八達通網上服務安全指南

本「八達通網上服務安全指南」旨在為閣下提供安全提示，以及於使用由八達通卡有限公司(「本公司」）的網上及流動服務時須注意的事宜。

1. 當使用由本公司提供的網上服務時：

1.1. 避免使用不可信的流動裝置或公用電腦使用本公司服務。

1.2. 如要進入本公司網站，請在網頁瀏覽器上輸入 http://www.octopus.com.hk。

1.3. 閣下應從本公司網站 http://www.octopus.com.hk 上所示的連結或認可的應用程式商店 – Google Play Store or Apple App Store 下載本公司的流動應用程式。

1.4. 閣下應從認可的應用程式商店下載認可流動支付應用程式以使用 Smart Octopus。

1.5. 當閣下透過網頁瀏覽器使用本公司的網上交易服務時，網頁瀏覽器上會顯示一個「安全鎖」圖像。當閣下點選該「安全鎖」圖像時，網頁瀏覽器會顯示本公司獲發的數碼證書。

1.6. 當使用八達通卡及產品（「八達通」）享用服務時，閣下必須提供八達通號碼（連同括號內的數字）以作核實。閣下可於成功登記閣下的八達通後，使用該已登記八達通進行網上付款及轉賬。

1.7. 請緊記於完成有關服務後關閉或登出(如適用)服務或程式。

1.8. 本公司不會在任何電郵或短訊中顯示閣下的個人資料，或要求閣下回覆電郵或短訊以確認任何個人資料或密碼。

1.9. 當使用八達通網上付款時

1.9.1. 於購物時，網上商戶可能會要求閣下提供姓名、電郵地址、電話號碼、送貨地址等，以履行閣下的訂單。除非另有註明，否則本公司不會獲悉或保存該等資料。

1.9.2. 除閣下要求提供慈善捐款收據外，於閣下使用網上付款服務時，本公司不會收集閣下的個人資料。

1.9.3. 如閣下要求提供慈善捐款收據，閣下可以選擇透過我們向有關慈善機構提供閣下姓名、電郵地址、電話號碼及郵寄地址。

1.9.4. 於確認付款前，先核對付款資料包括收款人、金額及捐款類別／賬單類別（如適用）。

1.10. 當使用八達通 O! ePay（**"O! ePay"**）服務時

1.10.1 請閣下務必透過指定途徑申請 O! ePay 賬戶。

1.10.2 於申請 O! ePay 賬戶時，本公司會要求閣下提供姓名、電郵地址、電話號碼及身份證明文件之圖像等資料。該等資料會以安全的方式保存於本公司的伺服器，以作閣下申請 O! ePay 及客戶服務之用。有關使用閣下個人資料的目的，請參閱八達通發卡條款。

1.10.3 使用 O! ePay 銀行轉賬服務時，八達通將要求閣下提供銀行和銀行帳號等資料，並使用閣下的全名和 O! ePay 帳號作服務操作之用。該等資料會以安全的方式保存於本公司的伺服器，以作閣下申請 O! ePay 及客戶服務之用。有關使用閣下個人資料的目的，請參閱有關八達通「好易畀」服務的銀行轉賬條款及細則。

1.10.4 請不要向任何人透露閣下的賬戶密碼，切勿抄寫記下，閣下應定期更改密碼。此外，閣下應選擇一個別人難以猜測，以字母數字組合的強密碼。

1.10.5 不要向任何人士披露閣下的密碼。本公司絕不會在任何通訊中要求閣下提供密碼。

1.10.6 我們保証只依靠 iOS / Android 來儲存和驗證閣下的生物特徵數據（例如指紋），我們並不記錄或儲存任何閣下的生物特徵數據。

1.10.7 在啟用指紋或 iOS Touch ID 或其他生物特徵數據以登錄 O! ePay 之前，請確保指紋或 iOS Touch ID 或其他生物特徵數據只屬於閣下本人，以防止閣下的 O! ePay 賬戶未經授權地被使用。

1.10.8 請小心查核他人向閣下發送的邀請。當其他用戶邀請閣下成為朋友時，螢幕上會顯示其手機號碼，以便閣下查核後才允許加入。請確保其他用戶為閣下認識及信任的人士，才加入為朋友。

1.10.9 閣下只可在八達通 App 內直接收發付款要求及付款提示等通知。該等通知不會經電郵或短訊發送。閣下可於八達通 App 內 O! ePay 項下交易記錄部分查閱該等付款要求。

1.10.10 於接受付款要求或發送 P2P 付款前，請小心查核付款詳情，包括收款人資料及付款金額。O! ePay 所有付款交易指示一經送出，均不可撤銷。

1.10.11 如閣下的手機號碼或其他個人資料有所更改，請盡快致電八達通顧客服務熱線 2266 2222，以便本公司為閣下更新紀錄。

1.10.12 如閣下更改了電郵地址，請盡快透過八達通 App 更新您的電郵地址以防止錯失任何重要通知。

1.10.13 請小心輸入閣下的手機號碼，以便接收閣下的 O! ePay 賬戶的短信通知提示。

1.10.14 請經常檢查閣下的 O! ePay 賬戶及八達通紀錄。如發現任何問題或可疑情況，請即致電八達通顧客服務熱線 2266 2222 聯絡本公司以便調查。

1.10.15 閣下可於八達通 App 下載 O! ePay 賬戶結單以作保存。

1.11 當使用 Smart Octopus 時：

1.11.1 如要查閱閣下的認可流動支付服務使用者賬戶，請務必透過官方／認可流動支付應用程式或認可流動支付服務供應商網站進入賬戶。

1.11.2 閣下的 Smart Octopus 須配合認可流動支付應用程式使用。

1.11.3 申請 Smart Octopus 時，本公司會要求閣下提供姓名及手機號碼等資料，該等資料會以安全的方式保存於本公司的伺服器，只作辦理退款手續之用。請參閱八達通發卡條款了解更多。

1.11.4 如要透過本公司網站申請 Smart Octopus 退款，閣下將需提供姓名及手機號碼；該手機號碼用於申請退款過程中接收含有驗證碼的 SMS 短訊。

1.11.5 如閣下的手機號碼有所更改，請盡快致電八達通顧客服務熱線 2266 2222 聯絡本公司以便為閣下更新紀錄。

1.11.6 請小心保管閣下認可流動支付應用程式的驗證密碼（如適用），切勿抄寫記下，閣下應定

期更改密碼。閣下應選用一組他人難人猜測，以字母及數字組合而成的強密碼。

1.11.7 如閣下使用的流動裝置支援虹膜或指紋驗證，閣下可以選擇以此授權進行網上交易，或其他 Smart Octopus 功能。請注意，八達通只依靠閣下認可流動支付服務供應商存儲和驗證閣下的虹膜／指紋資料，八達通不會記錄或儲存任何該等資料。

1.11.8 使用虹膜／指紋驗證前，請確保該驗證只屬於 Smart Octopus 持有人，以防止任何未經授權使用閣下的 Smart Octopus。

1.11.9 請定期查閱閣下登記 Smart Octopus 的交易紀錄。如有任何問題或發現任何可疑活動，請即致電八達通顧客服務熱線 2266 2222 與我們聯絡。

2. 本公司為閣下作出的保障措施

2.1. 本公司的伺服器及網絡基礎設施均受防火牆保護，以防止未經授權的存取。

2.2. 本公司伺服器與閣下的裝置及八達通之間進行的所有通訊，一概已採用業界標準技術加密處理。

2.3. 如交易未能於既定時間內完成，將會被自動取消。

2.4. 本公司的系統會記錄每一張八達通使用網上服務的情況，如五次輸入不相符的八達通號碼，該八達通之網上功能將會被暫停 24 小時。

2.5. 為確保安全進行交易，本公司所提供的流動應用程式會偵測閣下的流動裝置是否已獲得「Root」權限或已「越獄」(jail-broken)。本公司於偵測閣下流動裝置的狀況時，不會存取機上其他資料。

2.6. 八達通網上付款

2.6.1. 於付款前，八達通 App 或網站會顯示商戶資料及交易金額，以供閣下核實。

2.6.2. 當透過八達通 PC 閱卡機使用網上付款服務時

(i) 本服務透過 https 網站提供。請確保當閣下使用網上付款服務時，網頁瀏覽器上有顯示「安全鎖」。當閣下查看數碼證書時，螢幕會顯示「Octopus Cards Ltd」(即本公司）為擁有人。

(ii) 使用八達通網上付款服務時，資料會經 SSL 加密處理。閣下輸入的資料會在網際網路傳送時自行加密，除了我們或擁有鑰匙的授權者外，沒有其他人可以讀取。以保障閣下的私隱，八達通網上付款使用 128 位元加密技術，為現時業界通用的網上傳送資料保安標準。

(iii) 本公司只會透過 https://www.online-octopus.com 提供八達通網上付款服務。

2.7. **O! ePay 服務**

2.7.1. 每次可以使用兩部已登記的裝置登入閣下的 O! ePay 賬戶。

2.7.2. 當閣下使用 O! ePay 時，螢幕會顯示上次的登入時間及狀況。如發現任何可疑情況，請聯絡本公司。

2.7.3. 於閣下使用此服務期間，如閒置逾時，系統會自動登出。

2.7.4. 如閣下聯絡本公司查詢閣下賬戶的運作，將須提供核實編碼或個人資料以便核

實身份以保障閣下的賬戶資料。

2.7.5. 當閣下以新的流動裝置登入賬戶或增加閣下的每日交易限額時，系統會透過短訊向閣下的登記手機號碼發送驗證碼。該短訊會顯示驗證碼及該交易之目的。請於八達通 App 輸入驗證碼前查閱短訊之內容。如閣下收到有關此服務的可疑短訊，請即致電八達通顧客服務熱線 2266 2222 聯絡本公司以便調查。

2.7.6. 若閣下已向流動網絡服務商申請短訊轉送服務，該短訊將不會被轉送。請緊記切勿將驗證碼短訊轉送至其他流動裝置。

2.7.7. 如多次未能成功登入，閣下的賬戶將會被暫停。如發現閣下的賬戶被封鎖，請致電八達通顧客服務熱線 2266 2222。

2.7.8. 我們將透過推送訊息/電子郵件提供閣下的帳戶活動更新。 對於重要的交易，如設備註冊/取消註冊，以及加入收款人/朋友時，閣下會透過電郵及/或推送訊息收到賬戶動態更新通知。請緊記查閱該等電郵/訊息以核對你的交易紀錄。如發現任何差異，請即致電八達通顧客服務熱線 2266 2222。

2.7.9. 加入新朋友或登記八達通至 O! ePay 賬戶時，閣下會透過電郵收到每日之摘要。請緊記查閱該等電郵/訊息以核對閣下的交易紀錄。如發現任何差異，請即致電八達通顧客服務熱線 2266 2222。

2.7.10. 我們絕對不會透過電子郵件或通過嵌入在電子郵件中之超連結要求客戶核實個人及/或賬戶資料（如身份證號碼或登入密碼等）。

2.8. Smart Octopus

2.8.1. 每個認可流動支付服務使用者賬戶只可使用一張 Smart Octopus。

2.8.2. 與其他自動增值服務客戶相同，Smart Octopus 持有人可享有報失服務，以及於指定渠道申請退款。

2.8.3. 如閣下可於申請 Smart Octopus 時向本公司提供用以辦理 Smart Octopus 退款的姓名及手機號碼資料。在申請退款時，閣下的手機號碼將收到一組驗證碼作核實身份之用。

2.8.4. 如閣下聯絡本公司查詢閣下 Smart Octopus 的運作，將須提供 Smart Octopus 號碼及個人資料以便核實身分，以保障閣下的賬戶資料。

2.8.5. 如閣下轉移 Smart Octopus 至新的流動裝置，用以登記的電郵賬戶將收到一封電子郵件，在轉移 Smart Octopus 前，閣下將需要透過新流動裝置登入你的認可流動支付服務使用者帳戶。

2.8.6. 每次交易完成後，閣下將收到推播通知訊息及有關交易資料。透過認可流動支付應用程式，Smart Octopus 查詢頁面最多可顯示 40 項交易紀錄。請定期查閱交易紀錄。

2.8.7. 如閣下已向流動網絡服務商申請短訊轉駁服務，不論服務設定，申請退款時所接收到的驗證碼都不會被轉駁。為閣下安全起見，請勿將驗證碼短訊轉送至其他流動裝置。

2.8.8. 本公司絕不會透過電子郵件或通過嵌入在電子郵件或短訊中的超連結要求客戶核實個人及／或賬戶相關資料（如登記電郵或登入密碼）。

3. 閣下應作出的保障措施

3.1. 小心保管閣下的八達通，以保障八達通不會被擅自登記以作網上付款。

3.2. 請小心保管閣下的流動裝置。

如閣下的流動裝置無人看管，或會在閣下不知情下遭他人盜取，讀取機上儲存的資料及使用閣下機上的 Smart Octopus。

3.3. 請使用屏幕鎖功能以避免閣下的個人資料（如訊息、瀏覽紀錄、聯絡人名單）被他人讀取。

3.4. 使用遙距定位及遙距清除功能，讓閣下在遺失裝置時，追尋裝置所在位置或清除機上的資料。

3.5. 切勿點擊任何附有直接付款交易連結的電郵或短訊。

3.6. 當使用流動裝置作網上服務時，請特別小心有關裝置未必能提供與個人電腦同樣的安全配置。

3.7. 於設定密碼時，請留意：

- 避免將密碼設定為其他服務正在使用的密碼。
- 切勿使用容易記憶的個人資料（如聯絡電話、出生日期、香港身份證號碼、車牌號碼）作為閣下密碼的一部分。
- 請使用由大階及小階英文字母與數字組合而成的密碼，使他人難以猜中。
- 切勿抄寫記下，或使用電腦或流動裝置儲存密碼。如真的有需要記下密碼，請以秘語或錯亂次序記下。請定期更改密碼。

3.8. 在使用 O! ePay 時，請小心任何異常的登入程序，可疑的彈出視窗，或被要求提供額外的個人資料。在使用閣下的 O! ePay 賬戶後請立即登出服務。

3.9. 作為預防性的保安措施，閣下的八達通必須已登記，才可進行網上付款及查詢事宜。如希望加強保障，閣下可考慮使用具遮蔽功能的卡套，以防閣下的八達通被盜用。

3.10. 作為預防性的保安措施，閣下的 Smart Octopus 必須已登記，才可進行網上付款或與 O! ePay 賬戶進行轉賬。

3.11. 一般情況下，作為預防性的保安措施，當完成使用任何無線網絡功能（例如 Wi-Fi，藍牙或 NFC 近場通訊）後，閣下可考慮將其關閉。

3.12. 檢查閣下的八達通交易紀錄。如閣下發現任何可疑交易，請立即致電八達通顧客服務熱線 2266 2222 作跟進調查。

3.13. 請使用正版軟件

使用正版軟件可以減低閣下的軟件受電腦病毒或間諜軟件影響或入侵的機會。

3.14. 不要「越獄」（jail-break），獲得「Root」權限或更改作業系統

此等行動會減低作業系統的穩定性，及增加電腦或流動裝置感染病毒、間諜軟件的機會，以致損害或洩漏閣下的個人資料。如閣下使用「越獄」或獲得「Root」權限的流動裝置，本公司或未能提供閣下所要求的服務。不要使用盜版或不明來歷的軟件，

因其可能包含了間諜軟件、電腦病毒或其他不包含在原始軟件包的改動或修改，可能會增加閣下流動裝置感染病毒、間諜軟件或其他惡意軟件的機會，增加閣下的裝置受損壞或個人資料洩漏的風險。

3.15. 定時更新閣下的作業系統和網頁瀏覽器，可盡量提高流動裝置軟件之安全性。使用最新版本的流動應用程式。下載並安裝安全修補程式到流動裝置以防範已知的安全漏洞。

3.16. 使用並定期更新防毒軟件可以保護閣下的流動裝置免受不同來源的電腦病毒入侵。請定期更新「病毒定義檔」以有效地保護閣下的流動裝置。有關詳情，請參閱有關軟件的「幫助」部分。

3.17. 使用並定期更新反間諜程式軟件可阻止惡意軟件或間諜軟件安裝在閣下的流動裝置上，以防止任何跟踪閣下流動裝置使用行為的情況。部分反間諜程式軟件更可偵測及攔截釣魚網站，幫助閣下區分官方網站及冒充的複製網站。

3.18. 使用並定期更新防火牆軟件。這軟件可能已包括在閣下的作業系統內，閣下亦可從第三方供應商獲得。閣下的防火牆軟件需要定期更新，以保護閣下的電腦或流動裝置免受網絡攻擊。

3.19. 由於無線網絡技術建基於無線電信號，有機會讓他人於未獲授權的情況下近距進入閣下的網絡。如閣下使用個人的無線路由器，這能支援使用密碼或加密數據傳輸。

3.20. 提防虛假／釣魚電郵

閣下或會收到假冒由本公司發送的電郵。該等電郵會企圖欺騙閣下提供個人資料。請注意，本公司絕對不會透過電郵或其中所載連結，要求閣下提供個人資料或密碼。緊記切勿打開、回覆或點擊該等電郵。

3.21. 拒收垃圾郵件

垃圾郵件可能會包括接連到欺詐網站的連結。該等郵件會偽裝由閣下曾接觸的公司發出，企圖取得閣下的信任，以套取閣下的資料。處理垃圾郵件時，請格外小心。閣下應長期開啟電郵軟件中的拒收或過濾垃圾郵件功能，或使用網上電郵服務供應商提供的有關功能。

3.22. 提防外觀相似的網站

欺詐者及騙徒或會設置與閣下信任的網站相似的網頁，並要求閣下輸入個人資料。請仔細檢查網站域名或地址，以確保閣下瀏覽的網站真正是閣下所信任公司的官方網站。

3.23. 使用儲值支付工具的「智醒錦囊」

有關金管局提供的「智醒錦囊」及教育影片，請參閱這連結。