so (for example, where the instructions are unclear or where acting on such instructions might result in a breach of law).

For the avoidance of doubt, we will not be liable for any loss you incur if:

(a) we act on instructions in accordance withunder your account operating authority or any agreement you've entered into with us about email and fax instructions ;

(b) we act on instructions that are unauthorised, forged or fraudulently given where we could not reasonably have detected that from the instructions;

(c) we do not act on instructions we consider to be unclear, illegible or contradictory: or

(d) you do not comply with any relevant terms for giving instructions.

We are unable to verify the identity of any person who makes payments by accessing an Electronic Banking Service using Biometric Identification. We do not collect or hold any information about your Biometric Identification. The manufacturer of your device is responsible for the security of the device and the reliability of any methods of Biometric Identification. Before using Biometric Identification to access Electronic Banking Services, you should be confident that you are satisfied with the security of your device.

4. OTHER SECURITY MEASURES

To provide more security for Electronic Banking Services for retail customers, we provide a series of safety measures to protect your Accounts and funds, including:

(a) Anti-Fishing ActiveX: a safeguard measure against fraudulent phishing websites;

(b) Online Security Scan: a security check which assists with online scanning and killing of computer spyware that may affect the security of your Electronic Banking Services; and

(c) ICBC Internet Banking Assistant: a program that assists with downloading security and other programs required for Online Banking.

Further details are below.

4.1 Anti-Fishing Active X

We provide protective Anti-Fishing ActiveX controls to prevent your card number and password from being

stolen. You will need to download and install Anti-Fishing ActiveX before using Online Banking.

4.2 Online Security Scan

'Online Security Scan' is a security check for your computer, providing you with strong safeguards in your use of Online Banking. Online Security Scan is also able to detect vulnerabilities in the operating system of your computer and remind you to update your system regularly.

You will need to download and install the Online Security Scan before using Online Banking.

The Online Security Scan can only assist in scanning and killing computer spyware. We are not liable for any damages incurred by the scanning and killing activities of the computer spyware.

4.3 ICBC Internet Banking Assistant

To make it more convenient and stable for users to install needed programs, we provide a tool named 'ICBC Internet Banking Assistant' for you.

'ICBC Internet Banking Assistant' is a program, developed on the basis of the present installer which has automated controls and the related Microsoft patches, that can activate downloading of all programs needed for Online Banking and certificate authorization.

You can download 'ICBC Internet Banking Assistant' from our website and use its guidance function to complete the installation of the certificate drive, the controls and the system patches.

5. PRIVACY

By using Electronic Banking Services, you agree that we may collect and store information about your activity while using those services, and also information about the devices and network you use when accessing Electronic Banking Services. For example, you agree that we may collect, use, store and disclose your IP address and security information. You can find out about the way we collect and use personal information, your rights to access and correct personal information and our legal obligations in our privacy policy, which is available on our website. Our privacy policies apply to any information you give us or that we collect when you use Electronic Banking Services.

6. GOVERNING LAW AND ENFORCEABILITY

These Terms and Conditions are governed by the laws of New Zealand and the Courts of New Zealand shall have jurisdiction to hear and determine disputes in respect of these Terms and Conditions.

If any of our Terms is not enforceable for any reason, the remainder of our Terms will still be enforceable.

7. HOW TO CONTACT US

If you have any questions about Electronic Banking Services, please call us on 0800 995588 (from New Zealand) or 0064 937 95588 (from overseas). International toll charges apply. Our call centre is open 24 hours a day, 7 days a week.