Security Information

This webpage sets out the security information of the electronic banking ("e-banking") Services offered by Nanyang Commercial Bank, Limited ("the Bank"). e-banking services refers to banking services delivered over the internet, wireless network, ATMs, telephone network or other electronic network, terminals or devices, including but not limited to the Bank's Internet Banking (Personal and Corporate), Mobile Banking (Personal and Corporate), Phone Banking, NCB e+ Mobile Application ("NCB e+"), Automated Banking and WeChat official account.

Latest / Important Security Information

Beware of Mobile Device Malware Scams

Identify the Malware Scams

- Malware are designed to infiltrate, damage or obtain information from a mobile or computer device without the owner's consent. These include spywares, computer viruses and Trojan horses.
- Spyware is a type of software that is installed on a device, without permission from user. It could monitor and record device user's device user information or system behaviour by hiding its malicious purpose. It collects and transmits the gathered information (for example, personal credentials including user name, password and credit card numbers, etc.) to unauthorised third parties for own benefits.
- A virus may contain destructive code that can move into multiple programmes, data files or devices on a system and spread through multiple systems in a network, resulting in the malfunction of the devices and loss of the data.
- There is one more type of malware called trojan horse. It masquerades as legitimate programme, takes control of your device and performs illicit operations unnoticed by the users.

How to properly address

- You shall Search "NCB" (Nanyang Commercial Bank) for free download of NCB Personal Mobile Banking ("NCB Mobile APP"), NCB Corporate Mobile Banking ("NCB Corporate Mobile Banking") and NCB e+ Mobile Application ("NCB e+") from recognized official App stores (such as Google Play, App Store, and Huawei App Gallery HK, etc.).
- You shall ensure the device configuration remains correct, and should not download any mobile applications from unknown sources.
- Evaluate permissions requested from mobile applications carefully before installation, do not grant permissions lightly, especially those that could give third-party Apps complete control over your device or share your screen; if suspicious permission rights are required, do not install the mobile application.
- Firewall software and anti-virus software should be installed on personal computers and updated regularly.
- To ensure the security and confidentiality of devices accessing mobile banking, avoid modifying your mobile devices with Jailbreak or Root or use mobile devices that have been modified by such methods.
- Do not use applications from unknown sources under any circumstances. Do not click any links in unknown text messages, emails, webpages or social media content, nor download any files from these links. . If there are suspicious App for downloading, please do not login and stop proceeding the download immediately.
- You should ensure that your devices for accessing e-banking services do not being infected by virus or unauthorised accessed by malicious, corruptive or destructive program, for the retrieval, use and change of the password, Biometric Authentication (e.g., fingerprint, Face ID) or personal information.
- In response to recent malware scams and to protect customers' account security, the Bank has disabled screen capture and screen recording functions on mobile devices for the Mobile Banking App (Personal and Corporate). Meanwhile, if the Bank identifies potential risks on your Android device, such as suspicious applications installed, or applications that enable relevant "Accessibility" features; under such

cases, you might be unable to continue using the Mobile Banking App. The Bank recommends deleting the suspicious applications, or disabling the relevant accessibility features (if applicable), to protect your account security.

Beware of fraudulent calls, SMS, emails

Identify the fraudulent calls, SMS, emails

- A caller may claim to be from the Bank or another financial institution and may, for instance, invite you to apply for a financial service such as personal loan, and induce customers to provide personal information or make deposits into designated account to apply for banking services; or claim that there are some irregularities with your bank account or card, requiring you to provide personal information for account authentication or checking.
- Fraudsters may claim that unusual transaction record had been identified in your bank account / credit card through pre-recorded message phone call, and then request you to provide them sensitive personal information such as account number, username and log-on password for "investigation". They may even purport as courier company employee, government official, or your relative, friend or business partner and force you to provide personal information, or to transfer a sum of money to a designated bank account for various reasons.
- During the impersonation, fraudsters may have correspondingly provided bank staff information (as they can obtain such information through illegal means). Fraudsters may present a highly-imitated staff card, name card; or behave as no fear on identity verification by providing you a fake staff number in order to promote their reliability. Meanwhile, the bogus calls usually have poor call quality, as if they are long-distance calls.

How to properly address

- **Security Tips for Bogus Call**
  - Customers are reminded to stay vigilant to the bogus calls, and voice message telephone calls purportedly from banks.

- Customers shall not share any sensitive personal information (including login passwords or other authentication information, such as one-time passwords, "security code" generated from "Security Device" or "Mobile Token".) to any callers. If you have any inquiry or have shared any personal details with a caller, please contact us at: (852) 2616 6628, and report the call to the police immediately (or request the assistance through contacting the 24-Hour Enquiry Hotline 18222 of the Anti-Deception Coordination Centre, Hong Kong Police Force).
- Please be noted that, the Bank will never ask for your sensitive personal information in way of phone call, SMS or email (including login passwords or other authentication information, such as one-time passwords, "security code" generated from "Security Device" or "Mobile Token"), nor notify you of abnormal bank account activities through pre-recorded voice messages. Please stay alert if you receive a call or voice message claiming to be from the bank staff.
- To protect customers' interests, the Bank have joined the SMS Sender Registration Scheme ("Scheme") launched by the Office of the Communications Authority ("OFCA"). To facilitate customers verifying the identities of SMS senders and protect against fraudulent activities, please visit the Bank's website for details (the Bank's website> About Us>Notice> "Notice of Implementation – SMS Sender Registration Scheme").
- When receiving calls or messages from individuals purporting as employee of telecommunications company, courier company, online shopping or payment platforms, or government officials, you may firstly verify the caller's number and identify through official channels. Do not rush to transfer fund to or disclose personal information to unknown person.

- **Mitigating measures when receiving suspicious calls**
  - Customers are reminded that, if the call is made by a staff from the Bank, customers will be informed clearly with the information including but not limited to: the staff's name, the staff number, the contact number, and the message to reminder customers that one can verify the caller's identity by calling the Bank's 24-hour Security Hotline (852) 2616 6628.

- Customers can have a verification of phone calls purporting to be initiated by or related to the Bank based upon the information provided by the caller. Customers can further ask for the caller's department/branch name and office number and check that how they got your phone number and account information. If they are unwilling or reluctant to provide the information, please hang up immediately.
- If you have shared any personal details with a suspicious caller, please contact the Bank at: (852) 2616 6628, and report the call to the police (or request the assistance through contacting the 24-Hour Enquiry Hotline 18222 of the Anti-Deception Coordination Centre, Hong Kong Police Force).
- If you shared a caller with your password, change it immediately.
- You can call the Bank at: (852) 2616 6628 if you need to suspend your e-banking account function (You can visit any of our branches to resume your e-banking service afterwards).

- **You can choose the either way below to verify the identity of the caller:**
  - call the Bank's 24-hour Security Hotline (852) 2616 6628 (press "9" after language selection); OR
  - Fill and submit the form on Bank's website "Contact Us > Online enquiry and security issues", the Bank will follow up within 1-2 working days; OR
  - Visit any of our branches.

Beware of phishing

Identify the phishing

- Phishing is a common fraudulent technique. Fraudsters would pretend themselves to come from legitimate organisations such as banks, payment service providers and online retail merchants. They would trick a victim to provide sensitive information and authentication information (such as login password, one-time password) through electronic communications such as emails, SMS, or instant messages within counterfeit online shopping platform. The phishing emails may also include a

malicious hyperlink, attachment for the recipients, or providing a QR code for redirecting the recipient to illegal websites. Once connect to an illegal website, the recipient are usually required to enter personal sensitive information or authentication information (such as login number, account number, login password, one-time password). Phishing websites collect all information entered by victims, and fraudster use this information to steal funds from victims' account, resulting in financial losses.

How to properly address

- Please be noted that, the Bank will never ask for any sensitive personal information (including login passwords or other authentication information, such as one-time passwords, "security code" generating from "Security Device" or "Mobile Token") in way of third-party websites, mobile applications, phone call, SMS, or email, nor direct customers to conduct transactions on the Bank's website or mobile application through hyperlinks, OR codes, or attachments in SMS or email. Customers must carefully safeguard their personal information and authentication factors. If customers receive such request, please contact the bank immediately.
- To ensure transaction security, customers should directly enter the bank's website in the browser's address bar for logging in to Internet Banking. Do not log in to Internet Banking via any hyperlinks embedded in emails, SMS, QR codes, internet search engines, or social media platforms, nor through unauthorized third-party websites or mobile applications. If any doubt, please stop all operations immediately, refrain from entering any information and close the window.
- Customers should stay vigilant of any unusual login webpages during their Internet Banking login process (such as unusual screens pop up and/or the unusually slow computer response, repeated requests to enter passwords). Avoid logging in to Internet Banking by using unknown Wi-Fi or public computer.
- When conducting online transactions, please verify the transaction details carefully (such as transaction type, transaction amount, and currency) to review the transaction prior to entering authentication information for transaction authentication. Do not enter one-time passwords without reviewing the transaction details. Prior to entering any information or conducting transactions, check out

whether the webpage address is authentic and trustworthy. For inquiries, please contact the Bank immediately

- Prior to making payments with mobile phone number, email address, FPS ID, or QR code, please verify the payment details carefully, including the payee's name. If in any doubt, confirm with the payee first.

Other Important Security Information

- Customers are reminded not to log into e-Banking or provide any sensitive personal information through hyperlinks, QR Code or attachments embedded in any third-party websites, mobile Apps, emails, SMS or instant messages. To ensure secure transactions, customers should input directly the website address of the Bank into the browser address bar when logging into Internet Banking or should download mobile application from official App stores to login into mobile banking services.
- Customers should be aware of the obligations in relation to security for e-banking services including observing and following in a timely manner the "Conditions for Services" and the relevant security measures specified from time to time by the Bank for the protection of customers.
- Customers should be responsible to take reasonable steps to ensure the confidentiality and security of any device (for example, personal computers, security devices that generate one-time passwords and smart cards that store digital certificates) or authentication factor(s) (for example, personal password and authentication token) used for accessing e-banking services to prevent fraudulent behavior, including but not limited to:
  - destroy the original printed copy of the password;
  - You are advised to pay attention to the risk that has involved in using biometrics, soft tokens, or device binding as one of the authentication factors of conducting related transactions (such as the authentication factors have been lost, stolen, the information have been compromised or unauthorized used), and to take relevant protective measures to ensure the safety of the device and authentication factors. If you notice any unusual or suspicious transactions related to payment cards or accounts, please notify the bank immediately;

- not to allow anyone else to know or use their authentication factor(s);
- never write down the password on any device for accessing e-banking services or on anything usually kept with or near such device;
- not to write down or record the password without concealing it;
- once discovering any unusual or suspicious transactions/activities in the accounts, please call the Bank's 24-Hour Security Incidents Hotline (852) 2616 6628 to report the abnormalities and to suspend e-banking account function immediately; and
- ensure that the contact information registered with the Bank for receipt of important notifications from the Bank (such as SMS and email notifications for online payments) is valid and up-to-date so that relevant notifications can be sent to customers in a timely manner.

- The customer shall notify the Bank as soon as reasonably practicable where the customer discovers or believes that the authentication factors or devices used to access e-banking services have been compromised, lost or misappropriated, or that unauthorized transactions/activities have been recorded in their accounts.
- Unless a customer acts fraudulently or with gross negligence such as failing to properly safeguard his device or secret code for accessing the e-banking services, he will not be responsible for any direct loss suffered by him as a result of unauthorised transactions conducted through his account. This provision does not apply to any unauthorized transactions through cards as set out in the "Security tips for ATM and ATM Card" hereafter.
- Customers will be liable for all losses if customers have acted fraudulently. Customers may also be held liable for all losses if customers have acted with gross negligence (this may include cases where customers knowingly allow the use by others of their device or authentication factor(s)) or have failed to inform the Bank as soon as reasonably practicable after customers find out or believe that their authentication factor(s) or devices for accessing the e-banking services have been compromised, lost or stolen, or that unauthorised transactions have been conducted

in their accounts. This may apply if customers fail to follow the safeguards set out in this article where such failure has caused the losses.

- Customers are reminded to stay vigilant to anything abnormal when logging into e-banking services (e.g. unusual pop-up screens, unusually slow browser response, multiple requests for password input etc). In case of doubt, please do not follow the instructions of the suspicious web page or input any data. Customers are advised to terminate the operation of e-banking services immediately. Please contact the Bank in case of any enquiry.
- Customers should keep their personal information (including biometric data) secure. The Bank will not enquire customer's personal information, e.g. user name, password, one-time password or other account details by email, SMS, instant messaging or phone.
- Before inputting OTP as the transaction authorization for any transaction, you should verify the details of transaction request carefully, such as transaction type, amount and currency, etc. in order to confirm these are actually referring to the intended transaction. If you have any enquiry, please contact us immediately.
- To safeguard their payment cards, card information and authentication factors, customers should stay vigilant against card frauds and scams, particularly those involving binding of cards to mobile payment services.
- Customers may need to bear the consequences of not properly protecting their physical cards, card information, and authentication factors. In particular, the consequences for ignoring pre-and post-card transaction related messages from the bank.