



失卡碌爆照過數 滙豐懶理照追數

致電銀行難阻交易 用戶紛批兩道「保險線」失靈

在眾多數碼支付方式中，「碌卡」在香港佔絕對主導地位，有研究顯示信用卡支付在港使用率高達91%。消費者對信用卡的信賴建基於保安制度，包括簽賬額設上限，以防一旦被盜，也能將損失「封頂」。而在進行交易時，發卡銀行會傳短訊SMS通知卡主，為消費者提供保障。不過，近期一間銀行信用卡的多名用戶反映，銀行該兩道「保險線」失靈。有人信用卡被盜，賊人單次消費簽賬「碌爆」三成，交易仍獲正常進行，用戶在收到簽賬SMS信息後，立即致電銀行，卻無法阻止過數，更被銀行要求為賊人埋單，有人因此預起40萬元卡數。民建聯立法會議員梁熙認為，銀行對信用卡消費監督不足，金管局應敦促銀行完善措施，以保障消費者。

◆香港文匯報記者 唐文



◆梁熙認為，銀行對信用卡消費監督不足，金管局應敦促銀行完善措施，以保障消費者。 香港文匯報記者唐文攝



民建聯上週對信用卡被盜用的問題舉行記者會後，昨日再次聯同苦主舉行記者會，揭露信用卡兩道防線失效。苦主之一陳先生於去年8月赴馬來西亞期間，被人偷去了5張信用卡，包括兩張滙豐卡、一張花旗、一張安信和一張Aeon。「我剛進到酒店，就陸續接到這些銀行的SMS信息（簽賬通知），知道卡被偷了，並被人碌卡。我即時一問一問銀行打過去報失，滙豐是第一間打的，之後是Citi、安信和Aeon。」

中銀醒目及時中止交易

黎先生更慘，於今年1月被人偷走銀包，兩張滙豐卡和兩張中銀信用卡均丟失，其後收到中國銀行的SMS通知，指系統發現有多宗可疑交易，經核實後確定為非法交易，中止了交易，避免損失；但其滙豐卡已被盜用，簽賬購買超過15萬元的珠寶、海味等奢侈品。黎先生其中一張滙豐信用卡的簽賬額為5.8萬元，騙徒單次消費5.3萬元，加上黎先生當月的消費，該月簽賬額累達7.4萬元，較簽賬額超出約28%，但仍可成功過數，變相令信貸額形同虛設，令卡主失去最後一道防線。

梁熙表示，他在上次記者會後與金管局代表會面，提出不同銀行對「嚴重疏忽」有不同定義的問題，希望銀行有統一、清晰的處理，又建議對於超出使用者平常消費模式的大額或頻繁交易，需取得卡主確認才可進行交易。局方承諾會跟進，但暫未有時間表。

對有苦主的交易超出信貸額的仍獲放款，梁熙指出，根據目前銀行相關條款，銀行可視情況自行批出交易而不需要卡主同意，故認為條款有必要調整，以減低市民在失卡時可能出現的更大風險。

滙豐：有程序處理信用卡疑被盜個案

香港文匯報昨日就事件向滙豐銀行查詢，發言人表示理解客戶憂慮，重申該行有既定程序處理信用卡懷疑被盜用個案，一直與相關個案主保持溝通和積極跟進，以尋求可行的解決方案，並提醒大眾應妥善保管好信用卡，一次性密碼等敏感個人資料，如發現可疑交易或收到可疑短訊，應即時向銀行查詢或報警處理。

花旗安信須卡主確認才可交易

其中，花旗和安信當時已發現交易異常，需要他確認才可進行交易，而滙豐和Aeon均如常進行交易，但Aeon在收到報失通知後，經調查無須他承擔有關交易費用，只有滙豐堅持要他埋單，涉及逾18萬馬幣（約33.3萬港元）。

滙豐以當事人未能妥善保管信用卡屬「嚴重疏忽」為由，拒絕豁免盜刷費用，陳先生直言對該行的處理手法十分失望，「我用了該卡25年，從來沒有這樣消費過，半小時刷30萬港元，銀行竟然一點也不覺得可疑。」

張先生的情況與陳先生十分類似，分別在於他的信用卡在香港被盜，同樣涉及滙豐銀行。盜卡當晚，騙徒先是一筆過碌走30多萬元，其間張先生未收到任何SMS提示。

其後，騙徒又陸續小額交易約10萬元，他才收到相關SMS，立即要求銀行中止交易，但無補於事，最後更被滙豐追數逾40萬元。

若中「木馬程式」用手機銀行或遭偷卡資料

香港文匯報訊（記者 唐文）隨著手機數碼錢包逐漸普及使用，相關的罪行逐漸出現。有市民在沒有遺失實體信用卡的情況下，遭人盜取信用卡資料，賊人更在其手機錢包綁上事主的信用卡，導致賊人消費、事主埋單。有網絡保安專家相信，事主的手機已中了「木馬程式」，在平日用手機處理銀行服務時被賊人隔空盜取信用卡資料。立法會議員梁熙呼籲《銀行營運守則》應與時俱進，為新型電子支付制定監管制度。

苦主李小姐憶述，她於去年12月6日接到滙豐銀行職員來電稱，她前一日有三筆可疑信用卡交易，前兩筆交易不成功，第三筆交易使用google pay（手機錢包）成功過數。她當即取消信用卡及報警，但損失的1.3萬元卻無法追討。

對騙徒如何盜取信用卡信息，李小姐感到一頭霧水，「我這麼多年都是用Apple手機，從來都沒有註冊手機電子錢包，更沒有使用過google pay，為什麼銀行會允許別人碌我的卡？」她說，自己信用卡被盜用當晚並未收到任何短信驗證碼（OTP），亦未在任何地方輸入過驗證碼，但在與銀行交涉中，銀行則聲稱曾向她發送驗證碼。

李小姐指，既然銀行當時已懷疑交易有可疑，卻未有阻止交易進行，理應由銀行承擔損失。「銀行職員電話詢問我的態度好像在審犯，懷疑是我和騙徒一起密謀呢銀行錢，但又不肯透露騙徒消費的實體商戶地址，只知道是旺角的一間金舖。」

議員倡為新型電子支付制定監管制度

梁熙表示，現時金管局對綁定電子支付（如google pay、apple pay等）的信用卡交易，以及信用卡實體卡交易，採用同一套監管準則，但電子支付有更多傳統上難以預計的風險，故要求金管局檢討現時《銀行營運守則》，為新型電子

支付制定監管制度。「電子錢包中的信用卡，一般只顯示最後4位數字，也不會顯示卡主的全名，而實體信用卡具備這些信息。以往商戶一旦覺得交易可疑，可要求消費者出示其他證件，證明與信用卡上的姓名一致，但使用電子錢包就無這一重核對。」他說。

鑑於部分被盜卡主從未收到銀行發出的OTP，懷疑該短信可能被賊人截取，梁熙建議金管局考慮在信用卡綁定電子支付時，要求用戶進行OTP+密碼雙重認證，或OTP+生物特徵認證；對於剛剛綁定電子錢包的信用卡，首10宗消費，應發送SMS通知。

香港資訊科技商會榮譽會長方保僑向香港文匯報表示，相信事主的手機遭黑客入侵，被植入木馬程式而取得其信用卡資料和電子支付工具的一次性密碼（OTP），盜用其賬戶進行消費。

他解釋，現時手機會接收不少訊息，只要用戶不為意點選訊息內的連結，就可能令手機被植入「木馬程式」，「只要被植入了有關程式，黑客就可以遙控和取用戶手機內的所有資料，包括銀行和信用卡賬戶等信息。」

黑客可攔截驗證碼 用戶不知收過

使用電子支付工具時收到的驗證碼，黑客亦可以輕易盜取，「中咗木馬程式部手機就由黑客操控，銀行傳驗證碼來，黑客就攔截咗，然後遙距刪除，用戶自己也不知收過驗證碼，咁樣黑客就可以開一個電子支付賬戶，使用苦主的信用卡消費。」

方保僑強調，用戶要保護自己的個人私隱，手機不應保存有關銀行、信用卡賬戶等資料，收到任何信息後都不要胡亂點選內附的連結，更應安裝手機防病毒軟件。

議員：若感銀行失責 可向金管局投訴



對有信用卡用戶稱被人冒簽，即使簽賬額超出貸款額仍成功過數，以及致電銀行亦未能阻止交易進行，本身長期在銀行工作的金融界立法會議員陳振英直言，相信這些是極個別的事件，一般而言，簽賬額不能超出設定的限額，且信用卡公司在發現有大額交易或偵測到是高危交易時，必定會通知信用卡持有人確認是否獲授權。他表示，若信用卡持有人被冒簽而覺得銀行失責，可向金融管理局投訴，以至提出民事訴訟，交由法庭處理。

陳振英昨日在接受香港文匯報訪問時表示，銀行發出的信用卡為每名客戶設有簽賬限額，若超出有關限額就不能成功簽賬，有銀行容許超出信用限額的交易進行，相信這是個別銀行的情況。由於不清楚有關事件的來龍去脈，故他難以評論其中涉及的問題。

他強調，信用卡中心有保安部監察信用卡交易情況，倘發現有大額的不尋常交易和高危交易時，必會通知信用卡持有人，若持有人確認有關交易才會進行，故有苦主表示致電數間銀行都能成功阻止交易。至於有個別銀行收到電話後仍繼續容許交易進行，他重申：「一般信用卡公司的做法，（不尋常交易）一定會調查。」

可向發卡銀行提民事訴訟

陳振英表示，倘有信用卡用戶認為卡公司做法不合理令其招致損失，除了向銀行反映外，還可以向金管局作出投訴，也可以向發卡銀行提出民事訴訟，向法院陳述事件經過，由法庭判斷銀行方面有否失責。

◆香港文匯報記者 劉明



◆香港文匯報4月11日頭版報道「信用卡盜簽30萬 銀行竟逼客硬食」。 香港文匯報PDF版

針對金管局的建議

敦促銀行完善保障信用卡安全的措施

- ◆對於超出平常消費模式的大額或頻繁交易，銀行需取得卡主確認
- ◆對於超出信用卡額度的交易，銀行應釐定最高可超出比例
- ◆縮小不同銀行對非授權交易的處理差異，形成統一、清晰的標準
- ◆教導公眾何時需承擔損失，進一步為「嚴重疏忽」釋義

檢討現時《銀行營運守則》，為新型電子支付制定監管制度

- ◆綁定電子支付時，銀行須透過OTP+密碼雙重認證，或OTP+生物特徵雙重認證
- ◆對於剛綁定電子支付的信用卡，其頭10宗實體消費，應向卡主發SMS通知
- ◆新綁定電子支付的大額消費，需要卡主確認

資料來源：立法會議員梁熙 整理：香港文匯報記者 唐文

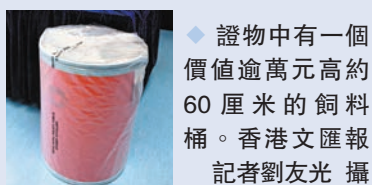
發「積分到期」短訊呃卡資料 3人被捕



◆警方破獲「積分到期」釣魚短訊詐騙集團，檢獲總值150萬元贓物，包括名牌手袋、首飾、現金等。 香港文匯報記者劉友光攝



◆警方檢獲贓物包括Tesla和平治兩輛私家車。 香港文匯報記者劉友光攝



◆贓物中有一個價值逾萬元高約60厘米的飼料桶。香港文匯報記者劉友光攝

香港文匯報訊（記者 蕭景源）「釣魚」短訊呃市民信用卡資料狂消費的案件有增加趨勢。警方近日再破獲以假冒電話商發「積分到期」短訊的詐騙集團。該集團發出短訊，誘使市民按超連結登入仿真度極高的假網站。騙徒更增加所謂電話號碼「驗證」程序，假扮查核嚴謹騙取市民信任，趁機套取市民信用卡資料，然後綁定騙徒的電子銀包，交給同黨「車手」極速瘋狂購買名貴物品。警方拘捕該集團3人，檢獲總值150萬元名牌手袋波鞋、香水等贓物，相信與全港多宗同類案件有關。

警方於本月上旬接獲5名市民報案，指接獲一個電話商的「積分到期」短訊，要求點擊附帶連結登入網站更新資料和辦理兌換手續。同一天，事主發現信用卡有未經授權的交易，懷疑被盜用。5人損失共約23萬元。

增電話「驗證」程序 降事主警覺性

據了解，警方發現在本宗案中，騙徒設計的電話商假網站仿真度極高，除了精美動畫，更有新「花樣」騙取卡主信任。以往事主在進入

同類假網站時，無論隨意輸入什麼內容，都會跳入輸入信用卡資料程序，容易引起事主懷疑或中途放棄。在今次案件的假網站，騙徒增添了一頁輸入電話號碼「驗證」的程序，讓市民收取確認短訊後，才能登入積分和換禮品頁面輸入信用卡資料，令事主警覺性降低。

由於騙徒在社交平台隱藏真實身份，增加了警方偵查的難度。邊界警區重案組高級督察黃潤彤昨日簡介案情時表示，警方經深入調查後，在本月18日和19日，分別在中區和元朗錦田拘捕兩男一女（28歲至35歲），分別報稱司機、美容師和地產代理。警方在他們住所及窩點檢獲逾150萬元名牌貨，包括名牌手袋、服裝、手機、波鞋等，同時扣查一輛Tesla和一輛平治私家車，兩車登記車主為其中一名被捕者。

門快購物 銷贓同黨轉售圖利

被捕的詐騙集團分工明確，由主腦獲得信用卡資料，迅速綁定在手機電子銀包後，再由「車手」到名店購物，在卡主發現前門快購物，最後由負責銷贓同黨將名牌貨轉售圖利，套現後交回主腦再分發予下線。

警方相信是次被捕3人中，有兩人是「車手」，一人是銷贓角色。由於贓物眾多，有理由相信詐騙集團活躍半年，干犯多宗案件，受害者包括海外人士。