Industrial and Commercial Bank of China (New Zealand) Limited

Terms and Conditions for Electronic Banking Services

Effective 21 March 2018

1. INTRODUCTION

1.1 Overview

This document contains the terms and conditions ("**Terms and Conditions**") for the Electronic Banking Services provided by us. Please take your time to read these Terms and Conditions carefully. These Terms and Conditions, along with our other terms and conditions, can be obtained at www.icbcnz.com, or by calling us on 09 379 5588 (charges may apply).

The terms and conditions governing your general banking relationship with us, including the operation of your bank accounts and other banking services we provide to you, are set out in the General Terms. If there is any conflict between any part of the General Terms and these Terms and Conditions, these Terms and Conditions will apply.

Please note that not all Electronic Banking Services may be available at the time of these Terms and Conditions. To check whether a service is available, please contact us on 09 379 5588 (charges may apply).

1.2 Changes to terms

These Terms and Conditions will continue to apply until we give you notice of any changes to them.

We can change these Terms and Conditions at any time. Notice of any changes to these terms will be given to you at least 14 days before the changes become effective, either at your most recent address as shown on our records, by public notice, on our website, or by display in our branches.

1.3 Interpretation

Words in these Terms and Conditions which are capitalised are words with specific meanings, as set out in clause 1.4 below. In addition:

- "**you**" means each person named as an account holder. 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 and our successors, assignees and authorised agents. "**Our**" and "**us**" have corresponding meanings;
- a reference to any document includes that document as amended, supplemented or replaced from time to time;
- a reference to "**person**" includes any individual, company, limited partnership, corporation, trust, 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

"**Account**" means an account you have with us which 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 person 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 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, Mobile Banking, and Alerts.

"**Fingerprint Login**" means the mode of accessing Mobile Banking by using fingerprint identification.

"**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.

"**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.

"**Loss**" means any costs, loss (whether direct or indirect) of profits, business, opportunity or anticipated savings or any indirect or consequential loss howsoever incurred by you or any third party.

"**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).

"**Password Token Device**" means any device or software, as issued by ICBCNZ from time to time, that is used in addition to an access number and password to securely identify you when you access or use Electronic Banking Services.

"**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.

"**Phone Banking**" means the mode of accessing your Accounts via a touch tone phone.

"**SMS**" means the short message service which sends short messages to portable electronic devices.

"**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 of our products or services, you acknowledge that you accept these Terms and Conditions.

1.6 Permission to contact

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 provided us.

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 which 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 in accordance with these Terms and Conditions, any applicable Specific Terms, our General Terms, and as directed by us from time to time.

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.

2.2 Availability of Electronic Banking Services

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.

2.3 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 enquires on your Account.

2.4 How you can cancel your access

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 visiting our branches.

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

We can suspend or cancel your access to Electronic Banking Services at any time. We do not need to give you notice of this. Where appropriate, we will give notice to you in accordance with 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 consecutive incorrect login attempts are made on your account, your access to Electronic Banking Services will be temporary or permanent suspended. In this case, please contact us by calling 09 379 5588 for assistance.

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

2.6 Fees and charges

A list of the fees and charges we may charge (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 in relation to Electronic Banking Services will be in addition to standard account, transaction and other customer fees.

2.7 Our responsibility

Subject to our obligations under the Consumer Guarantees Act 1993, 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 Selecting password

When you register for Electronic Banking Services, you will be asked to select a password and/or a PIN-. If there is more than one Authorised Person for your account, each Authorised Person must have his or her own password/PIN.

You must not choose passwords or PINs that are the same as other passwords or PINs for other services or that are too obvious and can be easily be guessed. Where applicable, passwords or PINs must not be:

(a) birth dates, months or years;

(b) sequential numbers (eg 3456);

(c) number combinations that can be easily guessed (eg 1111);

(d) parts of your telephone number or any other number associated with you (such as your driver licence number);

(e) parts of numbers printed on your cards; or

(f) family, street, or pet names.

3.3 Protecting your Login Details

You are responsible for keeping your Login Details secure. You must:

(a) memorise you Login Details— do not write them down anywhere or store them on your mobile phone or any other electronic device;

(b) not tell your Login Details to anybody—there is no reason anybody should ever ask for those details (this includes the police, and also us);

(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 elect to unlock your device using Biometric Identification, you may also elect to access your Mobile Banking and make payments using Biometric Identification without entering any further Login Details. However, we will not be able to verify the identity of any person who uses Biometric Identification to access your account from your device because details of the information used for the Biometric Identification will be stored on your device and not stored with us.

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 mobile device;

(b) never record the words or phrases used as part of your Biometric Identification such as the password;

(c) never allow someone else to record their voice as your Biometric Identification;

(d) not allow someone else's Biometric Identification to be to be recorded against your customer number;

(e) not allow any other person to access or open your device using Biometric Identification; and

(f) 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 telling us if you notice any.

You must not:

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

(e) allow any other person to access or open your device using Biometric Identification;

(f) disclose your Login Details to any other person including family members or those in apparent authority, including bank staff;

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

(h) leave your computer, mobile phone or other portable electronic device 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 General Terms) if you advise us as soon as reasonably possible that:

(a) you suspect or know that your Account has been accessed by someone else;

(b) you suspect or know that your Login Details have become known to anyone other than you;

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

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

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

You will not be liable for any Loss caused by Unauthorised Transactions that occur before you are able to access Electronic Banking Services, or during periods when we have prevented you from accessing Electronic Banking Services.

You will be liable for any and all Loss caused by Unauthorised Transactions if:

(a) you did not promptly advise us that someone other than you has accessed or is capable of accessing your Mobile Banking;

(b) you have left a computer or other portable electronic device unattended when logged on to Online Banking or Mobile Banking;

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

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

(e) you have enabled Biometric Identification to access to Mobile Banking on your device, and some else's Biometric Identification was stored on your device and was used to access Mobile Banking.

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 with your account operating authority or a power of attorney;

(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.

ICBCNZ is unable to verify the identity of any person who makes payments by Mobile Banking using Biometric Identification. ICBCNZ does not collect or hold any information about your Biometric Identification from your Mobile Banking.

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 Mobile Banking, you should be confident that you are satisfied with the security of your device.

4. OTHER SECURITY MEASURES

In order to provide more security for its Electronic Banking Services, ICBCNZ provides 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: 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': complete installation of the certificate drive, the controls and the system patches, realise one-stop program downloading.

4.2 Anti-Fishing Active X

ICBCNZ provides protective ActiveX controls to prevent your card number and password from being stolen.

You will need to download and install Active X before using Online Banking.

4.3 Online Security Scan

'Online Security Scan' is a security check for your computer, providing you with strong safeguard in your use of Online Banking. Online Security Scan is also able to detect the vulnerabilities in the operation system of your computer, and remind you to update your system timely, so that it can maintain a healthy condition.

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

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

4.4 ICBC Internet Banking Assistant

In order 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 which, developed on basis of the present installer which has automated controls and the related Microsoft patches, 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 installation of the certificate drive, the controls and the system patches.

5. ALERTS (WHERE AVAILABLE)

5.1 Alerts are only available for Accounts approved by us for that purpose and which you have nominated for Alerts.

5.2 Alerts cannot be sent to an overseas mobile phone number.

5.3 We may from time to time change the form and content of the Alerts without notice to you.

5.4 You agree to promptly advise us of any error or discrepancy relating to Alerts or any information provided by Alerts. We accept no responsibility or liability for the accuracy of the information you supply to us when setting up, changing or deleting your Alerts or for any unavailability or malfunction of the Alerts service. For the avoidance of doubt, this includes the sending of Alerts to email addresses or mobile phone numbers incorrectly entered by you. We do not accept any responsibility or liability for any internal or external use that you or anyone else may make of any data or information provided through or in relation to Alerts.

5.5 Alerts are not encrypted and may include personal or confidential information about you such as your name and Account activity or status.

5.6 Receipt of Alerts may be delayed or impacted by factor(s) pertaining to your internet service provider(s), mobile phone carriers, or other parties. We will not be liable for:

(a) losses or damages arising from any non-delivery, delayed delivery, or misdirected delivery of the Alerts; or

(b) inaccurate content in the Alerts.

5.7 You agree to keep the email and SMS devices (when available) which receive Alerts safe and secure. If these devices are lost or stolen you should go online to cancel your Alerts service or change the mobile or email address details that receive Alerts.

5.8 Fees and charges apply to all Alerts that are generated by us and sent to you, even if you do not receive these Alerts for reasons beyond our reasonable control. The Alert fees and charges are set out in our relevant Fees and Charges Brochure. We can, without notice, debit such fees or charges to the Account the Alert relates to.

5.9 You can cancel your Alerts function at any time. You will remain liable for any obligation that you have incurred in relation to Alerts prior to cancellation. Any amounts owing to us on cancellation of Alerts will become immediately due and payable and will be debited to the Account the Alerts relate to.

5.10 We can cancel or suspend your access to Alerts at any time. We will use reasonable endeavors to notify you prior to cancellation or suspension of the Alerts. We are not liable for any Loss you may incur as a result of your access to Alerts being suspended or cancelled.

6. ELECTRONIC PAYMENTS AND TRANSACTION LIMITS (WHERE AVAILABLE)

Electronic payments include electronic transfers (payment to your own accounts), ICBC payments (payment to an ICBCNZ account), local payments (payment to a non-ICBCNZ account), batch payments, sameday cleared payments and international remittances sending money overseas.

6.1 Notice to set up an Electronic Payment

You can set up and cancel electronic payments using Online or Mobile Banking. Minimum notice periods will apply before your electronic payment will be effective.

For corporate customers, additional restrictions may apply.

6.2 Reversing payments made into your Account

We can, without prior notice, reverse payments made into your Account based on reasonable grounds, including where:

(a) a payment has been dishonored by the paying bank;

(b) you receive a duplicate payment in error;

(c) a payment has been credited to your Account in error; or

(d) we are required to reverse the payment by law.

In the case of clause 6.2(c) above, we will use reasonable endeavors to notify you about the error prior to reversing the payment. However, if we are unable to contact you, we can still reverse the payment if we are reasonably satisfied that the payment was made in error.

6.3 Deducting payments from your Account:

We can debit your Account without prior notice, if we believe you have (or someone else has):

(a) acted fraudulently, negligently or in breach of the law; or

(b) acted in a way that will cause us loss resulting from unauthorised access to your Accounts.

6.4 Sufficient funds

If there are insufficient available funds to meet a payment from an Account we can, in our absolute discretion, choose whether or not to make a payment, retry to make a payment or dishonour a payment.

If we, at our discretion, allow the payment to go through, you will be in unauthorised overdraft and a fee will apply as set out in our relevant Fees and Charges Brochure(s).

Bill payments and automatic payments will only be paid if there are sufficient funds in the payment Account on the Business Day the payment is processed.

If we choose to retry a payment, the payment will be attempted again on the Business Day the payment is processed and the following Business Day until there are sufficient available funds for the payment to be paid. If there are still insufficient funds after that period, the payment will be cancelled and a fee charged.

6.5 Identifying Recipients

Always make sure that the recipient account number is correct. When processing payments we only use the account number to identify the recipient of a payment. Any further details, including the payee name are for your reference only and we are not responsible for matching this information with the account number.

6.6 Changing payment details

We may, without prior notice, change a name, account number or other payment detail in response to a request by the payee (for example, when that person or business changes banks or the business is sold).

6.7 Mistaken payments

We cannot reverse payments you make in error without the consent of the person who owns the account the funds were paid into. If we assist you to recover a payment made in error, a fee or charge may apply.

6.8 Priority of payments

We determine the order in which payments are made to and from your Account.

6.9 Payment date

If a payment is due or retried under clause 6.4 on a non-Business Day we might deduct the payment from your Account on that day, but the payment might not be processed to the payee until the next Business Day.

6.10 How to cancel/change an electronic payment

You may alter or revoke your instruction to make an electronic payment up until our payment cut-off time on the last Business Day before the payment is due to be made. Otherwise you agree that an instruction to make a future-dated payment or transfer continues until the expiry date nominated by you for that instruction.

You cannot stop, cancel, or change an electronic payment once it has been processed by us.

6.11 Liability for Payments

We will not be liable for any loss you incur if:

(a) your payment is not made, is delayed or is sent to the wrong person because you gave us the wrong details;

(b) we refuse to make, or delay, a payment for any reason; or

(c) you cannot use the Electronic Banking Services, for any reason.

6.12 Payments and electronic transfers

Payments and electronic transfers of funds between your Accounts can be processed instantly if your account has sufficient funds.

7. KEY INFORMATION

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.