信用卡/扣賬卡保安資訊及提示

感謝　閣下對華僑銀行(澳門)股份有限公司(“本行”)信用卡/扣賬卡的支持。為進一步讓　閣下了解信用卡/扣賬卡保安資訊提示及信貸資料之安排，請留意以下各點：

網絡釣魚及惡意軟件

- 慎防網絡釣魚。接收到電子郵件或短訊時，檢查發送人之身份，對不明人士或已長期沒有聯絡的朋友的電子郵件或短訊保持警覺，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通知您中獎或有積分換領，要求您提供您的個人資料、信用卡/扣賬卡資料及/或一次性密碼的電子郵件或短訊。
- 切勿向任何人透露您的一次性密碼。
- 切勿瀏覽不安全的網站、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要求您登入網上理財或輸入個人資料的電子郵件或短訊。
- 安裝防毒軟件及定期更新軟件，以辨識病毒檔案及預防電腦被病毒感染。

網上交易及網上/流動理財

- 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。只需預先下載本行之個人銀行流動理財程式，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 > 個人銀行服務 > 數碼理財用戶指南
  有關流動理財手機應用程式問題，請致電(853) 2832 2222查詢。
- 請瀏覽本行網頁 > 個人銀行服務 > 表格下載 > 電子銀行服務 > 使用生物認證服務之條款及細則，以了解採用生物特徵作為進行相關交易的認證因素之一所涉及的風險，以及確保裝置和認證因素安全的相關保護措施。
- 不論以任何方式作交易認證，於進行生物認證或輸入一次性密碼前，先仔細檢查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，以確保與將進行之交易內容一致。
- 透過官方渠道或信譽良好的平台進行網上購物，並於進行交易前清楚了解有關退款及退貨的政策及細則。
- 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/扣賬卡號碼、密碼、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/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，請按指示登出。

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，請先確認對方身份，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款包裹可取等)，騙取您的個人資料如銀行或信用卡/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/扣賬卡資料給陌生人。

日常注意

- 收到信用卡/扣賬卡後立即於背面簽署。
- 您應該將信用卡/扣賬卡視作現金，並妥善保管，切勿隨意擺放或借給任何人。
- 切勿向任何人士透露您的信用卡/扣賬卡號碼、密碼、驗證碼及其他個人敏感資料，除非您知道這是合法的要求。
- 在緊記密碼後，請將密碼函件銷毀。
- 切勿將密碼寫下或將密碼的任何紀錄與信用卡/扣賬卡存放在一起。
- 避免以身份證號碼、電話號碼或出生日期等容易猜測的號碼作密碼。
- 定期更改密碼，切勿與其他平台共用同一密碼。
- 輸入敏感資料前應提高警覺，留意附近是否有可疑人士窺探以防資料外洩。
- 簽賬後或完成自動櫃員機交易後，緊記取回信用卡/扣賬卡，並定期檢查以確保沒有遺失。
- 支付前，核對交易金額，並保留賬單副本以便核對。
- 仔細查核信用卡/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，本行不會以電話或電郵要求客戶提供敏感個人資料。

保障自己

- 在以信用卡/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，應先留意商戶之營運情況及清楚了解合約細則。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/扣賬卡帳戶扣款。一旦您簽訂協議並授權商戶後，取消直接付款授權安排的權利通常屬於商戶，您可能無法單方面取消。
- 如有懷疑騙案，請盡快通知本行，及聯絡澳門司法警察局防詐騙查詢熱線(853) 8800 7777。
- 如發現信用卡/扣賬卡有異常或可疑交易，請立即致電我們的客戶服務熱線(853) 2838 8144，或透過網上/流動理財通報本行。
- 作為持卡人，請時刻妥善保管您的信用卡/扣賬卡、信用卡/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/扣賬卡、信用卡/扣賬卡資料或認證因素遺失、失竊、未獲授權使用、不正當使用及/或外洩，請您立即致電本行的熱線 - 澳門(853) 2838 8144或香港(852) 3199 9000通知本行。您亦可透過網上/流動理財向本行通報信用卡/扣賬卡之遺失或失竊。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/扣賬卡賬戶之一切結欠**負全責**，不論該等結欠是否因任何未獲授權或不正當使用信用卡/扣賬卡、信用卡/扣賬卡資料或認證因素所引致。
- 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，以便本行的重要通知(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/扣賬卡服務之通告

為響應環保支持綠色生活，本行將會以電子形式發送有關信用卡/扣賬卡服務之通告予客戶(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　閣下欲更改現時接收形式收取有關通告，請致電客戶服務熱線(853) 2832 3641更改有關設定。

如有任何查詢，歡迎致電本行的客戶服務熱線(853)2832 3641。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(澳門)股份有限公司　謹啟
2025年7月

[1] 惡意軟件是指未經用戶同意下安裝在用戶的電腦或手機上的非法且難以察覺的軟件，從而入侵、破壞電腦系統、盜取用戶個人資料等進行不法行為。

Credit Card/Debit Card Security Information and Tips

Thank you for your support on OCBC Bank (Macau) Limited ("Bank") Credit Card/Debit Card. To provide more information in relation to credit card/debit card security information and tips and access to credit data arrangement, please refer to the followings:

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 that seem suspicious.
- Be vigilant to phishing email or SMS from fraudsters impersonating bank or other company, claiming that you have won a prize or you have points for redemption, to request your personal information, credit card/debit card information and/or One-Time-Password.
- Do not disclose your One-Time-Password to any person.
- Do not visit unsecured website, click the advertising hyperlink on social media platforms or mobile's apps which is suspicious, 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 and update the application regularly to detect virus and prevent virus infection.

Online Payment and Internet/Mobile Banking

- You are encouraged to enhance the security of your online transactions by adopting a more robust biometric authentication method. Download the Bank's Personal Mobile Banking APP, then log in to the mobile banking service, and ensure that your card is registered in your online banking account. Furthermore, enable push notifications and biometric authentication settings within the APP. By doing so, you will receive credit card online transaction notifications and be able to complete the authentication process securely. For details, please visit our Bank's website > Personal Banking > Digital Banking User Guide. Should you have any questions on the Mobile Banking APP, please contact (853) 2832 2222 for enquiries.
- Please visit our Bank's website > Personal Banking > Forms Download > Electronic Banking Services > Terms and Conditions for the use of the Biometric Authentication Service for understanding the risks associated with the adoption of biometric as one of the authentication factors used for initiating relevant transactions and the relevant protection measures to secure the devices and authentication factors.
- Verify the transaction details 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 or entering a One-Time-Password.
- Always 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 engaging in any transaction.
- Never connect to any unsecured or unencrypted network and do not enter your credit card/debit card number, password, other personal information and login internet banking/mobile banking in public computers or other's electronic devices.
- Never save any credit card/debit card or personal information in web browsers and stay alert to the information inputted by auto-fill function.
- Every time you use online or mobile banking services, please make sure you follow the proper log-out procedure.

Telephone Deception

- When you receive a suspicious incoming call from unknown person or someone claiming to be a government official or a staff of a telecommunication company, public sector or a bank, please confirm the caller identity and ask the caller how he/she has your phone number and account information. Terminate the call if the caller refuses to answer.
- Scammers will use 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/debit card information to conduct purchase or fund transfer. Stay alert and avoid disclosing your personal information or credit card/debit card information to strangers.

Daily Attention

- Sign on the card back once you receive it.
- Treat your credit card/debit card like cash. Keep it safe and never leave it unattended or lend it to anyone.
- Do not disclose your credit card/debit card number, password, verification code or other personal sensitive data to anyone unless you know it is a legitimate request.
- Destroy the PIN mailer after memorizing the PIN.
- Do not write down the PIN or keep any record of the PIN with your credit card/debit card.
- Avoid using numbers that can be easily guessed such as your ID card number, telephone number or date of birth etc. as password.
- Change your password regularly. Use a separate password which is not used for other platforms.
- Stay alert to people snooping around you when entering sensitive data to avoid data leakage.
- Remember to retrieve your credit card/debit card after purchase or completing ATM transaction and check it regularly to ensure it is with you.
- Verify the transaction amount before payment and keep a copy of your sales slip for the purpose of verification.
- Review your credit card/debit card monthly statement and transaction notification to ensure there is no unauthorised transaction.
- Stay alert to fraudulent calls purportedly from the Bank. The Bank never asks you to provide sensitive personal information via phone call or email.

Protect Yourself

- Before conducting a prepaid service transaction or signing a direct payment authorization agreement using a credit card/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/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 is any suspicious scams, please inform the Bank immediately and contact the Anti-Fraud Enquiry Hotline of Judiciary Police at (853) 8800 7777.
- If you have discovered any unusual or suspicious transaction on your card, please contact our Customer Service Hotline immediately at (853) 2838 8144 or report to the Bank via your Internet/Mobile Banking immediately.
- As a cardholder, please keep the credit card/debit card, the credit card/debit card information and the authentication factor at all times under your own control. You are fully responsible for all loses resulting from your failure to do so.
- Please notify the Bank on (853) 2838 8144 (Macau) or (852) 3199 9000 (Hong Kong) immediately upon discovery of the loss, theft, unauthorized use, misuse and/or disclosure of the credit card/debit card, the credit card/debit card information or the authentication factor. You may also report the loss or theft of credit card/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/debit card account whether due to the unauthorized use or misuse of your credit card/debit card, the Card information or the authentication factor **before the Bank receives the aforesaid notification**.
- Inform the Bank immediately for information update if there is any change in 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/Debit Card Service Notice in Electronic Format

In addition, to protect the environment, the Bank will send notices relating to credit card/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 (853) 2832 3641 for updating relevant setting.

For any enquiries, please contact our Customer Service Hotline on (853) 2832 3641.

If there is any inconsistency or conflict between the English and Chinese versions of this notice, the English version shall prevail.

OCBC Bank (Macau) Limited
July 2025

[1] Malicious Software means 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.