Industrial and Commercial Bank of China LTD VIENTIANE BRANCH

ICBC Vientiane Branch
E-finance Service Regulations

Article 1 ICBC Vientiane Branch starts network finance business in a move designed to provide its customers with better financial services and at the same time formulates the Regulations in accordance with Lao and Chinese national laws, statutes, and regulatory requirements.

Article 2 ICBC Vientiane Branch provides e-finance services to customers through communication channels, or public networks, or private networks established for specific self-service facilities or customers.

Article 3 The objects of e-finance services include natural persons, legal entities, or other organizations that comply with the laws and regulations of the Lao People's Democratic Republic (Laos) and the relevant requirements of the ICBC Vientiane Branch.

Article 4 Customers applying for the Branch's e-finance services and other participants of its e-finance services shall abide by the Regulations.

Article 5 Customers may register for e-finance services at the Branch's operation offices or through the Internet, mobile phones, and other self-service channels. Customers applying to the Branch for e-finance services shall provide relevant information in accordance with the Branch's requirements and ensure that the information provided is true, accurate, complete, and effective. The branch has the right to review and verify customer identities and data.

Customers shall notify the Branch of any changes to the information they provided. If the Branch is unable to provide e-finance services because of customers' failure to update their information or any error in the information they provided, it shall not be used as grounds for canceling the transaction or refusing the payment, and the customers shall be held liable for such failure.

Article 6 The authentication methods of e-finance service customer identities (hereinafter referred to as "authentication methods") include digital certificate, dynamic password, static password, and others. The Branch offers one or more authentication methods for customers to choose from depending on different types of e-finance services.

Article 7 The Branch provides customers with e-finance services according to customer categories, registration status, authentication methods, and services applied for. Customers who register at banking offices have access to a more comprehensive range of e-finance services compared to self-registered and unregistered customers.

Article 8 All e-finance operations such as the use of customer identifications (including bank account, bank account number, bank card number, user name, telephone or mobile phone number, terminal equipment, etc.) and identity authentication through the method set up by customers at the Branch are considered actions by customers themselves. The instructions given by customers are deemed as effective proof for handling e-finance services.

Article 9 Customers shall abide by the relevant transaction rules of the Branch and operate correctly according to the transaction tips when handling e-finance services.

The customers of electronic payment businesses shall conduct payments within their account payment capability and make sure that the account status is normal; strictly abide by payment and settlement businesses-related laws and regulations; shall not require change or revocation of the implemented electronic payment instructions verified by the Branch.

Article 10 Individual customers without full civil capacity cannot register or change

e-finance services.

Translated Version

Article 11 In the following circumstances, customers shall promptly go through the updating or replacement procedures of corresponding identity authentication media (USB key, electronic cipher, etc.).

(I) Expiry of the validity of the digital certificate or electronic cipher.

(II) Loss of authentication media, leakage of information, or failure of normal use.

Article 12 Customers shall pay attention to the prevention of risks involved in the use of network finance, including but not limited to.

(I) Important information such as e-finance login password, payment password, or user name is guessed or peeped by others, or obtained by means of Trojan horses, fake websites, spoofed text messages, fake phone numbers, etc., which may result in the leakage of customers' bank account information, theft of funds, and malicious operations by others.

(II) USB keys, electronic ciphers, and other authentication media are stolen or used by others without permission, and the authentication media password is stolen at the same time, which may result in the theft of account funds and other consequences.

(III) The theft or unauthorized use of customers' mobile phones by others may cause leakage of information such as bank accounts and authentication received through the mobile phone and may result in the theft of account funds. If the ICBC text messages and other e-finance services are not canceled but the mobile number to receive them is changed, it may lead to customer information leakage provided that the original mobile number resold to others by the telecom operator.

(IV) Important information related to the handling of e-finance services including identity documents, bank cards, passbooks, and reserved bank seals fraudulently used or stolen by others due to loss or improper safekeeping may result in the registration of network finance by others, the leakage of bank account information, and the theft of funds, etc.

Article 13 Customers shall take risk prevention measures for the safe use of e-finance services. Including but not limited to:

(I) Properly keep all important items or information related to e-finance services such as identity documents, bank cards, passbooks, USB keys, electronic ciphers, reserved bank seals, and mobile phones and never hand them over to others or unauthorized personnel for safekeeping; do not leave personal information such as bank card numbers, passbook accounts, ID numbers, frequently used phone numbers at untrusted websites or other places in case of being used by others.

(II) Take good care of bank card passwords, passbook passwords, ICBC electronic cipher passwords, USB key passwords, and other important data, and do not tell anyone including bank staff members, and do not record or save these data on computers, mobiles, telephones, or other electronic devices. After an e-finance service is handled through a device that has a function to store and display input numbers, the stored information like passwords and account numbers should be cleared immediately.

Customers are recommended to promptly exit the network financial system before temporarily leaving in the process of using e-finance services or upon completion of e-finance transactions.

(III) Avoid using obvious personal information (names, birthdays, useful telephone numbers, identity card numbers, etc.) or characters with apparent regularity (such as repeated or continuous numbers or letters) as passwords. Ensure that the passwords for handling e-finance services are different from the passwords for other purposes (bank card/deposit passwords, passwords of the members of other websites, instant messenger passwords, e-mail passwords, and the like); set different passwords for logging onto the e-finance system and payment and frequently change the passwords.

(IV) Adopt effective measures (i.e., installing genuine operating systems, anti-virus software, and network firewalls, and updating them when needed) to protect the security of terminal equipment such as computers or mobile phones used for dealing with e-finance services so as to prevent information leakage or manipulation by others. Customers are recommended not to use online banking on computers shared by multiple people in an Internet café or other places or telephone banking via a pay phone. After changing the mobile number, customers should promptly change their mobile banking, ICBC messenger, SMS authentication, and other e-finance services.

(V) To use Internet banking, please log onto vientiane.icbc.com.cn or www.icbc.com.la to use telephone banking, please dial +856-21-258888-8000 or +856-21-255588.

Download the client software from the Branch's website or the device's designated software website only. Customers should avoid logging into the e-finance service website through other websites, numbers, links, or software.

(VI) Customers using their bank accounts opened with the Branch shall make online payments only through the merchants having a collaborative relationship with ICBC other than the websites or merchants from unknown sources to prevent leakage of passwords and dynamic passwords.

(VII) When using Internet banking to make payments, customers are required not to boot the operating system and the remote assistance functions of MSN, QQ, and other software tools. Customers should check the payee, the payment amount, and other information for errors before the payment; after using Internet banking and logging out safely, take out the USB key and customer certificate media in time and keep them properly.

(VIII) Customers should always check the account funds for any change. If the bank accounts are found being operated by others or the e-finance passwords leaked, or in other suspicious circumstances, customers should immediately go through the procedures of suspending the accounts, resetting the password, replacing identity authentication media, etc.

Article 14 The Bank shall be liable for customers' loss of account funds caused by the rule-breaking operations of the Branch's staff or due to other reasons. For any losses suffered by customers due to their own reasons, such as disclosure of transaction passwords, improper safekeeping of USB keys and other identity authentication media, and failure to meet the obligation to prevent risks and maintain confidentiality, the Bank will not accept responsibility.

The Branch is not responsible for customer losses due to force majeure, computer hacking, system crash, communication fault, network congestion, power supply system failure, computer virus, malicious program attack, and other circumstances that cannot be attributed to the Branch.

Article 15 In order to provide better services to customers and to protect the security of customer accounts and customer funds, when customers access the Branch's website, Internet banking, or mobile device client, and use related services, the Branch may record the information associated with customer operations, including but not limited to network information, device identifiers, hardware information, page resolution ratio, operating system version and language, browser version and language, and the Branch's services related logs; the branch may also obtain such data as the country or city where the customer's mobile phone is located from the cooperating mobile operator based on customers' transactions; the above information can only be used to help recognize customer identities and thus protect their transactions and will not affect customers' normal use of the Branch's services. The Branch will take all reasonable physical, electronic, and administrative security measures to protect the security of customer information and will not make such information available to any third party. The Branch may send text messages and emails or make phone calls to customers based on the communication methods given by themselves. After receiving relevant information, customers should actively cooperate with the Bank to protect their accounts and funds.

The Branch will not under any circumstances take the initiative to ask customers to transfer

funds to a specific account through emails, text messages, or phone calls, nor will it ask customers for bank passwords or other content.So, do not tell anyone else (including bank staff) your bank account passwords. When receiving text messages or emails requesting or enticing them to enter the e-finance password or dynamic password or requiring them to transfer funds to another bank account, customers should remain vigilant and carefully identify the authenticity of the information. If in doubt, customers should immediately dial +856-21-255588-8000 service hotline or to consult with the Branch's operation offices.

Article 16 If customers want to suspend their accounts through Internet banking, it shall take effect once the suspension procedure is completed. The Branch is not responsible for any financial loss arising from customer accounts before account suspension becomes effective.

The suspension of a bank account through Internet banking is interim loss reporting and shall take effect when the formalities are completed. Interim loss reporting is valid for 15 days and will become invalid upon expiration. So, customers should go through the formal suspension procedures at the Branch's operation offices before the term of validity expires or promptly renew the formalities of interim loss reporting. The Branch is not responsible for the economic losses incurred by customers on the above account media before the effective date of or after the expiration of the account suspension.

The reporting can only be terminated at the Branch's operation office.

Article 17 Customers shall pay relevant fees when handling e-finance services in accordance with the charges for e-finance services. The Branch will publish any changes in the above charges beforehand through appropriate means such as its website or operation offices.

Article 18 The Branch shall have the right to suspend or terminate the provision of e-finance services to its customers in any one of the following circumstances:

(I) Customers take advantage of errors or malfunctions in the network financial system to unjustly gain profits or cause losses to others; use the network financial system for malicious or other illegal purposes to conduct unfair transactions.

(II) There is an incident in which lawbreakers fraudulently use a customer's identity to embezzle e-finance information or other incidents that threaten the security of customers' account funds, or there is the possibility of occurrence.

(III) The e-finance services have not been used for more than three years after registration and have not been paid on time.

(IV) Some customer uses false and invalid documents or impersonates another person's documents to register for e-finance services.

(V) When handling e-finance services that use specific terminal information (mobile /telephone number, email address, device identification code, etc.), customers provide incorrect terminal information or fail to notify the Branch of the changes to the terminal information in time, resulting in the bank's inability to provide normal services to all the terminal users.

Article 19 The branch shall have the right to upgrade or adjust e-finance service functions and related transaction rules in accordance with its business development needs, and adopt appropriate means like website announcements and deal alerts to inform customers to handle e-finance services in accordance with the upgraded and adjusted business functions or transaction rules.

Article 20 In the course of engaging in e-finance services, the Branch will not provide sensitive customer information to a third party without customer authorization, except as otherwise stated by national laws and regulations.

Article 21 Customers requiring e-finance services shall confirm compliance with relevant agreements and business instructions. When customers use e-finance services, if the functions of the e-finance service they use are related to other business of the Branch, they must also comply with the articles of association, agreements, or transaction rules related to that business; if the

functions of the e-finance service they use involve a third party, they shall also obey the transaction rules of the third party.

Article 22 In the process of handling e-finance services, if customers encounter problems or are unable to obtain the services, they may make inquiry or consultation in the following ways:

(I) Log into the Branch's website at vientiane.icbc.com.cn or www.icbc.com.la.

(II) Call the Branch's service hotline +856-21-255588 or -856-21-258888-8000.

(III) Visit the Branch's operation offices for advice or assistance in handling e-finance services.

Article 23 If disputes arise in the process of handling e-finance services, customers may negotiate with the Branch to resolve the dispute in accordance with relevant laws, the Regulations, and the provisions of associated service agreements.

Customers, after telling the Branch abnormal e-finance status, should assist the Branch in carrying out investigation and be responsible for the truthfulness of the information provided.

Article 24 The Regulations shall be prepared, amended, and interpreted by ICBC Vientiane Branch. If the Branch modifies the Regulations, it will publish the altered Regulations through appropriate means such as operation offices and websites 30 days in advance. In the notification period, any customers who object to the amendment and decide not to continue using the Branch's e-finance services may go through the e-finance cancellation procedure. If the e-finance services are not withdrawn by the end of the notification period, it shall be deemed to have agreed to accept the changes to the Regulations.

Article 25 The Regulations shall be implemented on 02-11-2020.