



臺灣臺北地方法院檢察署新聞稿

Taipei District Prosecutors Office Press Release

發稿日期:105年9月13日

聯絡人:張介欽襄閱主任檢察官

電話:(02) 23146881

臺灣臺北地方法院檢察署偵辦第一商業銀行股份有限公司（下稱第一銀行）ATM 現鈔跨國盜領案件，於今日偵查終結，茲簡要說明如下：

壹、偵查結果

- 一、被告 P○ A○（下稱安德魯）、C○ M○（下稱米海爾）、P○ N○（下稱潘可夫）3 人所為，係共同涉犯刑法第 339 條之 2 第 1 項之以不正方法由自動付款設備取得他人之物罪嫌、第 358 條之無故利用電腦系統漏洞而入侵他人電腦罪嫌、第 359 條之無故變更他人電磁記錄罪嫌、第 360 條之無故以電腦程式干擾他人電腦與相關設備罪嫌及第 362 條之製作專供犯妨害電腦罪章之電腦程式等罪嫌，均提起公訴。
- 二、被告 B○ S○（下稱貝瑞左夫斯基）等 19 人均另案通緝。
- 三、本案除起訴及通緝之被告外，是否尚有人嫌犯其他犯罪，已另分案偵辦中。

貳、有關起訴部分之簡要犯罪事實

- 一、安德魯（拉脫維亞籍）、米海爾（羅馬尼亞籍）潘可夫（摩多瓦籍）、與貝瑞左夫斯基（俄羅斯籍）、B○ V○（俄羅斯籍，下稱柏克曼）、M○ G○（俄羅斯籍，下稱曼紐肯）、A○ K○（俄羅斯籍，下稱艾迪恩）、M○ O○（羅馬尼亞籍，下稱馬力克）、S○ I○（羅馬尼亞籍，下稱賽克亞瑞）、V○ I○（羅馬尼亞籍，下稱維利科羅）、B○ E○（俄羅斯籍，下稱比比）、U○ V○（羅馬尼亞籍，下稱烏爾蘇）、A○ A○（羅馬尼亞籍，下稱阿爾謝）、T○ X○（愛沙尼亞籍，下稱譚恩）、K○ V

○（澳大利亞籍，下稱維克特）、G○ Y○（白俄羅斯籍，下稱雅克夫）、I○ J○（拉脫維亞籍，下稱約瑟夫）、I○ R○（俄羅斯籍，下稱拉菲克）、L○ A○（俄羅斯籍，下稱洛夫斯基）、S○ O○（俄羅斯籍，下稱莎琪蘇娃）、B○ E○ P○ P○（法國籍，下稱保羅）、F○ R○（拉脫維亞籍，下稱雷納斯，上 19 人均另案通緝）等 22 人，與真實姓名年籍不詳之成員，共同組成入侵銀行內部網路以盜領自動提款機（下稱 ATM）內款項之國際犯罪集團。分工方式係由集團中之不詳成員（另案偵辦中），負責入侵銀行內部網路並製作、布署盜領 ATM 所需之電腦程式；由貝瑞左夫斯基、柏克曼、曼紐肯、艾迪恩、馬力克、賽克亞瑞、維利科羅、烏爾蘇、阿爾謝、譚恩、維克特、雅克夫、約瑟夫、拉菲克等 14 人擔任俗稱之「車手」，負責依編組至 ATM 盜領款項兼為同組車手把風；由巴比擔任俗稱之「車手頭」，負責至 ATM 盜領款項並兼向各組車手收取贓款；再由安德魯、潘可夫、米海爾、洛夫斯基、莎琪蘇娃、保羅、雷納斯負責贓款之後續搬運、寄藏等分工細膩。上開集團成員於民國 105 年 5 月 31 日前某日間，藉由網際網路探知我國之第一商業銀行股份有限公司（下稱第一銀行）倫敦分行，有一可同時連結網際網路及第一銀行內部網路之電話錄音主機存在電腦系統之漏洞，以及第一銀行內部使用之自動提款機，有多數為德國「Wincor Nixdorf」公司所生產之「ProCash 1500」型提款機，且得知該型提款機內部吐鈔模組之運作與控制機制後，即共同基於意圖為自己不法所有、製作專供犯妨害電腦使用罪章之電腦程式、無故利用電腦系統漏洞而入侵他人電腦、無故變更、刪除他人電磁紀錄、無故以電腦程式干擾他人電腦與相關設備之犯意聯絡，依下列步驟，共同為入侵第一銀行內部網路及盜領 ATM 內款項犯行：

- （一）集團內之不詳成員，先於 105 年 7 月 5 日前某日時（105 年 7 月 5 日係集團內之成員最早來台之日期），製作專供取得「ProCash 1500」型 ATM 內現鈔資訊之電腦程式「cnginfo.exe」、專供命令該型提款機執行吐鈔動作且限定僅能於 105 年 7 月間執行之電腦程式「cngdisp.exe」與「cngdisp_new.exe」、專供犯案後呼叫「sdelete.exe」之電腦程式，功能係針對欲刪除之檔案進行磁

區抹除，使得刪除後之檔案難以透過專業軟體進行復原，以徹底刪除「cnginfo.exe」與「cngdisp.exe」進行滅證之電腦批次檔「cleanup.bat」等專供犯妨害電腦使用罪章之惡意電腦程式後，並於105年5月31日晚上22時36分許，侵入第一銀行倫敦分行電話錄音主機電腦系統之漏洞，便利作為日後侵入其他第一銀行電腦之跳板。

- (二) 謀議既定後，陸續於105年6月28日起至7月4日間，利用第一銀行倫敦分行電話錄音主機作為跳板，侵入第一銀行內部網路中負責「ProCash 1500」型ATM電腦程式更新派送暨監控之應用程式伺服器，連續將目的係在各ATM電腦上執行盜領前準備工作之電腦指令，例如刺探ATM電腦軟硬體資訊、在ATM電腦上建立具有管理者權限之帳號「support_487566a0」等準備工作之電腦指令，包裝為附檔名為dms之封裝檔，先後共33個，以操作AP伺服器上之派送程式，將前揭封裝檔派送至該集團為犯案選定位於臺北市、新北市、臺中市，共計41部之「ProCash 1500」型ATM之電腦上執行，而變更該等ATM電腦上之使用者帳號紀錄，並蒐集取得該等ATM電腦之資訊，作為進行盜領前之準備。
- (三) 安排妥適後即於105年7月5日前某日時，再利用第一銀行倫敦分行電話錄音主機作為跳板，侵入第一銀行內部網路中負責針對第一銀行所使用另一系列由NCR公司生產之ATM，進行ATM電腦程式更新派送之NCR伺服器，將上開惡意程式「cnginfo.exe」、「cngdisp.exe」、「cngdisp_new.exe」、「cleanup.bat」存放在該伺服器內，以便後開始進行盜領時，供上述41部第一銀行ATM得以連線至NCR伺服器後以ftp方式加以下載。另為驗證前述入侵與布署惡意程式機制是否可行，並於105年6月30日凌晨2時11分，選擇位於台北市萬華區第一銀行西門分行ATM進行測試，透過NCR伺服器傳送「86.exe」程式至該西門分行ATM之電腦，再於同日凌晨3時52分許，經AP伺服器將作用為建立上開管理者帳號並呼叫「86.exe」程式以提高該帳號telnet權限之電

腦指令封裝檔，派送至該西門分行 ATM 之電腦，以建立具有 telnet 連線能力之帳號後，復於同日晚上 9 時 18 分 5 秒至 31 秒期間，一方面委請真實姓名年籍不詳男子，至該西門分行 ATM 前觀察，另一方面由集團內成員自第一分行倫敦分行電話錄音主機以 telnet 方式連線至該西門分行 ATM 之電腦，執行諸如「cnginfo.exe」之程式以測試該 ATM 吐鈔口開闔情形，並由該不詳之人觀察後以手機回報，因而確認前述入侵與布署惡意程式之機制確實可行。

- (四) 嗣入侵第一銀行內部網路及惡意電腦程式之製作與布署等前期作業完成後，即自 105 年 7 月 8 日起負責之車手暨車手頭共 15 人先後分組、分批入境，並自同年月 10 日凌晨 0 時許起開始分組犯案，均利用手機通訊軟體通知該集團不詳之成員，由該成員利用第一銀行倫敦分行電話錄音主機作為跳板，以 Telnet(遠端登錄服務)之方式與該 ATM 電腦建立連線，並輸入事先已建立在該 ATM 電腦上之管理者帳號「support_487566a0」暨密碼後，侵入上述 41 部 ATM 之電腦，再由該 ATM 之電腦上以 FTP(檔案傳輸服務)之方式，自 NCR 伺服器下載取得上開盜領用惡意電腦程式「cnginfo.exe」、「cngdisp.exe」與「cngdisp_new.exe」、「cleanup.bat」，隨即執行「cnginfo.exe」確認 ATM 之吐鈔模組狀態，再執行「cngdisp.exe」或「cngdisp_new.exe」，以干擾 ATM 電腦及 ATM 內之吐鈔模組，使該 ATM 在未經 ATM 電腦與第一銀行帳務系統連線稽核之狀況下，直接由 ATM 之吐鈔模組吐出上開惡意程式所指定數額之現鈔，並由守候在各該 ATM 前之車手或車手頭取款，而以此等不正方式，自各該具有自動付款功能之 ATM 內盜取款項，共計達新臺幣(下同)8,327 萬 7,600 元，足生損害於第一銀行。
- (五) 得手後，上開集團內成員，為將侵入第一銀行內部網路布署上開電腦程式之跡證湮滅，復於 105 年 7 月 12 日，利用第一銀行倫敦分行電話錄音主機作為跳板，再次侵入第一銀行內部網路中之 AP

伺服器，將目的在於執行上開「cleanup.bat」程式，以便將犯案用惡意程式「cnginfo.exe」、「cngdisp.exe」與「cngdisp_new.exe」進行徹底刪除之電腦指令，包裝為檔名為「60712001.dms」之封裝檔，再以 AP 伺服器上之派送程式將該封裝檔派送至遭盜領 ATM 之電腦上執行，以徹底刪除做案用之惡意程式及該等程式產生所產生諸如「displog.txt」之電磁紀錄。另又針對作為跳板第一銀行倫敦分行電話錄音主機，將硬碟內電磁紀錄刪除，使該電腦無法連線登入查看其狀態，足生損害於第一銀行。

(六) 繼之集團成員為處理贓款後續搬運、寄藏暨掩護同案共犯等事宜，上開犯罪集團復自 105 年 7 月 9 日起安排陸夫斯基等 7 位成員來台接應。而上開集團內之各組車手暨車手頭完成 ATM 之取款後，第 1 組車手之贓款，連同該組車手柏克曼於 105 年 7 月 11 日凌晨 4 時 38 分許，至第 5 組車手投宿之旅社內收取之第 5 組車手之贓款，將款項放置於所投宿之留在君悅飯店房內，等候同集團後續來臺成員入住該房間後進行後續處理；第 3 組、第 4 組車手之贓款係由車手頭巴比收取後，於 105 年 7 月 12 日下午 5 時 58 分許，將款項裝入黑色大型行李箱、藍色小型行李箱各 1 只內，分別暫置在臺北車站地下 1 樓東出口前置物櫃；第 2 組、第 6 組車手之贓款則係由洛夫斯基收取後，與莎琪蘇娃共同處理，並於同年月 11 日下午 5 時 55 分許，裝在白色大型行李箱 1 只內，暫置於投宿之寒舍艾美酒店房內，復由車手頭巴比與保羅於同年月 13 日下午 5 時 54 分許，在寒舍艾美酒店會面後，由巴比至艾美酒店房內取走該只白色大型行李箱，並於同日下午 6 時 47 分許，存放在臺北火車站地下 1 樓東出口前置物櫃。安德魯則經上開集團之指示來臺，於同年月 11 日下午 6 時 52 分許，至臺北市君悅酒店，以訪客身分向櫃檯取得房卡後，取得第 1 組車手甫於同日上午離開時（未辦理退房，並事先已告知櫃檯將有另 1 名俄籍友人來訪，請櫃檯配合給予房卡），暫置該房間內之行李箱內之贓款，準備進行贓款之後續處理；惟斯時因第一銀行 ATM 遭盜領之新聞已見諸媒體報導，安德魯經集團成員之指示，於同年月 12 日自君悅酒店

退房，隨後攜帶贓款入住臺北市中山區民生東路之套房，並於同年月 13 日凌晨 5 時 3 分許，將贓款裝放於 1 只黑色行李袋、1 只電腦手提包後，藏放在臺北市內湖區內湖路登山口上方約 50 公尺處旁草叢內後返回上開套房，又於同日上午 9 時 2 分許再度回到上址藏放處，以便將該地點之 GPS 座標，透過手機通訊軟體回傳集團成員，並依指示前往宜蘭縣躲避，上開集團則另指派雷納斯，於同年月 16 日午間將新購得之三星牌 A5 型手機空機 1 支，藏放在宜蘭縣頭城鎮烏石港之消波塊中，指示安德魯前去取用，準備伺機再進行贓款之後續處理。而米海爾則經由巴比之指示偕同潘可夫來臺，於同年月 16 日下午 4 時 50 分許，自臺北車站地下 1 樓東出口前置物櫃，取得裝有贓款之上開 3 只行李箱，準備進行贓款之後續處理。

二、嗣於 105 年 7 月 10 日晚上 8 時 17 分許，有民眾蔡姓夫婦在臺北市大安區之第一銀行古亭分行，見艾迪恩、曼紐肯行色慌張，ATM 之吐鈔口遺有 6 萬元之現鈔而察覺有異，遂報警處理，經警循線追查後，安德魯於 105 年 7 月 17 日下午 5 時 10 分許，在宜蘭縣南澳鄉省道臺 9 線 120.4 公里處為警查獲，並扣得其攜帶之手機 SAMSUNG、HTC 手機空機各 1 支、國外門號 SIM 卡 3 張與贓款 5 萬 9,000 元；潘可夫、米海爾於同年月 17 日晚上 8 時 15 分許，在臺北市中山區敬業四路維多利亞酒店房內為警查獲，並扣得分別裝有贓款 2,689 萬 4,000 元、2,255 萬 3,000 元、1,079 萬 3,000 元之黑色大型行李箱、白色大型行李箱、藍色小型行李箱各 1 只、現金 8,000 元及潘可夫攜帶之 iPhone 5 手機 2 支、米海爾攜帶之 iPhone 6 手機 2 支；復於同年月 20 日下午 1 時 40 分許，在臺北市內湖區內湖路 1 段登山口上方約 50 公尺處旁草叢內，查獲安德魯藏放在該處，裝有贓款 1,263 萬 900 元之行李袋 1 只；另民眾柯○林（另案偵辦中）於同日晚上 10 時許，繳回其於上午 6、7 時許在上開安德魯藏款處附近拾獲電腦手提包內之 454 萬 2,200 元贓款，總計查獲贓款 7,748 萬 1,100 元。經法務部調查局新北市調查處將第一銀行倫敦分行電話錄音主機、AP 伺服器、NCR 伺服器及 41 部 ATM 之電腦送鑑定、分析比對，始查悉上開犯罪集團入侵電腦，植入惡意

程式之犯案細節。

參、所犯法條

核被告安德魯、米海爾、潘可夫 3 人所為，均係犯刑法第 339 條之 2 之以不正方法由自動付款設備取得他人之物、第 358 條之無故利用電腦系統漏洞而入侵他人電腦、第 359 條之無故變更他人電磁紀錄、第 360 條之無故以電腦程式干擾他人電腦與相關設備、第 362 條之製作專供犯妨害電腦使用罪章之電腦程式等罪嫌，並請從一重處斷。又被告 3 人與同案被告 19 人以分組、分工方式，接受集團中之不詳成員遠端遙控指令，於不同時段，在臺北市、新北市、臺中市所為 12 次盜領 ATM 款項之犯行間，犯意分別，行為互殊，為數罪，請予分論併罰。

肆、量刑意見

請審酌本案為國內首見橫跨歐洲，由多國犯罪成員所組成國際性有組織之犯罪集團，以入侵銀行電腦系統，植入惡意程式於遠端遙控，在我國內盜領款項之智慧型犯罪模式，短期間內即盜得 8,327 萬餘元之鉅款，對國內金融秩序造成嚴重擾亂、破壞，更引發國人極大恐慌，影響深遠；且上開犯罪集團成員甚多，計畫縝密、分層負責、分工細密，於犯案後再度入侵銀行電腦系統，進行滅證，免遭追緝。而被告 3 人受命入台處理鉅額贓款之責任非輕，期間被告安德魯不斷變裝、遷移居處、變換計程車並迂迴繞路、丟棄通訊手機、藏身偏遠海邊，並將贓物藏於山區隱匿處並定位座標回傳等情；被告米海爾、潘可夫 2 人於入台前即經由媒體之報導知悉本案，其 2 人仍事前蒐集、安排處理贓款相關事宜；另被告米海爾專責提供資訊與集團重要成員車手頭巴比及安排交通等情，足徵渠等犯罪手法專業、細膩，均屬國際盜領犯罪集團核心分子無疑，況被告 3 人犯後均避重就輕，否認係集團成員參與盜領計畫或處理贓款，徒以受託來台拿取行李廂等詞狡飾，犯後態度非佳；衡諸前述一切情狀，請各量處有期徒刑 12 年，以茲懲儆。至扣案之物，併請依法宣告沒收之。

伍、偵辦契機

本署近年來有感於詐騙犯罪日趨嚴重，因此將打擊詐騙犯罪列為重點工作之一，本案為國際上罕見之跨國集團性詐騙犯罪，在偵辦上倍增困難，全案之所以能將留滯在臺之嫌犯予以收押禁見，並追回大量贓款，順利偵結本案，端賴於熱心國人蔡姓夫婦之挺身而出，見義勇為，形成本案破案之契機，之後方能在檢警調等相關單位鍥而不捨、合作無間之努力下，順利偵結本案，法務部邱部長為感念蔡姓夫婦之義行，鼓勵國人勇於檢舉犯罪，強化打擊犯罪之能量，特別親自接見蔡姓夫婦並致贈「義行可風」金馬琉璃一座，附此敘明。