八達通網上服務安全指南

本文件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」、「我們」）的網上及流動服務時所須注意的事宜。閣下可以閱讀有興趣了解的資訊內容：

目錄

本公司或會要求閣下提供個人資料，以作客戶服務或營運用途。如閣下想了解有關個人資料的收集目的和使用詳情，請參閱八達通發卡條款。如閣下在使用我們的服務時有任何疑問或發現任何可疑活動，請即致電八達通顧客服務熱線 2266 2222。請注意，本公司人員絕不會要求閣下提供密碼。

1. 關於使用本公司提供的線上服務

1.1. 進入本公司的網上服務

- 閣下應使用可靠的流動裝置。切勿以公用電腦使用本公司服務。
- 如要進入本公司網站，請在網頁瀏覽器上輸入http://www.octopus.com.hk。
- 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（例如 Google Play Store或Apple App Store）下載本公司的流動應用程式。
- 如要使用Smart Octopus，應從認可的應用程式商店下載認可的流動支付應用程式。
- 當閣下透過網頁瀏覽器使用本公司的網上交易服務時，網頁瀏覽器上應顯示出「安全鎖」圖像。當閣下點選該「安全鎖」圖像時，網頁瀏覽器應顯示出本公司獲發的數碼證書。
- 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。
- 請緊記於完成有關服務後關閉或登出（如適用）服務或程式。
- 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。如發現任何可疑活動，請即致電顧客服務熱線2266 2222。

1.2 使用八達通網上付款

- 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、送貨地址等個人資料，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。
- 除非閣下要求提供慈善捐款收據，否則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。
- 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的姓名、電郵地址、電話號碼及郵寄地址。
- 於確認付款前，請先清楚核對付款資料，包括收款人、金額及捐款類別 / 賬單類別（如適用）。

1.3 使用八達通O! ePay（「O! ePay」）服務

- 請閣下務必透過可靠的指定途徑申請O! ePay賬戶。
- 當閣下申請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。
- 使用O! ePay銀行轉賬服務時，八達通將要求閣下提供銀行名稱和銀行賬號等資料，並使用閣下的全名和O! ePay賬號作服務操作之用。
- 該等資料將以安全的方式保存於本公司的伺服器，以作服務操作之用。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。
- 請小心保管閣下的賬戶密碼，切勿向他人透露或抄寫記下，並應定期更改密碼。此外，閣下應選擇一個別人難以猜中，以字母及數字組合而成的強密碼。本公司人員絕不會要求閣下提供密碼。
- 本公司只依靠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。
- 在啟用指紋、iOS Face ID或其他生物特徵數據以登錄O! ePay之前，請確保有關生物特徵數據全屬於閣下本人，以防止閣下的O! ePay賬戶被未經授權使用。
- 請小心查證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，以便閣下查證後才允許加入。請確保其他用戶為閣下認識及信任的人士，才加入為朋友。
- 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」部分查閱該等付款要求。
- 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。所有O! ePay付款交易指示一經送出，均不可撤銷。
- 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，以確保閣下的聯絡資料為最新資料。
- 如閣下已更改電郵地址，請盡快透過八達通App更新電郵地址，以避免錯失任何重要通知。
- 請確保閣下的手機號碼輸入正確，以便接收閣下O! ePay賬戶的短信通知。
- 閣下可於八達通App下載O! ePay賬戶結單以作保存。
- 請定期查閱閣下的O! ePay賬戶及八達通交易紀錄。如有任何疑問或發現任何可疑活動，請即致電八達通顧客服務熱線2266 2222。

1.4 使用Smart Octopus

- 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。
- 閣下的Smart Octopus須配合認可流動支付應用程式使用。
- 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，並只作辦理退款手續之用。詳情請參閱八達通發卡條款。
- 如要透過本公司網站申請Smart Octopus退款，閣下必須提供姓名及手機號碼。該手機號碼將於申請退款過程中用以接收驗證碼短訊。
- 如閣下的手機號碼有所更改，請盡快透過認可流動支付應用程式更新紀錄，以確保閣下申請Smart Octopus退款所需的均為最新資料。
- 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，並應定期更改密碼。閣下應選用一組他人難以猜中，以字母及數字組合而成的強密碼。本公司人員絕不會要求閣下提供密碼。
- 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儲存和驗證閣下的虹膜 / 指紋資料，八達通不會記錄或儲存任何該等資料。
- 使用虹膜 / 指紋驗證前，請確保該驗證全屬於閣下所有，以防止任何未經授權使用閣下的Smart Octopus。
- 請定期查閱閣下的Smart Octopus交易紀錄。如有任何疑問或發現任何可疑活動，請即致電八達通顧客服務熱線2266 2222。

2. 本公司為閣下提供的保障措施

- 本公司的伺服器及網絡基礎設施均受防火牆及入侵防禦 / 偵測系統保護，以防止未經授權的存取。
- 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。
- 如交易未能於指定時間內完成，將被自動取消。
- 本公司的系統會記錄每一張八達通使用網上服務的情況，如八達通App記錄有五次輸入無效或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。
- 為確保交易安全進行，如本公司偵測到閣下的流動裝置已獲得「Root」權限或已

「越獄」（ jail-broken），本公司或會封鎖閣下的存取權。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。

2.1 八達通網上付款

- 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。
- 當透過八達通PC閱卡機使用網上付款服務時：
  i. 本服務將透過https網站提供。當閣下使用八達通網上付款服務時，請確保網頁瀏覽器上有顯示「安全鎖」圖像。當閣下查看數碼證書時，網頁瀏覽器應會顯示「Octopus Cards Ltd」（即本公司）為擁有人。
  ii. 使用八達通網上付款服務時，資料會經傳輸層安全（TLS）機制加密處理。閣下輸入的資料會在網絡傳送時自行加密，除了我們或擁有鑰匙的授權者外，他人無法讀取。為保障閣下的私隱，八達通網上付款服務使用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。

2.2. O! ePay服務

- 閣下每次可以使用最多兩部已登記的裝置登入閣下的O! ePay賬戶。
- 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，請即致電八達通顧客服務熱線2266 2222聯絡本公司跟進。
- 閣下使用此服務期間，如閒置逾時，系統會自動登出。
- 為保障閣下的賬戶資料，如閣下聯絡本公司查詢閣下O! ePay賬戶的運作，將須提供核實編碼或個人資料以核實身份。
- 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聯絡本公司跟進。
- 請注意，即使閣下或流動網絡服務商已為裝置設定短訊轉送服務，該驗證碼短訊亦不會被轉送。請緊記，切勿將驗證碼短訊轉送至其他流動裝置。
- 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。
- 我們將透過推送訊息 / 電子郵件通知閣下有關賬戶的動態更新。如有重要的活動，例如裝置登記 / 取消登記，以及加入收款人 / 朋友時，閣下會透過推送訊息及其

他渠道（例如已登記電郵）收到賬戶動態更新通知。

- 每當加入新朋友或登記八達通至O! ePay賬戶時，閣下會透過已登記電郵收到每日摘要。
- 我們絕對不會透過電子郵件或其中所載的超連結，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）。
- 請定期查閱更新及通知以核對閣下的交易紀錄。如發現任何異常，請即致電八達通顧客服務熱線2266 2222。

2.3. Smart Octopus

- 每個認可流動支付服務使用者賬戶只限使用一張Smart Octopus。
- 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，並可於指定渠道申請退款。
- 申請Smart Octopus時，閣下可選擇向本公司提供用以辦理Smart Octopus退款的姓名及手機號碼資料（有關姓名及流動電話號碼可於隨後不時更新）。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。
- 為保障閣下的賬戶資料，如閣下聯絡本公司查詢閣下Smart Octopus的運作，將須提供Smart Octopus號碼及個人資料以核實身份。
- 如閣下轉移Smart Octopus至新的流動裝置，已登記的電郵賬戶將收到一封電郵通知。在轉移Smart Octopus前，閣下須以新的流動裝置登入閣下的認可流動支付服務使用者賬戶。
- 每次交易完成後，閣下將收到推送通知及交易資料。閣下可透過認可流動支付應用程式，於Smart Octopus查詢頁面查閱最多40項交易紀錄。請定期查閱交易紀錄。
- 請注意，即使閣下或流動網絡服務商已為裝置設定短訊轉送服務，該驗證碼短訊亦不會被轉送。請緊記，切勿將驗證碼短訊轉送至其他流動裝置。
- 本公司絕對不會透過電子郵件或通過電子郵件或短訊中所載的超連結，要求客戶核實個人及 / 或賬戶相關資料（例如登記電郵或登入密碼）。

3. 閣下應採取的保障措施

- 閣下任何時候均應小心保管個人財物。如八達通無人看顧，或會被他人擅自登記以作網上付款。如裝有Smart Octopus的流動裝置無人看顧，或會在閣下不知情下遭他人盜用機上的Smart Octopus，甚或讀取機上儲存的資料。
- 請保持使用鎖屏功能以避免閣下的個人資料（如訊息、瀏覽紀錄及聯絡人名單等）被他人讀取。
- 如裝置具備「遙距定位」及「遙距清除」功能，請啟用此等功能。萬一閣下遺失裝置，亦可以追尋裝置所在位置，避免遺失個人資料。
- 如電郵或短訊附有要求閣下付款的交易連結，請保持警惕，切勿隨便開啟。本公司不會在電郵或短訊中嵌入此類連結。
- 當透過流動裝置使用網上服務時，請小心留意是否已有適當的安全配置。閣下的流動裝置未必能提供與個人電腦相同的安全配置。
- 當設定密碼時：
  - 應避免於多項不同服務上使用同一個密碼。
  - 切勿使用個人資料（如聯絡電話、出生日期、香港身份證號碼、證件號碼）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，令他人難以猜中。
  - 切勿抄寫記下，或使用電腦或流動裝置儲存密碼。
  - 請定期更改密碼。
- 使用O! ePay時，請留意是否有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。使用完O! ePay服務後，請即登出賬戶。
- 作為預防性的保安措施，閣下必須事先以部分八達通號碼作登記，方可進行網上付款及查詢事宜。如閣下希望加強保障，可考慮使用具遮蔽功能的卡套，以免閣下的八達通被盜用。
- 閣下的Smart Octopus必須事先透過八達通App登記，方可進行網上付款或進行轉賬。
- 每次使用完任何無線網絡功能（例如Wi-Fi、藍牙或NFC近場通訊）後，應將其關閉。
- 請不時查閱閣下的八達通交易紀錄。如發現任何可疑交易，請即致電八達通顧客服務熱線2266 2222。
- 請使用正版軟件以減低閣下受電腦病毒或間諜軟件影響或入侵的機會。盜版或不明

來歷的軟件可能含有或經間諜軟件、電腦病毒或其他不包含在原始軟件包的程式改動或修改。使用此等軟件可能會增加閣下流動裝置受病毒、間諜軟件或其他惡意軟件影響的機會，以致裝置受損或個人資料洩漏。

- 切勿「越獄」（jail-break）、獲得「Root」權限或更改作業系統。此等做法會減低作業系統的穩定性，增加系統感染電腦病毒及受間諜軟件攻擊的機會，從而損害或洩漏閣下的個人資料。如閣下使用已「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。

- 定期更新閣下的作業系統和網頁瀏覽器，以盡量提高流動裝置的安全性。請使用最新版本的作業系統和流動應用程式，並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。

- 使用並定期更新防毒軟件，可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。詳情請參閱有關軟件的「幫助」部分。

- 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至閣下的流動裝置上，從而防止任何追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。

- 使用並定期更新防火牆軟件。該軟件可能已包括在閣下的作業系統內，閣下亦可能已從第三方供應商安裝額外的防火牆軟件。閣下的防火牆軟件應定期更新，以保護閣下的電腦或流動裝置免受網絡攻擊。

- 由於無線網絡涉及無線電信號，有機會讓他人於未獲事先授權的情況下近距離進入閣下的網絡。閣下使用個人的無線路由器時，請務必使用密碼或加密數據傳輸。

- 請提防虛假 / 釣魚電郵，閣下或會收到假冒由本公司發送的電郵。該等電郵會試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。

- 垃圾郵件可能會包含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。

- 請提防外觀相似的網站，欺詐者及騙徒或會製作與閣下信任網站相似的網頁，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是閣下所信任公司的正式官方網站。

- 閣下可參考由香港金融管理局提供的教育資訊，按此觀看「智醒錦囊 - 儲值支付工具篇」短片。

- 完 -