Two-factor Authentication Tools

To enhance online security, the Internet Banking and Mobile Banking Services of the Bank provides customers with a "Security Device" and "Mobile Token" as the two-factor authentication tools. "Security Device" with audio capability is also provided for the convenience of the visually impaired using Internet/Mobile Banking. Customers are required to use the "Security Device" or "Mobile Token" and agreement to receive specified transaction notification to conduct online Designated Transactions.

In addition, corporate customers can apply the "Security Device" at any of our branches.

Mobile Token

- "Mobile Token" is a built-in function of NCB Mobile App. Once the "Mobile Token" is activated, you will be spared the hassle of carrying a separate physical "Security Device" to truly enjoy convenient and secure banking.
- Upon activating the "Mobile Token" on compatible mobile device, you can confirm designated Mobile Banking transactions or designated investment transactions via the preset passcode or using "Biometric Authentication". In addition, you can also confirm designated Internet Banking transactions by generating a one-time "Security Code"/"Transaction Confirmation Code" via the "Mobile Token".

Points to Note for “Mobile Token”:

- For security reasons, customer can only activate “Mobile Token” on one mobile device and please do not login Mobile Banking and activate "Mobile Token" on others’ mobile phone.
- For personal customers, upon successfully activation of “Mobile Token”, the “Security Device” (if any) will be suspended. For reactivation of “Security Device”, customers are required to suspend the “Mobile Token” on your mobile device, and visit any branch of the bank personally to reactivate the “Security Token” or via Corporate Internet Banking for corporate customers.
- Please keep your mobile device that has activated “Mobile Token” function in a safe and secure place. If you find or suspect that your mobile device that has activated

"Mobile Token" function is lost or stolen, you may log in mobile banking service via another mobile device and activate "Mobile Token" function to automatically deactivate the "Mobile Token" function on the lost or stolen mobile device.

Biometric Authentication

- You can register "Biometric Authentication" (e.g., Fingerprint, Face ID) on your mobile device for logging in Personal Mobile Banking. When you further activate "Mobile token" function, you can then use "Biometric Authentication" to enable "Mobile Token" to confirm designated Mobile Banking transactions, or to enable the "Mobile Token" to generate a one-time "Security Code"/"Transaction Confirmation Code" to confirm designated Internet Banking transactions.
- When you activate "Mobile token" function on Corporate Mobile Banking, you can register "Biometric Authentication" (e.g. Fingerprint, Face ID) on your mobile device for logging in Corporate Mobile Banking service. You can use "Biometric Authentication" to enable the "Mobile Token" to generate a one-time "Security Code"/"Transaction Confirmation Code" to confirm designated Internet Banking transactions.
- To learn how to activate the "Mobile Security Code", operating system requirements and compatible mobile devices, please visit: www.ncb.com.hk/nanyang_bank/faq/person-bank/SecurityCode.
- Please ensure proper protection of your biometric authentication information, including but limited to fingerprint(s), facial feature(s) or any other biometrics as recognised by the Bank from time to time, and ensure the confidentiality of the security codes as well as the password that you use to store your biometric credential(s) and register the biometric authentication on your designated mobile device. If you have found or suspected your biometric credential(s) has/have been compromised, please contact us immediately, or directly contact the Hong Kong Police Force.

Security Device

Application for the "Security Device" can be made through our Internet Banking, at any of our branches. Upon receipt of customers' application, we will send the "Security Device" to customers' registered correspondence address.

Please be reminded of the following when you use the "Security Device":

- Please visit any of our branches to apply for a “Security Device”.
- Upon receipt of the "Security Device", please log into the Internet Banking immediately and follow our instructions to activate the "Security Device".
- No extra software / driver or authorisation code generated by a third party is required.
- Corporate customers who have selected the "2FA Login", please enter “Challenge Code” on “Security device” to have a “Transaction Confirmation Code” to log into the Corporate Internet Banking.
- Personal customers who have selected the "2FA Login", please enter one time “security code” generating from “Security Device” to log into the Personal Internet Banking.
- Customers are required to enter specific transaction information (e.g., “Challenge Code”) into the "Security Device" to generate a one-time Transaction Confirmation Code for Designated Transactions.
- Please keep your "Security Device" in a safe and secure place. You should not allow anyone to use your "Security Device" or leave it unattended. In case of loss or damage, please contact our staff immediately.

How does the "Security Device" work?

- Each "Security Device" contains a unique serial number, internal information and a clock. Once the "Security Device" is activated, the internal clock will synchronise with our system. When you press the button on the "Security Device", a one-time Security Code will be generated according to the information and clock inside the Device. The Code, for verifying the identity of customers, is valid within a short time interval. If the time permitted for the entry of the Security Code expires, you have to press the button again to generate another Security Code.

How do I use the "Security Device"?

- Different Security Codes will be generated by the "Security Device" depending on the nature of transactions. Customers should follow online instructions to complete authentication procedures.
- When logging into the Corporate Internet Banking or performing general transactions, you should press the button at the bottom right hand side of the "Security Device". A 6-digit Security Code will be displayed on the LCD screen of the "Security Device". The Security Code, valid within a short time interval, is for one-time use only.
- When performing "Designed Transactions", you should press the button at the bottom left hand side of the "Security Device" and enter the digits highlighted in RED online into the number keys of the Device. After you have input the required information, please press the left button at the bottom again. A 6-digit Transaction Confirmation Code will be displayed on the LCD screen of the "Security Device". The Transaction Confirmation Code, valid within a short time interval, is for onetime use only.

I have entered the "Security Code" or "Transaction Confirmation Code" into Internet Banking, but my transaction instruction cannot be verified. Why?

- Your transaction instruction may not be verified by Internet Banking due to the following reasons:
  - Entry of incorrect code

- The time permitted for entry of the code has expired
- The "Security Device" has been hit or exposed to heat, cold or wet conditions or magnetic fields

- Please follow our online instruction and enter a valid "Security Code" or "Transaction Confirmation Code". If your transaction instruction still cannot be verified, please contact our staff to reset the status of your "Security Device".
- In case the verification process is still not successful after resetting of the device's status, Customers can apply to replace a "Security Device" and it will be free of charge.

What if the message "BATT" is displayed on the LCD screen?

- "BATT" means that the "Security Device" will soon run out of battery. The battery normally lasts for 3 to 5 years, depending on the frequency of your usage. Customers must visit any of our branches to apply for replacement. Please note that the battery of the "Security Device" cannot be replaced. Any attempt to remove the components of the "Security Device" may cause malfunction of the Device.

OTP for activation of "Security Device" and "Notification of Execution of Designated Transactions"

- The Bank's SMSs (if any) in respect of "OTP" and "Notification of Execution of Designated Transactions" will be sent only to your mobile phone number registered with the Bank. Such SMSs will not be forwarded to any other mobile phone number even if you have enabled the "SMS Forwarding Service" provided by any the following local mobile phone service providers in Hong Kong:
  - SmarTone Mobile Communications Holdings Limited
  - CSL Limited
  - Hutchison Telephone Company Limited
  - China Mobile Hong Kong Company Limited

- You are advised to check carefully the transaction details sent by the Bank through an SMS and an email against the transaction conducted by you via the Internet Banking/Mobile Banking. Please contact us immediately if you have any enquiry.