

16 October 2026

Important Notice: Credit Card Fraud Prevention and Cybersecurity Tips

In light of the recent surge in credit card fraud cases during smartphone pre-sales, and in preparation for the upcoming pre-sales campaign in mid-October, the Bank hereby reminds customers to adhere to the following security guidelines to safeguard your account:

1. Keep Sensitive Credit Card Information Confidential

Please securely store your credit card details. Never disclose your credit card number, expiration date, the 3-digit card verification value (CVV) on the back of the card, or one-time passwords (OTP) with anyone, including individuals claiming to be bank staff or law enforcement officers.

2. Beware of Phishing Websites and Fake SMS Messages

* Do not click any suspicious hyperlink or visit any suspicious website, or enter personal or financial information on unauthorised or suspicious websites.

* The Bank uses the "Registered SMS Sender IDs" with the prefix "#" as follows to send SMS messages to our customers: #CHBank, #CHBANK, #Chong Hing, #ChongHing, #CHB.

Please note that the SMS Sender Registration Scheme is not applicable to: (1) SMS messages of which receiving parties are expected to reply to the senders via phone numbers (2-way SMS). Such messages from the Bank will be sent from the following numbers: (852) 622649931188 or (852) 68224927100; (2) Local users who use mobile services with Single-Card-Multiple Numbers/One-Card-Two Numbers provided by non-Hong Kong operators.

3. Real-time Monitor Transaction Notifications and Regularly Review Credit Card Statements

Ensure that your mobile phone is set to receive SMS notifications. Carefully review each transaction notification upon receipt and regularly check your credit card monthly statements to verify transaction records. If you identify any unauthorised or suspicious transactions, contact the Bank immediately.

4. Adjust "Card-Not-Present" Transaction Limits and Card Usage Controls

You can log in to Mobile Banking or Internet Banking to flexibly set the transaction limits for "Card-Not-Present" transactions based on your daily spending habits. You can also temporarily disable the "Card-Not-Present" transaction function via Mobile Banking/Internet Banking, or suspend your card at any time when it is not in use.

5. Suspect Fraud? Notify the Bank Immediately and Suspend Your Credit Card

If you suspect fraud or notice any unauthorised/unusual transactions, please immediately call our



24-hour hotline at (852) 3768 8811 to inform the Bank, and suspend your credit card via Mobile Banking/Internet Banking or by calling the same hotline to protect your funds.

Special Alert (Beware of "Secondary Scams"): Fraudsters may impersonate banks, merchants, or law enforcement agencies by sending “refund notifications” or “assistance in recovering funds” messages to trick victims into providing sensitive information such as bank account/credit card details, login credentials, or OTPs. Please note: Banks will never send refund messages containing links requesting you to enter personal passwords!

- End -