Industrial and Commercial Bank of China (New Zealand) Limited

Terms and Conditions for Electronic Banking Services

Effective 14 July 2017

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 "**ICBC NZ**" 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 via email or SMS text.

"**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".

"**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 on your mobile device.

"**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.

"**Gesture Login**" means the mode of accessing Mobile Banking by using human gestures identification originating from any bodily motion or state but commonly originating from the face or hand.

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

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

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

"**SMS**" means the short message service which sends short messages to digital mobile phones.

"**Telephone Banking**" means the mode of accessing your Account via a touch tone phone.

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

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

"**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, and email 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. Other Electronic Banking Services can be cancelled online.

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.

If three consecutive incorrect login attempts are made on your account, your access to Online and Mobile Banking will be suspended for the rest of the day. If ten consecutive incorrect login attempts are made, your access will be suspended indefinitely. In either case, please contact us 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. 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 mobile while it is unattended).

3. SECURITY

3.1 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 passwords or PINs for other services or that contain:

(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.

3.2 Keeping password / PIN /Fingerprint or Gesture Login safe

You are responsible for keeping your passwords and PINs safe. You must:

(a) memorise you PINs and passwords—do not write them down anywhere;

(b) not tell you PIN or password 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 PIN or password;

(e) tell us about any possible disclosure of your PIN or password as soon as possible;

(f) not allow any other person to access or open your mobile device using Fingerprint or Gesture Login; and

(g) make sure any Authorised Person does not allow any other person to be able to access or open your (or the Authorised Person's) mobile device using Fingerprint or Gesture Login.

3.3 Registering and using Fingerprint Login/Gesture Login

If you elect to unlock your mobile device using Fingerprint Login or Gesture Login, you may also elect to access your Mobile Banking using Fingerprint Login/Gesture Login without entering any further login details. However, we will not be able to verify the identity of any person who uses Fingerprint Login/Gesture Login to access your account from your mobile device because details of the fingerprint or gesture used for the Fingerprint Login or Gesture Login will be stored on your mobile device and not stored with us.

3.4 PIN compromised

If you believe someone may have learned your PIN, password, or that someone else (other than an Authorised Person) has access to your accounts (including by way of Fingerprint or Gesture Login), you need to immediately change your PIN, password, Fingerprint or Gesture Login (as applicable) and tell us straight away. Our contact number is 09 379 5588.

3.5 Password Token Device

You will need to use a Password Token Device in order to perform certain actions in Electronic Banking Services, such as making a payment. The Password Token Device is an additional layer of security, and does not replace or alter your existing Pin, access number or Password, Fingerprint or Gesture Login.

We may, from time to time and at our discretion, require you to use a different form of Password Token Device.

3.6 Keeping your banking secure

You must take reasonable care when accessing your Accounts to ensure that your password and Password Token Device and any details related to your Password Token Device are not disclosed to any other person. In particular, ensure that you are not observed while entering your password or any details related to your Password Token Device on your computer, mobile phone, telephone, or other 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 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:

(i) permit any other person to use your password, Pin or Password Token Device;

(ii) allow any other person to access or open your mobile device using Fingerprint or Gesture Login;

(iii) disclose your password or any details related to your Password Token Device to any other person including family members or those in apparent authority, including bank staff;

(iv) leave your Password Token Device or mobile phone or other portable electronic device that you use to access the Service in a location where it can be accessed by other people; or

(v) leave your computer, mobile phone, or other portable electronic device unattended when logged into Online or Mobile Banking.

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 PIN or password or any details related to your Password Token Device 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 Mobile Device that is registered for Fingerprint or Gesture Login; 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 losses 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.

3.8 Instructions

We may carry out any transactions initiated by any means using your password and/or PIN (including by way of Mobile Banking using Fingerprint or Gesture Login), 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 unauthorized, 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.

4. OTHER SECURITY MEASURES

In order to provide more security for its Electronic Banking Services, ICBC NZ 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 your Internet Banking security; and

(c) ICBC NZ 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

ICBC NZ 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 Internet 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 Internet 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 Internet Banking.

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

4.4 ICBC NZ Internet Banking Assistant

In order to make it more convenient and stable for users to install needed programs, ICBC NZ provides a tool named Internet Banking Assistant for you.

ICBC NZ 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 Internet Banking and certificate authorization.

You can download ICBC NZ 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 Brochures . 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 Bill payments (a one-off payment to a non-ICBC NZ account), Automatic payments, ICBC NZ - ICBC NZ payments (a one-off payment to another customer's ICBC NZ account) and electronic transfers of money between your accounts. All these payments are limited to accounts in banks within New Zealand.

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. [NB. ICBC to confirm that there is a notification process in place]

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. 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 payments Services, for any reason.

6.12 ICBC NZ - ICBC NZ Payments and electronic transfers

ICBC NZ - ICBC NZ payments and electronic transfers of funds between your own ICBC NZ bank accounts can be processed instantly if your account has sufficient funds.