信用卡/商務扣賬卡保安資訊及提示

為進一步讓　閣下提昇信用卡/商務扣賬卡重要的保安資訊及了解信貸資料之安排，請留意以下提示：

網上交易及網上/流動理財安全防護

- 為加強防範詐騙及欺詐行為，本行將透過手機應用程式採用更安全的生物識別驗證/流動保安編碼方式，用作驗證客戶於指定的線上付款或交易。客戶在透過官方渠道或信譽良好的平台進行網上交易時，須清楚了解商戶有關退款及退貨的政策及細則。
- 不論以任何方式作交易認證，客戶於進行生物認證/流動保安編碼或輸入一次性密碼前，應先仔細核對交易認證提示或短訊之內容，包括商戶名稱、交易金額、交易貨幣等資料，以確保有關資料與將進行之交易內容一致。
- 本行鼓勵客戶以更安全的生物辨識資料方式進行網上交易認證。個人信用卡客戶只需預先下載本行之手機應用程式，登錄流動理財服務及確認卡號已登記於網上理財賬戶後，並啟動推送通知及生物認證設定，以便接收有關信用卡網上交易認證提示及進行交易認證，詳情請瀏覽本行網頁 > 個人理財 > 卡服務 > 查看所有信用卡 > 卡服務 > 生物認證進行網上交易 (ocbc.com.hk/iwov-resources/hk/ocbc/personal/pdf/cards/C47.pdf)。如有關手機應用程式問題，請致電(852) 3199 9188查詢。
- 商務信用卡/扣賬卡客戶持有商業手機應用程式登入權限，啟動推送通知及流動保安編碼認證設定，以便接收有關信用卡網上交易認證提示該交易詳情，並以流動保安編碼進行交易認證。
- 採取適當措施以保護您的裝置 (包括手機、平板電腦及電腦)，以保障與信用卡相關的資料並減低未經授權使用的風險。如裝置遺失或被盜，您應盡快採取行動，例如在可行情況下啟用遙距鎖定或資料清除功能，並儘快通知本行。
- 切勿連接任何不安全或沒有加密之網絡系統及於公用電腦或他人的電子設備輸入信用卡/商務扣賬卡號碼、私人密碼 (PIN)、其他個人資料及登入流動理財服務。
- 切勿在瀏覽器儲存任何信用卡/商務扣賬卡或個人資料，並對以自動填寫功能輸入之資料保持警覺。
- 每次使用網上及流動理財服務後，按照指示登出。

妥善保管卡密碼、認證因素及個人資料

- 收到信用卡/商務扣賬卡後，立即於卡背面簽署。
- 客戶應該將信用卡/商務扣賬卡視作現金般妥善保管，切勿隨意放置或借予任何人。
- 切勿向任何人士透露信用卡/商務扣賬卡號碼、私人密碼 (PIN) /認證因素及其他個人敏感資料，除非您知道這是合法的要求。
- 在記妥私人密碼 (PIN) 後，立即銷毀載有私人密碼 (PIN) 的函件。
- 切勿將私人密碼 (PIN) 寫下記錄或將任何載有私人密碼 (PIN) 的紀錄與信用卡/商務扣賬卡一同存放。
- 避免使用身份證號碼、電話號碼或出生日期等容易猜測的號碼作私人密碼 (PIN)。
- 定期更改私人密碼 (PIN)，並切勿與其他平台共用同一私人密碼 (PIN)。
- 於輸入敏感資料 (包括但不限於卡號碼、私人密碼 (PIN) /認證因素) 前，應時刻保持提高警覺，並留意附近是否有可疑人士窺探以防資料外洩。
- 於完成簽賬交易或自動櫃員機提款後，謹記取回信用卡/商務扣賬卡，並時刻檢查以確保卡片沒有遺失。
- 進行交易前，應核對交易金額是否正確，並保留賬單副本以作日後核對之用。
- 定期仔細查核信用卡/商務扣賬卡月結單及交易通知，確保沒有未經授權之交易。
- 慎防偽冒本行的來電、電郵或短訊等其他通訊，本行不會以電話、電郵或短訊要求客戶提供敏感個人資料。

網絡釣魚及惡意軟件

- 慎防網絡釣魚。於接收到電子郵件或短訊時，應仔細核實發送人之身份，並對來歷不明人士或久未聯絡之朋友的電子郵件、短訊或電話保持警覺，切勿點擊或下載任何可疑的連結、附件或掃瞄二維碼。
- 提防騙徒假冒銀行或其他公司，以中獎通知或積分換領為由，透過電子郵件或短訊要求客戶提供您的個人資料、信用卡/商務扣賬卡號碼及/或一次性密碼的電子郵件或短訊。
- 切勿向任何人士披透露您的認證因素 (例如私人密碼、一次性密碼及/或流動保安編碼等)。
- 切勿瀏覽不安全的網站，避免點擊任何在社交媒體或手機應用程式上的可疑廣告連結或下載任何惡意軟件[1]。
- 本行不會發出含有超連結並要求客戶登入網上理財服務或輸入個人資料的電子郵件或短訊。
- 於電子裝置上安裝防毒軟件及定期更新軟件，以協助辨識有病毒檔案或惡意程式及預防電子裝置被病毒感染。

電話詐騙

- 當收到不明人士、自稱政府官員或自稱電訊公司、公營機構或銀行職員的可疑來電，先確認對方身份，詢問來電者如何取得您的電話號碼及戶口資料，如來電者拒絕透露便應終止對話。
- 騙徒會以欺詐手法 (如訛稱有特別優惠、假冒政府官員、訛稱速遞公司或郵局員工通知您有欠資包裹可取等)，騙取您的個人資料如銀行或信用卡/商務扣賬卡資料以進行交易或轉賬。提高警覺，慎防洩露您的個人資料或信用卡/商務扣賬卡資料給陌生人。

短訊發送人登記制

- 本行已登記參與通訊事務管理局辦公室 (通訊辦) 推出之「短訊發送人登記制」，本行向本地流動服務用戶所發出的短訊均會以「#」號開頭，「已登記的短訊發送人名稱」為 #OCBCHK / #OCBCHK1 / #OCBCHK2 / #OCBCHK3，以協助客戶識別本行發送人之身份，從而防止及打擊騙徒發出的偽冒短訊。

多重保障措施

- 在使用信用卡/商務扣賬卡進行預付服務交易或與商戶簽署直接付款授權協議前，客戶應先留意商戶之營運情況及清楚了解合約內的條款及細則。此類安排通常由持卡人授權商戶直接從持卡人的指定信用卡/商務扣賬卡賬戶中扣款。一經簽訂協議並作出授權後，取消直接付款授權安排的權利通常歸於商戶，客戶可能無法單方面取消有關安排，敬請留意相關風險。
- 如有懷疑涉及任何欺詐個案，盡快通知本行，及聯絡香港警務處反詐騙協調中心「防騙易18222」熱線進行求助。
- 如發現信用卡/商務扣賬卡有異常或可疑交易，立即致電本行的客戶服務熱線 (852) 2543 2223，或透過網上/流動理財服務向本行作出通報。
- 作為持卡人，時刻妥善保管您的信用卡/商務扣賬卡資料及認證因素，因您須對因沒有履行前述責任而導致之一切損失承擔責任。
- 一經發現信用卡/商務扣賬卡賬戶號碼或私人密碼遺失、失竊、未獲授權使用、不正當使用及/或外洩，立即致電本行客戶服務熱線 – 香港 (852) 3199 9000 或澳門 (853) 2838 8144。客戶亦可透過網上/流動理財向本行通報信用卡/商務扣賬卡之遺失或失竊情況。在本行**未接獲**您前述的通知之前，作為持卡人，您須對信用卡/商務扣賬卡賬戶之一切產生的所有未經授權交易款項**承擔全部責任**，不論該等結欠是否因任何未獲授權或不正當使用信用卡/商務扣賬卡、信用卡/商務扣賬卡資料或認證因素所引致。如持卡人並無作出任何欺詐或嚴重疏忽行為，並在發現其信用卡/商務扣賬卡被盜取，或其認證因素或卡資料已遭外洩後，以合理地可行之情況下盡快通知本行，則持卡人**對於未獲授權之交易 (不包括現金透支) 須負責之最高金額將不超過港幣500元**。
- 想了解更多提防詐騙資訊，可瀏覽香港金融管理局官方網頁及/或社交媒體平台相關宣傳影片及資訊了解詳情。
- 如任何個人資料 (包括通訊地址、聯絡電話及電郵地址) 有所更改，立即通知本行作資料更新，確保本行的重要通知 (如網上或大額交易等) 能夠及時向您發送。

以電子形式發送有關信用卡/商務扣賬卡服務之通告

為響應環保及支持綠色生活，本行將以電子形式向客戶發送有關信用卡/商務扣賬卡服務之通告 (此安排並不影響　閣下現有收取電子結單、電子交易通知書及推廣資訊之設定　(如適用))，而有關安排將不會收取額外費用。如欲更改現時接收有關通告方式、請致電本行客戶服務熱線 (852) 2543 2223更改有關設定。

查閱信貸資料之安排 (如適用)

本行或會在未來12個月，就現行之信貸安排 (包括但不限於更改信用額、取消信貸或債務安排計劃之執行) 進行審查，並可能會於有關期間內**多於一次**查閱於信貸資料服務機構內的信貸資料。您亦可直接致電本行客戶服務熱線作有關查詢。

如有任何查詢，歡迎致電本行的客戶服務熱線 (852) 2543 2223。本函之電子版本請瀏覽ocbc.com.hk/iwov-resources/hk/ocbc/personal/pdf/C8.pdf。如本函中英文版之內容有歧義，一概以英文版為準。

華僑銀行 (香港) 有限公司　謹啟
2026年10月

[1] 惡意軟件是指未經用戶同意的情況下，安裝在用戶的電腦或手機上的非法且難以察覺的軟件，其目的可能包括入侵、破壞電腦系統、盜取用戶的個人資料等進行不法行為。

Credit Card/Business Debit Card Security Information and Tips

To provide you with important information regarding credit card/business debit card security, as well as useful tips and details on accessing your credit data arrangement, please refer to the following:

Security Protection for Online Transactions and Internet/Mobile Banking

- To strengthen fraud and scam prevention, the Bank has implemented a more secured biometric authentication/soft token method via its mobile app, to authenticate certain online payments or transactions. Customers are encouraged to purchase through official sales channels or reputable online platforms and fully understand the relevant terms and policies in relation to product refund and return before entering into any transaction.
- Always verify the transaction details shown in push notification or SMS message, including merchant's name, transaction amount, and currency etc., to ensure it is the intended transaction before performing biometric authentication/soft token or entering a One-Time-Password.
- You are encouraged to enhance the security of your online transactions by adopting a more robust biometric authentication method. Personal credit card cardholder can download the Bank's mobile app, log in to the mobile banking service, and ensure that your card is registered in your e-Banking account. Furthermore, enable push notifications and biometric authentication settings within the mobile app. By doing so, you will receive notifications for online credit card transactions and be able to complete the authentication process securely. For details, please visit our Bank's website > Personal Banking > Cards > See all Card Services > Online Transaction with Biometric Authentication Flow cards (ocbc.com.hk/iwov-resources/hk/ocbc/personal/pdf/cards/C47.pdf). Should you have any questions on the mobile app, please contact (852) 3199 9188 for enquiries.
- Business credit card/debit card cardholder with login authority for the Bank's business mobile app and enable push notifications and Soft Token authentication settings. This allows you to receive authentication alerts for online credit card transactions details, and complete transaction authentication using the Soft Token PIN.
- Take appropriate measures to protect your devices (including mobile phones, tablets, and computers) to safeguard card-related information and reduce the risk of unauthorized use. If a device is lost or stolen, you should take prompt action, such as enabling remote locking or data wiping where available, and notify the Bank as soon as practicable.
- Never connect to any unsecured or unencrypted network and do not enter your credit card/ business debit card number, PIN, other personal information and login internet/mobile banking in public computers or other's electronic devices.
- Never save any credit card/business debit card or personal information in web browsers and stay alert to the information entered using auto-fill function.
- Whenever you use online or mobile banking services, please ensure that you follow the proper log-out procedure.

Safeguard Card PIN, Authentication Factors and Personal Information Properly

- Sign on the back of the credit card/business debit card immediately upon receipt.
- Customer should treat their credit card/business debit card as cash and keep it properly at all times and never leave it unattended or lend it to anyone.
- Do not disclose your credit card/business debit card number, PIN, verification code/authentication factor or other personal sensitive data to anyone unless you are certain that the request is legitimate.
- Destroy the PIN mailer after memorizing the PIN.
- Do not write down the PIN or keep any record of it together with your credit card/business debit card.
- Avoid using easily guessable numbers such as your ID card number, telephone number or date of birth etc. as your PIN.
- Change your PIN regularly. Use a PIN which is not used for other platforms.
- Stay alert to people around you when entering sensitive data (including but not limited to card numbers, PINs/authentication factors) to avoid data leakage.
- Always retrieve your credit card/business debit card after purchase or completing ATM transaction and check it regularly to ensure it remains in your possession.
- Verify the transaction amount before payment and keep a copy of your sales slip for the purpose of verification.
- Review your credit card/business debit card monthly statement and transaction notifications to ensure there are no unauthorized transaction.
- Stay alert to fraudulent calls purportedly from the Bank. The Bank will never ask you to provide sensitive personal information via phone call or email or SMS.

Phishing and Malicious Software

- Stay alert to phishing. Verify sender's identity when receiving an email or SMS and be vigilant to the email or SMS from an unknown person or a person who has not contacted for a long time. Do not click the hyperlink or download the attachment or scan the QR code which is suspicious.
- Be vigilant against fraudsters impersonating the Bank or other banks, institutions or companies who, under the pretext of prize notifications or reward points redemptions, request customers to provide personal information, credit card/ business debit card information and/or One-Time-Password via email or SMS.
- Do not disclose your authentication factors (e.g. PIN, One-Time-Password and/or soft token, etc.) to any person.
- Do not visit unsecured websites, click suspicious advertising hyperlinks on social media platforms or mobile apps, or download any Malicious Software[1].
- The Bank will never send you email or SMS with embedded hyperlink for logging to internet banking or entering your personal information.
- Install antivirus software on your devices and update it regularly to detect viruses or malware and prevent virus infections.

Telephone Deception

- When you receive a suspicious incoming call from unknown person or someone claiming to be a government official or a staff member of a telecommunication company, public sector or a bank, please remain vigilant. Verify the caller's identity and ask how he/she obtained your phone number and account information. Terminate the call immediately if the caller refuses to provide a clear explanation.
- Scammers will use various fraudulent tactics (e.g. claiming to have special offer, pretending to be a government official, pretending to be a staff of courier company or Post Office notifying you of an underpaid parcel, etc.) inducing you to disclose your personal sensitive information such as bank or credit card/business debit card information to conduct purchase or fund transfer. Stay alert and avoid disclosing any personal information or credit card/business debit card information to strangers.

SMS Sender Registration Scheme

- The Bank has participated in the "SMS Sender Registration Scheme" which was launched by the Office of the Communications Authority (OFCA). The Bank will send SMS using "Registered SMS Sender IDs" with prefix "#" (i.e. #OCBCHK/ #OCBCHK1/ #OCBCHK2/ #OCBCHK3) to local subscribers of mobile services, in order to assist you in ascertaining the authenticity of sender, thereby combatting scams.

Multiple Precautionary Measures

- Before conducting a prepaid service transaction or signing a direct payment authorization agreement using a credit card/business debit card with a merchant, you should pay attention to the merchant's operational situation and clearly understand the contract details. Such arrangements typically involve the cardholder authorizing the merchant to directly withdraw funds from the cardholder's designated credit card/business debit card account. Once you sign the agreement and authorize the merchant, the right to cancel the direct payment authorization arrangement usually belongs to the merchant, and you may not be able to cancel it unilaterally.
- If there are any suspicious scams, inform the Bank immediately and contact the Anti-Deception Coordination Centre (ADCC) of the Hong Kong Police Force through the "Anti-Scam Helpline 18222" hotline.
- If you have discovered any unusual or suspicious transactions on your card, please contact our Customer Service Hotline on (852) 2543 2223 or report to the Bank via your internet/mobile banking immediately.
- As a cardholder, keep the credit card/business debit card, the credit card/business debit card information and the authentication factor at all times under your own control. You are fully responsible for all losses resulting from your failure to do so.
- Please notify the Bank on (852) 3199 9000 (Hong Kong) or (853) 2838 8144 (Macau) immediately upon discovery of the loss, theft, unauthorized use, misuse and/or disclosure of the credit card/business debit card, the credit card/business debit card information or the authentication factor. You may also report the loss or theft of credit card/business debit card to the Bank via your internet/mobile banking. As a cardholder, you are **fully liable** for all amounts that the Bank debit to your credit card/business debit card account whether due to the unauthorized use or misuse of your credit card/business debit card, the card information or the authentication factor **before the Bank receives the aforesaid notification**. Provided that the cardholder has not acted fraudulently, with gross negligence or has not otherwise failed to inform the Bank as soon as reasonably practicable after having found that their card/authentication factor has been lost or stolen, or their authentication factor or card information has been disclosed, the cardholder's **maximum liability for unauthorized transactions (other than cash advances) is HK$500**.
- To learn more anti-fraud and prevention tips, please visit Hong Kong Monetary Authority's website and/or social media to watch the relevant videos.
- Inform the Bank immediately of any changes or updates to your personal particulars (including correspondence address, contact number and email address) to allow the important notifications (such as online or large amount transactions, etc.) from the Bank to be delivered to you timely.

Sending Credit Card/Business Debit Card Service Notice in Electronic Format

In addition, to protect the environment, the Bank will send notices relating to credit card/ business debit card service to customers in electronic format (it does not affect your existing settings for receiving eStatement, eAdvice and promotional message (if applicable)) and no additional fees and charges will be imposed on this arrangement. If you would like to change the existing receiving format of the relevant notice, please contact our Customer Service Hotline on (852) 2543 2223 to update the relevant setting.

Access to Credit Data (If Applicable)

During the next 12 months, the Bank may access your consumer credit data held by the credit reference agency(ies) **more than one time** for the purpose of reviewing your existing consumer credit facilities (including but not limited to credit line adjustment, cancellation of credit or implementation of a scheme of arrangement). You may also check the relevant details by calling our Customer Service Hotline.

For any enquiries, please contact our Customer Service Hotline on (852) 2543 2223. For electronic version of this notice, please visit ocbc.com.hk/iwov-resources/hk/ocbc/personal/pdf/C8.pdf. If there is any inconsistency or conflict between the English and Chinese versions of this notice, the English version shall prevail.

OCBC Bank (Hong Kong) Limited
October 2026

[1] Malicious Software refers to an illegal and imperceptible software installed on user's computer or mobile without user's consent. Thereby, it will be invading and destroying the computer system, stealing the user's personal information, and committing illegal acts.