

一般資料概要 – 網上銀行服務

本文檔提供有關使用網上銀行服務（「網上銀行服務」）的一般資料概要，僅供參考。詳情請參閱：

- [戶口及有關服務的條款及條件\(個人戶口\)](#)，
- [網上銀行服務的條款及條件](#)，或
- 銀行網站。

1. 費用及收費

- 與網上銀行服務相關的費用及收費，請參閱[服務收費表（一般銀行服務）](#)。

2. 個人資料保護

- 有關網上銀行服務對客戶個人資料的保障，請參閱[有關個人資料\(私隱\)條例之客戶通告及私隱政策聲明](#)。

3. 客戶的承諾與義務

- 客戶應承諾在使用網上銀行服務(包括但不限於銀行網站、銀行流動應用程式、保安編碼器和流動保安編碼)時遵守[網上銀行服務的條款及條件](#)，以及銀行不時規定的有關網上銀行服務的使用政策及程序。
- 除此之外，客戶承諾：
 - 不會對網上銀行服務、銀行網站、銀行流動應用程式、流動保安編碼或前述所包含的任何軟件的任何部分進行干擾、修改、解讀、反向工程或以其他方式變動或未經授權進入網上銀行服務、銀行網站、銀行流動應用程式、流動保安編碼或前述所包含的任何軟件的任何部分；
 - 不會以在流動裝置或作業系統供應商支持或確保的配置外進行過修改的任何裝置或作業系統（例如，已經被「越獄」或「刷機」的裝置）進入或使用銀行網站、銀行流動應用程式或流動保安編碼。被越獄或刷機的裝置指在未經流動服務提供商及/或電話製造商批准的情況下不再受限於其所設置之限制的裝置。在被越獄或刷機的裝置上使用銀行網站、銀行流動應用程式或流動保安編碼可能會損害安全並導致欺詐性交易；及
 - 僅從官方流動電話應用程式網上商店（例如 Google Play 或 Apple App Store）下載銀行流動應用程式及其更新。
- 如果客戶違反上述承諾，銀行有權終止客戶的網上銀行服務（包括但不限於銀行網站、銀行流動應用程式、保安編碼器和流動保安編碼）而不通知客戶，並就此對客戶採取法律行動。
- 如果客戶未採取本行或客戶電子裝置製造商不時告知或公佈的任何安全措施，客戶須對因使用網上銀行服務而引致或與其相關的所有後果全權負責並承擔所有責任。
- 客戶使用網上銀行服務時一旦遇到任何不正常情況或困難，客戶應儘快通知銀行。

- 客戶向銀行聲明及保證，客戶使用網上銀行服務時將符合一切適用法律、規則及法規，以及網上銀行服務適用的用戶手冊、政策及程序、[網上銀行服務的條款及條件](#)及客戶與本銀行訂立的任何其他協議（可不時予以修訂）。

4. 客戶對未經授權的交易的責任

- 一般而言，如發生未經授權的網上銀行交易，而客戶方面並無嚴重疏忽、欺詐或錯誤（例如客戶未能妥善保管接駁網上銀行服務（包括但不限於銀行網站、銀行流動應用程式、保安編碼器及流動保安編碼）的設備），則客戶將無須負責其所蒙受的任何直接損失。
- 但客戶應明白及確認客戶的信用卡、客戶名稱、私人密碼、流動保安編碼密碼和流動保安編碼（如適用）及/或保安編碼有被未獲授權人士不當使用或被用於未獲批准的用途的風險。如果有下列任何情形，客戶應在合理可行情況下儘快通知銀行：
 - i. 客戶得知或懷疑信用卡、客戶名稱、私人密碼、流動保安編碼密碼（如適用）、保安編碼器（如適用）及/或保安編碼已遺失、被竊、受損害、被洩露給任何未獲授權人士或被任何未獲授權人士取得；
 - ii. 或有人用信用卡、客戶名稱、私人密碼、流動保安編碼密碼（如適用）及/或保安編碼作出任何未獲授權的指示或交易；或
 - iii. 流動保安編碼受到任何損害或未獲授權的使用。
- 若客戶未能在合理可行情況下儘快通知銀行該等事情，或存在欺詐或嚴重疏忽行為，一切由他人使用任何信用卡、客戶名稱、私人密碼、流動保安編碼密碼（如適用）、流動保安編碼（如適用）及/或保安編碼進行的交易及所引致的直接損失，可能需由客戶負責。

客戶重要通知

- 客戶應對其所有作為和不作為負責，並應遵守相關申請表和[網上銀行服務的條款及條件](#)。
- 如有詐欺行為，客戶將須承擔所有損失。
- 如果客戶有重大過失（這可能包括客戶故意允許他人使用其設備或身份驗證資訊的情況），或在發現其用於登入網上銀行服務的身份驗證資訊或設備已被洩露、遺失或被盜，或在發現未經授權的交易後後未能在合理可行的情況下儘快通知銀行，則客戶將須承擔所有損失。
- 若客戶未能遵守下列保障措施，則將需承擔所有損失：
 - i. 客戶有義務採取合理措施確保用於登入的任何電子裝置及網上銀行服務（例如個人電腦、產生一次性密碼的安全設備和儲存數位憑證的智慧卡）或身份驗證資訊（例如密碼和保安編碼）安全且保密。
 - ii. 客戶必須採取合理措施確保其電子裝置安全和其身份驗證資訊保密（例如密碼），以提防詐欺。
 - iii. 除此之外，應提醒客戶：
 - a. 銷毀密碼的原始印刷本；

- b. 採用生物識別憑據、流動保安編碼或裝置綁定作為啟動相關交易（例如非接觸式行動支付）作為身份驗證資訊之一所涉及的風險，以及確保電子裝置和身份驗證資訊安全的相關保護措施；
 - c. 不應允許其他人使用他們的身份驗證資訊；
 - d. 定期更改密碼和流動保安編碼密碼（如適用）；
 - e. 切勿將密碼寫在任何用於存取電子銀行服務的電子裝置上或通常存放着該電子裝置或附近的任何物品上；
 - f. 不得在未經掩飾的情況下寫下或記錄密碼；
 - g. 當他們發現其帳戶出現異常或可疑交易後，應盡快通知銀行；和
 - h. 需要確保他們在銀行註冊的聯絡方式是最新的，以便及時接收銀行的重要通知（例如，用於線上支付的簡訊和電子郵件通知）。
- 如果客戶未採取本行或客戶電子裝置製造商不時告知或公佈的任何安全措施，客戶須對因使用網上銀行服務而引致或與其相關的所有後果全權負責並承擔所有責任。

5. 安全事件報告

- 如果客戶的保安編碼器或與流動保安編碼綁定之流動裝置遺失或被竊，客戶應在合理可行情況下儘快撥打銀行不時規定的電話號碼通知銀行，並在銀行要求時作出書面確認。
- 如客戶未能在合理可行情況下儘快向銀行知會該等事項，或在其他情況下有欺詐或嚴重疏忽的行為，所有涉及任何人士使用其所失之保安編碼器或與流動保安編碼綁定的流動裝置（視乎情況而定）所進行的未經授權交易而引致的直接損失，一律可能需由客戶負責。銀行補發新保安編碼器或流動保安編碼（如適用）時可收取費用。
- 客戶可以透過以下任何一種方式向銀行發出通知：
 - i. 致電銀行於銀行網站或銀行流動應用程式發佈之 24 小時客戶服務熱線 +852 2779 5533;
 - ii. 聯絡銀行任何分行; 或
 - iii. 銀行不時通知的任何其他方法。

若本一般資料概要的英文版本和中文版本之間有任何不一致，則以英文版本為準。