上海商業銀行
SHANGHAI COMMERCIAL BANK

June 2025

Notice of Amendments to "Terms and Conditions for Mobile Security Token"

Dear Valued Customer,

Thank you for your valued support to Shanghai Commercial Bank ("the Bank") services.

Please be informed that the Terms and Conditions for Mobile Security Token provided by the Bank will be amended with effect from 31 Jul 2025 ("the Effective Date").

For your easy reference, we have set out below a summary of the major amendments to the Terms and Conditions. In the event of conflict between the summary and the revised Terms and Conditions, the latter shall prevail.

Affected Clause	**Amendments**
Introduction	These terms and conditions ("Terms") apply to and regulate the use of the: **(i)** authentication service of Mobile Security Token, namely and including biometric authentication (including Fingerprint / Face ID authentication / Touch ID) and self-assigned Security Passcode (collectively, the "Authentication Service") **; and (ii) push notification service of Mobile Security Token ("Push Notification Service")** provided by Shanghai Commercial Bank Limited ("the Bank"). By registering or using the Authentication Service **and/or Push Notification Service,** you ("the Customer") are deemed to accept and agree to these Terms.
5.	Clause 5 shall be amended as follows: 5. If the Customer has applied for the Bank's physical Security Device, the Customer should keep it safe as : i. After the Customer registers the Authentication Service successfully, the Customer **may** ~~**is**~~ still ~~**required**~~ **have** to use physical Security Device / SMS One-Time Password to logon Internet / Mobile Stock Trading Services, **as the case requires,** and ii. Once the Customer registers the Authentication Service successfully, the physical Security Device will not be applicable to authenticate Personal Internet Banking transactions. However, once the Authentication Service is disabled due to any reasons, the Customer can use the original physical Security Device to authenticate Personal Internet Banking transactions.

New Clause
To enhance our services, we will be updating the “Terms and Conditions for Mobile Security Token”, including provisions related to push notifications. For full details of the changes, please refer to clause 8 of the “Terms and Conditions for Mobile Security Token” at our website www.shacombank.com.hk (Latest News).

Save as mentioned above, the Terms and Conditions for Mobile Security Token shall remain unchanged and continue in full force and effect.

Please note that the above amendments shall be binding on you if you continue to use or retain the services after the Effective Date. If you do not accept the above amendments, we shall not be able to continue providing services to you and you can notify the Bank for termination of service before the Effective Date.

Should you have any enquiries, please call our Customer Service Hotline on 2818 0282 or visit any of our branches.

Yours faithfully,
Shanghai Commercial Bank Limited

This is a computer-generated printout and no signature is required. In case of inconsistency between the English and Chinese versions of this letter, the English version shall prevail

上海商業銀行
SHANGHAI COMMERCIAL BANK

Terms and Conditions for Mobile Security Token

These terms and conditions ("Terms") apply to and regulate the use of the: **(i)** authentication service of Mobile Security Token, namely and including biometric authentication (including Fingerprint / Face ID authentication / Touch ID) and self-assigned Security Passcode (collectively, the "Authentication Service")**; and (ii) push notification service of Mobile Security Token ("Push Notification Service")** provided by Shanghai Commercial Bank Limited ("the Bank"). By registering or using the Authentication Service **and/or Push Notification Service**, you ("the Customer") are deemed to accept and agree to these Terms.

1. The Authentication Service provides the Customer with an alternative means to log into i-Banking Services (including but not limited to Internet / Mobile Banking Services) via the Bank's Mobile Application - Shacom Bank ("Shacom Bank") and other systems as specified by the Bank from time to time or to authorize instruction in respect of transactions as specified by the Bank from time to time by using biometric authentication record(s) stored on the Customer's designated mobile device or self-assigned Security Passcode. Designated mobile device means a mobile device which is compatible to Shacom Bank and the Authentication Service as may be determined by the Bank from time to time.

2. By registering the Authentication Service, the Customer agrees that the Bank may treat and consider as valid and binding on the Customer any instruction given, or agreement made with the Bank, which is authenticated through the Authentication Service without the Bank making any further inquiry as to the authority or identity of the person making or purporting to give such instructions or to make such agreement or their authenticity notwithstanding any error, misunderstanding, fraud, forgery or lack of clarity in the authorization. The Customer acknowledges that the Bank may still require the Customer to authenticate a transaction by the password and/or another form of authentication even though the Customer has authenticated the same by the Authentication Service.

3. The Authentication Service is provided as part of the Bank Services, and accordingly:
   i. these Terms are in addition to and shall be read in conjunction with Terms and Conditions for i-Banking Services and any other documents forming part of the Bank's banking agreement (and any reference to the Terms and Conditions for i-Banking Services shall include reference to these Terms);
   ii. in the event and to the extent of any inconsistency between these Terms and the Terms and Conditions for i-Banking Services, these Terms shall prevail.

4. The Customer acknowledges and agrees that in order to use the Authentication Service for Shacom Bank and/or other electronic systems of i-Banking Services of the Bank:
   i. The Customer must be a valid user of the Bank's Personal Internet Banking ;
   ii. The Customer must install Shacom Bank using a designated mobile device;

iii. The Customer will need to activate the biometric authentication function on the designated mobile device;

iv. The Customer must register the Authentication Service through Shacom Bank by using Personal Internet Banking User ID and Password and SMS One-time password and (a) register biometric authentication and setup a Security Passcode; or (b) setup a Security Passcode only (applicable to the mobile devices which do not support biometric authentication function or other cases determined by the Bank);

v. The Customer understands that upon the successful registration of the biometric authentication service on the designated mobile device, any fingerprint(s) or facial map that is/are stored on the Customer's designated mobile device can be used for the purpose of the Authentication Service. The Customer must ensure that only authorized fingerprint(s) or facial map is/are stored on the Customer's designated mobile device to access the device;

vi. The Customer agrees that the Customer must and undertake to protect the designated mobile device which has installed Shacom Bank and registered for the Authentication Service, including but not limited to (a) setting safe device password for the designated mobile device which has installed Shacom Bank and registered for the Authentication Service, (b) not allowing any other person to register Biometric Credentials, create password on the designated mobile device which has installed Shacom Bank and /or use the Authentication Service, and (c) not allowing jailbreak/ rooted mobile device registered for the Authentication Service. The Customer acknowledges that the use of the Authentication Service on a jailbreak / rooted mobile device may compromise or affect security and lead to fraudulent / unauthorized transactions and the Bank will not be liable for any costs, expenses, damages, liabilities, interests, losses or any other consequences suffered or incurred by the Customer as a result. The Authentication Service registered under the Customer's account is for the Customers' own use only, (d) not using facial recognition to verify and confirm the Customer's identity if the Customer has an identical twin sibling or relatives who look very alike, in which case the Customer is recommended instead to use Fingerprint or Personal Internet Banking User ID and Password or physical Security Device to verify and confirm the Customer's identity, (e) not using facial recognition to verify and confirm the Customer's identity if the Customer is an adolescence while the Customer's facial features may be undergoing a rapid stage of development, in which case the Customer is recommended instead to use Fingerprint or Personal Internet Banking User ID and Password or physical Security Device to verify and confirm the Customer's identity; and, (f) the Customer should not take any action to disable any function provided by, and/or agree to any settings of, the Customer's mobile device that would otherwise compromise the security of the use of the Customer's biometric credentials for biometric authentication (e.g. disabling "attention-aware" for facial recognition); and

vii. The Customer will use all reasonable care to keep the designated mobile device secure. The Customer will notify the Bank as soon as reasonably practicable if the Customer finds or believes that the designated mobile device has been lost or stolen or that any unauthorized transactions have occurred. The Bank reserves the right to suspend or terminate with or without notice the access to and/ or use of the Authentication Service (or any other services) without any liability, at the Bank's sole discretion.

5. If the Customer has applied for the Bank's physical Security Device, the Customer should keep it safe as :
   i. After the Customer registers the Authentication Service successfully, the Customer **may** ~~**is**~~ still ~~**required**~~ **have** to use physical Security Device / SMS One-Time Password to logon Internet / Mobile Stock Trading Services, **as the case requires,** and
   ii. Once the Customer registers the Authentication Service successfully, the physical Security Device will not be applicable to authenticate Personal Internet Banking transactions. However, once the Authentication Service is disabled due to any reasons, the Customer can use the original physical Security Device to authenticate Personal Internet Banking transactions.

6. The Customer acknowledges that the authentication is performed by the Bank's Shacom Bank by interfacing with the security authentication module on the designated mobile device and the Customer agrees to the authentication process. The Bank will not collect/store the security authentication record in any manner at any stage of the Customer's registration or use of the Authentication Service.

7. The Customer can cancel the Authentication Service at any time on the left navigation menu "Settings > Mobile Security Token" in Shacom Bank or contacting the Bank's customer service hotline. Please note that after the Customer has cancelled the Authentication Service, the Customer's biometric data will be continuously stored on the Customer's designated mobile device. The Customer may consider to cancel the data in the mobile device at own decision.

8. ~~**The Customer must allow receiving push notifications for Shacom Bank on the Customer's designated mobile device. Otherwise, the Customer may be unable to use Shacom Bank; and will not be able to receive notifications from Shacom Bank.**~~

Push Notification Service is provided as part of Mobile Security Token and the Bank Services. By using Push Notification Service, Customer agrees and undertakes to comply with the User Requirements for Push Notification Service (the provisions of which are reproduced hereunder for reference only and do not form part of these Terms) as may be amended by the Bank from time to time. The Bank has the right to specify or vary the scope and extent of (or otherwise discontinue) the Push Notification Service and its features from time to time without prior notice. To the extent permitted by law, the Bank shall not be liable for any direct and indirect, consequential, or incidental loss and/or damage which will be incurred or suffered by the Customer in connection with the use of Push Notification Service.

User Requirements for Push Notification Service
i. The Customer may register one mobile device (iOS or Android OS device) to receive push notifications. The Customer's mobile device should use the updated iOS or Android OS version specified by the Bank. Push notifications could only be sent via the services provided by Apple Inc. ("Apple") or Google LLC. ("Google"). The Customer must register Mobile Security Token on the Customer's mobile device in order to use the Push Notification Service.
ii. In order for the Customer to receive notices and communications from the Bank,

the Customer must allow receiving push notifications for Shacom Bank mobile app on the Customer's designated mobile device and make sure the Customer has Cellular Data Internet Connection or Wi-Fi Internet Connection. If the Customer is travelling overseas and wishes to receive push notification messages, the Customer should check whether data roaming is enabled. The Customer is responsible for any fees and charges arising from internet connection (whether local or international). Push Notification Service may not be available in certain countries/regions on certain types of mobile devices.

iii. **Each push notification will only be sent once. If the Customer deletes a push notification sent to the Customer, that notification will not be sent again.**

iv. **The content sent by push notifications may not be encrypted and may not be secure from corruption by third party. Push notifications may not be free from interference, interception, interruption, intervention or meddling by third parties. The Bank shall not be liable for any loss, cost or damage of any kind incurred or suffered by the Customer to the extent that it is attributable to any cause or circumstance that is beyond the Bank's reasonable control. The Bank shall not be liable for any loss if there is any delay or failure in delivering push notifications due to any defects or problems in the services of Apple, Google, other third party service providers or otherwise whatsoever, whether under the Bank's control or not. Android users may be unable to receive push notifications due to limitations on Google services in some countries or regions.**

v. **The Customer is responsible for ensuring that the Customer's mobile device has sufficient anti-virus protection and to make sure that the Customer's mobile device is enabled with auto-lock and passcode lock to prevent unauthorized access. The Customer should keep the Customer's mobile device safe and secure.**

vi. **Any information provided through push notifications is for reference only and should not be relied on by you. We do not warrant the accuracy, reliability, completeness or timeliness of this Service and shall not be liable for, to the extent permitted by law, any direct and indirect consequential or incidental loss or damage which will be incurred or suffered by you in connection with the use of this Service.**

vii. **All services, products and offers stated in push notifications are subject to the relevant terms and conditions of that services, products and offers.**

viii. **The Customer's pre-existing instructions to the Bank in receiving direct marketing materials will not be affected by switching on this Service.**

ix. **The Customer can disable the Push Notification Service at any time on the Customer's mobile device. After the Customer disables the Push Notification Service, the Customer's pre-set notification preference may be removed on the designated mobile device. The Customer may re-define the Push Notification Service preference in the mobile device at own decision after re-enablement.**

9. If the Customer's biometric data or self-assigned Security Passcode of the Customer's designated mobile device has been compromised, the Customer is required to re-register or cease the Authentication Service.

10. The Customer will be liable for all losses incurred if the Customer has acted fraudulently or negligently, or has allowed any third party to use the designated mobile device, or has failed to comply with the obligations under these Terms, Terms and Conditions for i-Banking Services, security information and/or other relevant documents as provided by the Bank from time to time. The Customer would not otherwise be responsible for any direct loss incurred as a result of unauthorized transactions conducted through the Customer's account.

11. In addition to and without prejudice to the disclaimers and exclusions of liability in the Terms and Conditions for i-Banking Services:
    i. The Customer understands that the biometric authentication module of the designated mobile device is not provided by the Bank, and the Bank makes no representation or warranty as to the security of the biometric authentication function of any designated mobile device and whether it works in the way that the manufacturer of the device represents.
    ii. The Bank does not represent or warrant that the Authentication Service will be accessible at all times, or function with any electronic equipment, software, infrastructure and/or other Internet Banking that we may offer from time to time. The Bank shall not be liable for any loss incurred by you as a result of this.
    iii. The Customer will indemnify the Bank and keep the Bank fully indemnified against all consequences, claims, proceedings, loses, damages, liabilities, interests, costs and expenses (including all legal costs on an indemnity basis) which are of reasonable amount arising from or in connection with any use of the Authentication Service provided by the Bank, except any direct loss or damages caused by breach, negligence or default on the part of the Bank.
    iv. These Terms may be amended or supplemented by the Bank at its sole discretion from time to time with reasonable prior notice (as practicable) to the Customer. Such amendments or supplements will be sent to the Customer by post or posted on the Bank's Website, branches, advertisement, electronic communications (e.g. email) or any other channels that the Bank specified from time to time and will become effective on such date and time as stipulated by the Bank, which shall be binding on the Customer if the Customer continues to use the Authentication Service after the Bank's designated effective date and time of such amendment/ supplement. Each access to and use of the Authentication Service shall be subject to provisions of these Terms then in force.

12. The Bank shall be entitled, at any time with or without immediate or prior notice, to suspend or terminate the Customer's registration for any of the Authentication Service and without any liability, at the Bank's sole discretion, in such circumstance as the Bank may solely see fit which shall include without limitation:
    i. The Bank has reasonable grounds to believe or suspect that the security of the Customer's data or registration details is at risk;
    ii. It is appropriate or prudent for the Customer's protection;
    iii. The Bank has reasonable ground(s) to believe or suspect that the Customer's registration has been used in relation to fraudulent or illegal activities;

iv. The Bank is required to do so by any applicable laws, regulations, compliance requirements, listing rules, regulatory authority, competent court of law or governmental body requirement.
v. The Customer's biometric record of the Customer's designated mobile device has been changed
vi. The Customer registers the Authentication Service in other devices in respect of the same Personal Internet Banking account;
vii. The Customer has exceeded the threshold imposed by the Bank from time to time for invalid Security Passcode input attempt;
viii. The Customer has exceeded the threshold imposed by the Bank from time to time for invalid biometric authentication attempt;
ix. The Customer's Personal Internet Banking account has been terminated;
x. The Customer's Personal Internet Banking password has been reissued.

13. The laws of the Hong Kong Special Administrative Region of the People's Republic of China shall govern these Terms. The Customer hereby irrevocably submitted to the non-exclusive jurisdiction of the Hong Kong courts.

14. The Chinese version of these Terms are for reference only and if there is any conflict between the English and Chinese versions, the English version shall prevail.