客戶重要通知

詞彙定義

1. "本行" – 指澳門商業銀行股份有限公司

2. "本網站" – 指澳門商業銀行互聯網網站(www.bcm.com.mo)

3. "網上服務" – 指【BCM Net 網上銀行服務】、【澳門商業銀行流動銀行服務】、【BCM eCorp 商業網上銀行服務】、【BCM eCorp 商業流動銀行服務】、【網上證券買賣服務】、【流動證券買賣服務】及【BCM 網上結單及賬戶查詢服務】

4. "電子網絡" – 指互聯網 及/或 流動數據網絡

閱覽須知

1. 本網站及網上服務部份資料只提供中文或英文內容。

2. 使用 Microsoft Edge 瀏覽器瀏覽此網站，有更佳的效果。

3. 網頁的效果會因使用不同瀏覽器而有所差異。

4. 用戶需在電腦內安裝 Adobe Acrobat Reader 5.0 或以上閱覽某些需下載的文件或表格。

資料及材料之使用

本網站及網上服務內所包含之資料及材料，不論是由本行或任何其它資料提供者提供，均並非蓄意提供任何專業忠告。本行對所有投資產品及服務並無任何責任或擔保，而此等產品及投資服務亦附帶風險。

免保證

本網站及網上服務之所有資料及材料，不論是否由本行或任何其他資料提供者提供，只供參考之用並不時在未事先通知用戶情況下作出修改。雖然本行會盡力但本行對上述資料及材料之準確性或完整性不予保證。

互聯網通訊

客戶明白到電子網絡可能會因為未能預計的擠塞、開放和公開性質及其他原因，導致電子網絡未必是可靠的通訊媒介，而這些不可靠性是在銀行可控制範圍之外。這些因素可導致交易傳送延誤、錯誤資料傳送、延誤執行指示或執行指示和發出指示時的價位偏差、銀行和客戶在通訊上的誤會和錯誤、傳送缺失、阻礙等。

責任之承擔限制

於任何情況下，本行或其僱員均不對本網站及網上服務之使用或不能使用而引致之任何損失或損毀　　承擔任何責任或賠償；不論該等損失或損毀為直接的、間接的、特別的、意外的或後果性的損失，均不承擔任何責任或賠償。此外，本網站及網上服務所提供的網站超連結服務，旨在為客戶提供利益及方便。本行不曾對該等網站之內容、表達之意見、準確性及其所提供之其他相關網站予以核實
，監控或贊同。

顧客承諾 (a) 本身及促使其授權簽署人及(如適用) 受委人士會確保其個人密碼、保安密碼及用以使用本行網上服務的任何設備，包括但不限於個人電腦及手提裝置之安全和保密。若顧客及其各授權簽署人及 (如適用) 受委人士均秉誠行事及盡力保障其個人密碼、保安密碼及裝置之安全，顧客將不須為任何經互聯網或電子媒介發出之指示而導致的未經授權之交易負責； (b) 當得悉或懷疑有未經授權人士獲知其本身或任何其授權簽署人或 (如適用) 受委人士之個人密碼或有未經授權之交易被執行，或發現或懷疑其個人密碼、保安密碼　及/或　裝置遭洩露、遺失或被盜用時，須在合理可行的最短時間內知會銀行，否則顧客須為任何未經授權交易負責；及 (c) 如顧客或其任何授權簽署人或 (如適用) 受委人士以欺詐手段或嚴重疏忽行事，包括未能妥善地保存其等之個人密碼、保安密碼　及/或　裝置，則須為所有損失負責。

版權

根據版權條例，本網站及網上服務內包含之所有資料及材料均屬本行及其資料提供者所有。任何人士在未經本行同意下，不得拷貝、複製或分發本網站及網上服務內包含之所有資料及材料。

網絡保安

使用網上服務進行網上交易是否安全?

本行的網上服務提供多項網上交易的保安措施，以確保客戶之銀行及賬戶資料得到適當保障：

Transport Layer Security (TLS) 128-元位加密

為確保資料保密，本行的系統採用 TLS 加密技術。客戶和本行之間所有透過電子網絡傳送的資料，會以此技術加密，以保障客戶的賬戶資料安全。當客戶連線時，請留意瀏覽器右下角狀態列所顯示的「安全鎖」標誌。這些標誌及信息是用作提示客戶的網上交易資料已作加密處理。

用戶名稱及密碼及保安密碼認證

為加強網上保安，客戶必需設立「用戶名稱」及定時更改「登入密碼」/「保安密碼認證」。

流動銀行服務保安密碼認證

保安密碼認證可以提供高級別的安全保障功能作身份驗證，只有使用您所設定的保安密碼才可以用於登入澳門商業銀行BCM Net 網上銀行服務 / 澳門商業銀行流動銀行服務 / BCM eCorp 商業網上銀行服務 (只限授權者) / BCM eCorp 商業流動銀行服務 (只限授權者) 及 流動證券買賣服務。您的保安密碼不會被儲存於 BCM 手機應用程式內，亦不會被儲存於任何澳門商業銀行的內部記錄。您亦可以隨時登入澳門商業銀行流動銀行服務及於「保安認證設定」啟動或停用保安密碼認證(啟動保安認證需通過雙重認證)。

流動銀行服務指紋認證(生物認證)

指紋可以提供高級別的安全保障功能作身份驗證，只有儲存在您的流動裝置上的指紋才可以用於登入澳門商業銀行BCM Net 網上銀行服務 / 澳門商業銀行流動銀行服務 / BCM eCorp 商業網上銀行服務 (只限授權者) / BCM eCorp 商業流動銀行服務 (只限授權者) 及 流動證券買賣服務。您的指紋不會被儲存於 BCM 手機應用程式內，亦不會被儲存於任何澳門商業銀行的內部記錄。您亦可以隨時登入澳門商業銀行流動銀行服務及於「保安認證設定」啟動或停用指紋認證(啟動保安認證需通過雙重認證)。

流動銀行服務 Face ID 認 證 (生物認證)

Face ID 認證可以提供高級別的安全保障功能作身份驗證，只有儲存在您的流動裝置上的 Face ID 才可以用於登入澳門商業銀行BCM Net 網上銀行服務 / 澳門商業銀行流動銀行服務 / BCM eCorp 商業網上銀行服務 (只限授權者) / BCM eCorp 商業流動銀行服務 (只限授權者) 及 流動證券買賣服務。因此，您應只儲存您自己的 Face ID於您的流動裝置上而絕不應儲存或容許第三者的 Face ID 儲存在您的流動裝置上。您的 Face ID 不會被儲存於澳門商業銀行手機應用程式內，亦不會被儲存於任何澳門商業銀行的內部記錄。您亦可以隨時登入澳門商業銀行流動銀行服務及於「保安認證設定」啟動或停用 Face ID 認證功能(啟動保安認證需通過雙重認證) 。

請注意Face ID 認證有可能會因某些情況，例如雙胞胎、長相相似的兄弟姊妹或青少年兒童以及您裝置設定中「使用臉部識別需要注視螢幕」的功能被停用，而出現錯誤解鎖。如您仍然希望啟用 Face ID 認證功能，敬請細閱有關條款及細則，及接受相關風險和後果。

流動銀行服務臉部識別認證(生物認證)

臉部識別可以提供高級別的安全保障功能作身份驗證，只有儲存在您的流動裝置上的臉部特徵才可以用於登入澳門商業銀行BCM Net 網上銀行服務 / 澳門商業銀行流動銀行服務 / BCM eCorp 商業網上銀行服務 (只限授權者) / BCM eCorp 商業流動銀行服務 (只限授權者) 及 流動證券買賣服務。因此，您應只儲存您自己的臉部特徵於您的流動裝置上而絕不應儲存或容許第三者的臉部特徵儲存在您的流動裝置上。您的面貌特徵不會被儲存於澳門商業銀行手機應用程式內，亦不會被儲存於任何

澳門商業銀行的內部記錄。您亦可以隨時登入澳門商業銀行流動銀行服務及於「保安認證設定」啟動或停用臉部識別功能(啟動保安認證需通過雙重認證)。
請注意臉部識別有可能會因某些情況，例如雙胞胎、長相相似的兄弟姊妹，而出現錯誤解鎖。如您仍然希望啟用臉部識別功能，敬請細閱有關條款及細則，及接受相關風險和後果。

自動結束

網上服務提供自動結束時間控制，如在十五分鐘內沒有使用任何功能或進行交易，連接網上服務之接駁將會自動終止。

自動暫停服務

基於保安理由，客戶如於過去連續12個月（即1年）或以上未有登入BCM　Net網上銀行服務、澳門商業銀行流動銀行服務、網上證券買賣服務、流動證券買賣服務或BCM網上結單及賬戶查詢服務，有關服務將會被暫停使用。客戶需親臨本行任何一間分行辦理登入密碼重置，以重新啟用服務。

電子證書

本網站的伺服器已安裝電子證書，以確認本行之身份。

澳門商業銀行採取哪些保安措施防止電腦駭客?

網上服務的保安對於銀行及客戶都是其中一個非常關注的問題；雖然網上服務帶來方便及快捷的銀行服務，但如果沒有適當的安全及保護措施，駭客入侵或網上的漏洞便會潛在危機。因此，本行採取多項融合科技與管理的措施以確保本行網絡的高度安全。

打擊電腦駭客的措施

為防止駭客入侵，本行專責網絡保安的同事會監察任何駭客試圖入侵本行監察系統，以確保網絡安全。如果客戶懷疑自己的戶口有非授權的交易指示或涉及保安問題的事件，請立即與本行聯絡。

防火牆

本行的網上系統及伺服器均安裝了雙重知名防火牆，不斷地探測及防止未授權之人仕進入系統。

加密技術

本行系統採用了互聯網認可標準的 128 元位「TLS」加密技術以確保客戶的瀏覽器與本行伺服器之間的傳送得到保密。換句話說，客戶和本行之間所有透過電子網絡進入網上服務而傳送的重要資料，均會以此技術加密，以保障客戶的個人資料安全。

Cookies

網上服務使用 Cookies 存取每次連結的識別碼(Session identifier)，以識別在該連結時用戶的身份。當連結完結時，該 Cookies 便會過期。

安全電郵

一般電郵的安全措施未必能確保安全，但「BCM Net 網上銀行服務」的系統特別設有【聯絡本行】的電郵功能，並引用相關的加密技術，而所有經本行以此功能傳送給客戶的個人或交易資料已採用該系統的保密技術加密。

私人密碼

為加強客戶的私人密碼的保密程度，本行透過適當的條例以防止客戶採用容易被推測的密碼，以防止被人盜用；如不能使用相同的號碼及字母或連續數。本行建議客戶避免使用生日日期、電話號碼或姓名等容易被人盜用的數據作為私人密碼。

登入記錄

為提高客戶的警覺性，當每次登入網上服務時，本行會提供有關客戶於上一次登入網上理財的資料。如客戶發現有任何不符的地方，請立即與本行聯絡。

供客戶匯報實際及/或懷疑保安事故之途徑

如客戶發覺其戶口有任何不尋常活動(例如發現或懷疑其私人密碼或設備遭泄露、遺失或被盜用，又或者其帳戶曾錄得未經授權交易等)，應盡快致電商業理財通 8796 8888 匯報有關事項。

客戶應採取怎樣的保安措施保護自己的密碼安全?

除了本行保安措施之外，閣下亦須不時查閱本行提供的保安建議及採取以下適當步驟以避免閣下之賬戶遭入侵：

有效及妥當運用閣下的密碼

閣下的私人密碼乃為保障客戶使用網上服務及進行交易的安全而設，請勿隨便公開。閣下須採取一切合理步驟以妥善保管閣下的私人密碼，及接駁網上服務所用的任何設備，並確保其安全和保密以防欺詐行為。尤其，閣下必須：

- 請勿向任何人透露閣下的私人密碼 / 保安密碼認證，包括閣下的親友及本行的職員。當客戶收到私人密碼之通知信後，請牢記閣下的私人密碼，然後撕掉通知信，並於首次成功登入後更改閣下的私人密碼。
- 請勿使用容易讓人取得的個人資料作為私人密碼 / 保安密碼認證，包括閣下的生日日期、身份證號碼、電話號碼或類似的數字、或閣下的姓名的可辨認部份。
- 請勿寫下或紀錄密碼/ 保安密碼認證而不加掩藏。

- 請勿使用於其他網站登記使用之用戶號碼或密碼 / 保安密碼認證作為私人密碼或以您的私人密碼接駁其他服務(如接連互聯網或其他網址)。
- 請勿讓他人士使用閣下的私人密碼 / 保安密碼認證。
- 請設定難以猜破及與其他服務不同的密碼/ 保安密碼認證，並定期更新。
- 設定密碼 / 保安密碼認證時同時使用小寫和大寫字母，並使用字母和數字的組合。
- 絕對不可將閣下的密碼 / 保安密碼認證寫在任何使用網上服務平台等所需的裝置上例如：個人電腦及其他流動裝置上，或其他經常與此等裝置放在一起或放在附近的物件上，或隨身物品上，如手袋或銀包。
- 閣下應經常更改網上服務私人密碼 / 保安密碼認證，例如每隔 30 天便將密碼更改一次。
- 當發現或懷疑其他人擅用閣下的私人密碼 及/或 保安密碼認證，請立即通知本行。同時，閣下亦應該立刻更改私人密碼，以防止未經授權人士使用閣下的網上賬戶。
- 小心保管閣下的個人電腦 / 流動裝置，切勿亂放。
- 避免使用瀏覽器的「記住網站密碼」之功能。當瀏覽器提示「是否記住此網站密碼」時，切勿選擇「是」。

切勿隨便透露閣下的密碼及個人資料

- 本行不會透過電郵、電話或任何其他途徑向閣下客戶索取閣下的任何網上理財、電話理財或自動櫃員機服務等的登入資料或個人資料，這包括閣下的用戶名稱、密碼、賬戶號碼、保安密碼認證、身份證或護照號碼、地址及電話等。
- 提防要求索取閣下的密碼 / 保安密碼認證 及/或 其他個人資料的可疑電話，電郵，手機短訊或釣魚網站。
- 除了要在電郵中給予閣下更親切的感覺而顯示閣下名字外，本行不會在電郵中透露上述資料，或要求閣下回覆電郵確認任何私人資料。

保護閣下的電腦

- 於電腦上安裝「個人防火牆」，能探測及防止未獲授權的人仕透過不同的途徑進入閣下的電腦盜取資料或下載有害的程式。若閣下為寬頻用戶，本行更建議閣下儘快向電腦或軟件供應商選取最適合的「個人防火牆」。
- 而安裝「病毒防護軟件」能檢測常見的電腦病毒以防止電腦駭客竊取閣下的賬戶資訊或摧毀閣下的電腦檔案。一般的「病毒防護軟件」都需要定期更新版本，這樣，閣下才可以獲得最先進的保護，以確保自己的資料獲得週全保障。
- 請勿開啟不明及可疑來源的電郵附件，它們可能含有病毒。
- 避免進入可疑網站或從可疑網站下載軟件或檔案。
- 如果有任何不尋常的彈出式視窗 及/或 電腦速度異常緩慢，請立即登出網上服務，並以最新版本的病毒防護軟件掃描電腦。

保護閣下的網上交易

- 應留意登入本網站 及/或 網上服務及過程有否異樣(如出現可疑的彈出視窗、被要求提供額外的個人資料等) 及是否有人窺看密碼。
- 請勿使用共用或公眾電腦登入網上服務，因為閣下不能確保那些電腦內沒有被安裝駭客程式。
- 避免透過公共無線網絡登入網上服務。
- 請勿中途離開閣下的電腦工作間及於每次使用網上服務後，先按「登出」(Logout) 功能以登出該服務，免遭他人盜用閣下的賬戶，請謹記只關閉瀏覽器是不能登出網上服務的。
- 除非閣下仍在使用互聯網，否則應避免在不使用電腦時保持連線狀態，尤其是使用寬頻上網時更應加注意。
- 網上服務的首頁顯示閣下上一次登入服務的日期及時間。閣下應經常檢查該資料。如有任何懷疑，請立即與本行聯絡。
- 請小心核對閣下的交易指示，於確定後，指示便不能更改或推翻。
- 定期查閱戶口結餘及進支紀錄，當發現有懷疑的交易項目，應立即通知本行。
- 及時查閱由銀行發出的手機短訊及通訊，並查核有關交易紀錄。若發現可疑情況，應立即通知銀行。
- 請勿將流動電話的來電及短訊轉駁至其他不明來歷的流動電話號碼或設備。如需到海外旅遊，建議閣下使用相同 SIM 卡及電話接收來電及短訊，避免使用轉駁功能。

注意電郵騙案

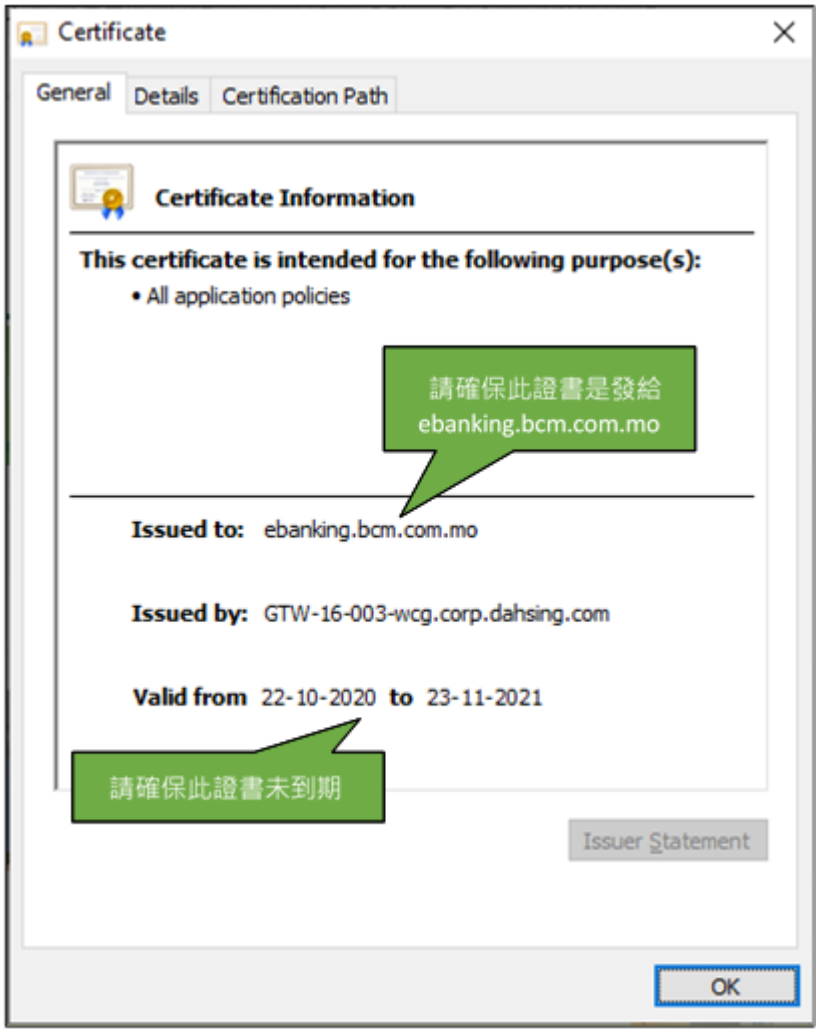
電郵於現今社會是一種普遍的溝通方式，一般會用以聯絡親友以及商業上的伙伴。有些不法分子會利用駭客技術入侵電郵戶口，以各種方法騙取受害人匯款。而有些受害人亦因此受騙，蒙受鉅額金錢損失。閣下需對可疑電郵保持警覺，提高對此類騙案的防範意識，包括匯款前主動以電話、傳真或其他方式確認對方真正身份或該項要求的真確性，以防止此類案件的發生。請閱讀「**客戶應採取怎樣的保安措施保護自己的密碼安全?**」並採取防範措施以預防黑客入侵電腦。

確保閣下所瀏覽的網頁是本行轄下的加密保安網頁

如遇騙徒向金融機構的客戶發出帶有欺詐成份的電子郵件，這些電郵會引導客戶按超連結至偽造網站，藉此要求客戶按入用戶名稱、私人密碼、個人資料及銀行機密資料。為保護閣下的個人及私人資料，切勿於電郵、網上搜尋器、可疑的彈競式視窗或任何其他可疑的渠道中按會直接聯繫到網上服務的超連結，閣下可從瀏覽器直接登入，如果閣下已將www.bcm.com.mo 加入到「我的最愛」，更可從中選擇該連結登入，這能避免被引導至偽造網站。

緊記：由本行所發出的電郵不會有超連結直接指向登入網上服務的網頁。以下的說明可以助您更快辨識索取資料者的真偽，及進一步了解如何保障個人戶口及各種交易的安全。
當輸入用戶名稱及密碼或重要的個人資料前，請檢查螢幕右上角是否有的「安全鎖」的出現🔒。
「安全鎖」🔒代表安全連結，只須按下鎖扣，即可查察安全憑證詳情。

以下是 Microsoft Edge 安全憑證的螢幕顯示範本以供參考：



注意：如閣下按下「安全鎖」後發現任何信息與以上所顯示的不符，請聯絡本行提供資料或協助。

為防止連結到假的網上銀行服務，請避免使用電郵內或其他網站上的連結去直接登入網上銀行服務。

如果閣下發現可疑的銀行網站，請不要輸入任何資料(包括用戶名稱、私人密碼)，並應立即通知銀行。

指定服務之保安措施

使用流動證券買賣服務應注意的事項

客戶須負責採取合理步驟確保安全地使用流動證券買賣服務，包括：

- 閣下必須採取上述一切合理步驟以妥善保管有關服務之私人密碼以登入流動證券買賣服務，並確保其安全和保密以防止欺詐行為。
- 當完成使用流動證券買賣服務後，請即時登出有關之應用程式。
- 請勿開啟不明及可疑來源的短訊或多媒體短訊中的連結，因此類連結可能含有病毒或惡意軟件。
- 安裝任何應用程式前請細閱並評估應用程式的所需權限。

- 不時監察流動通訊裝置的運作環境，停止不必要的應用程式在系統內共同運作。
- 經常登入查詢閣下的戶口結餘，股票持倉，交易指示和交易紀錄。
- 在閣下的流動通訊裝置上只使用由認可供應商提供的獲授權或正式的應用程式。
- 請勿使用 Jailbreak (越獄) 或 Root 機等手法破解閣下的流動通訊裝置，並只使用合法及未經私自修改的作業系統。
- 經常更新閣下的流動通訊裝置的作業系統和應用程式，並應只從官方應用程式商店或可信的來源下載及升級應用程式。
- 適當設定閣下的流動通訊裝置，例如設定不允許安裝來源不明的應用程式。
- 不要將閣下的流動通訊裝置放置在無人看管的地方。
- 啟動流動通訊裝置的自動上鎖功能及解鎖密碼，並應設定難以猜破的密碼。
- 在公眾地方使用閣下的流動通訊裝置時，請以安全的網絡連接互聯網及避免透過公共無線網絡登入流動證券買賣服務。
- 關閉無需使用的無線網絡功能(如 Wi-Fi、藍芽、NFC)。如需使用 Wi-Fi，應選用加密的網絡，並移除不必要的 Wi-Fi 連線設定。

使用澳門商業銀行流動銀行服務應注意的事項

客戶須負責採取合理步驟確保安全地使用澳門商業銀行流動銀行服務，包括：

- 閣下必須採取上述一切合理步驟以妥善保管有關服務之私人密碼以登入澳門商業銀行流動銀行服務，並確保其安全和保密以防止欺詐行為。
- 閣下應為您的流動裝置上唯一的指紋 / Face ID / 臉部識別登記人，以達到保安認證服務的最高安全保障作登入澳門商業銀行流動銀行服務及作驗證網上交易之用。當閣下使用指紋認證 / Face ID 認證 / 臉部識別來作為保安認證，任何儲存在您裝置上的指紋 / Face ID / 面貌特徵均會適用。因此，閣下不應儲存或容許第三者的指紋 / Face ID / 面貌特徵儲存在您的流動裝置上。
- 當完成使用澳門商業銀行流動銀行服務後，請即時登出有關之應用程式。
- 請勿開啟不明及可疑來源的短訊或多媒體短訊中的連結，因此類連結可能含有病毒或惡意軟件。
- 安裝任何應用程式前請細閱並評估應用程式的所需權限。
- 不時監察流動通訊裝置的運作環境，停止不必要的應用程式在系統內共同運作。
- 經常登入查詢閣下的戶口結餘和交易紀錄。
- 在閣下的流動通訊裝置上只使用由認可供應商提供的獲授權或正式的應用程式。
- 請勿使用 Jailbreak (越獄) 或 Root 機等手法破解閣下的流動通訊裝置，並只使用合法及未經私自修改的作業系統。
- 經常更新閣下的流動通訊裝置的作業系統和應用程式，並應只從官方應用程式商店或可信的來源下載及升級應用程式。
- 適當設定閣下的流動通訊裝置，例如設定不允許安裝來源不明的應用程式。
- 不要將閣下的流動通訊裝置放置在無人看管的地方。
- 啟動流動通訊裝置的自動上鎖功能及解鎖密碼，並應設定難以猜破的密碼。

- 在公眾地方使用閣下的流動通訊裝置時，請以安全的網絡連接互聯網及避免透過公共無線網絡登入澳門商業銀行流動銀行服務。
- 關閉無需使用的無線網絡功能(如 Wi-Fi、藍芽、NFC)。如需使用 Wi-Fi，應選用加密的網絡，並移除不必要的 Wi-Fi 連線設定。
- 閣下如遺失或被盜取了已啟動指紋認證 / Face ID 認證 / 臉部識別 / 保安密碼認證的流動裝置，請即致電與我們的客戶服務員聯絡，閣下的澳門商業銀行流動銀行服務的保安認證服務可能會被停用以防止他人盜用。

更新於二零二四年七月