

刑事

雙月刊 中華民國109年4月

CRIMINAL

BIMONTHLY

95



本期主題：

全方位打擊詐欺 阻斷集團犯罪鍊

P03 新修正洗錢防制法下的
金融面向打擊作為

P06 創新預防解除分期付款詐騙策略-
以國內外指標電商成功案例說明

P09 偵辦猜猜我是誰手法「數位式移動節費
設備」(Digital Mobile Trunk) 詐欺話務
機房案實務研析

拓展警政外交 加強國際合作

全球化浪潮紛起與資通訊科技迅速發展，縮短人與人之間的距離，國際間的經濟與文化交流日益緊密，亦導致各類犯罪得以輕易跨越國界，不法之徒共組集團，利用各國法制及執法差異，穿梭其間以牟取龐大利益及逃避法律制裁。這類跨越國境、地區的新興犯罪不同於傳統犯罪，型態多變且影響範圍深遠，對各國執法單位而言，均是當前艱鉅的考驗。

為防制跨國及跨境犯罪，我國於重點國家派駐警察聯絡官及短期任務型聯絡官，與各國友軍單位保持密切聯繫，並透過邀訪外國警政首長、參加國際警察組織活動等，與各國執法機關建立管道分享情資，以追查國內外涉案犯嫌及不法情事，共同合作打擊跨國犯罪集團，且藉由推展國際警政交流，增進我國警察偵辦案件與打擊犯罪的專業知能。

本局自107年起連續2年協助警政署舉辦國際警察合作論壇國際研討會，邀集超過30個國家警政高層及執法單位人員與會，探討電信詐欺、毒品犯罪等國際關注之治安議題，分享交流打擊跨國犯罪之豐富經驗，不僅有效增加我國在國際社會的能見度，更讓各國執法單位深切體認，於打擊跨國犯罪問題方面，我國是不可或缺和不容忽視的重要成員。

刑事雙月刊第96期將以「拓展警政外交 加強國際合作」為主題，探討近年各國警察機關跨境合作打擊毒品、詐欺等各類犯罪之偵處經驗與防制策略，以及積極推展跨區域平臺，加強情資交流、追查贓款及遣返罪犯等執法作為，預定於109年6月出刊，歡迎各界踴躍投稿。



歡迎各界踴躍投稿

投 | 稿 | 信 | 箱

paper@email.cib.gov.tw



全方位打擊詐欺 阻斷集團犯罪鍊

蔡總統於 108 年首次署務會報中肯定警方在反詐方面成績亮眼，要求相關單位未來應持續全力以赴，爰本局續將「打詐」列為治安重點項目，與各國執法單位保持緊密合作，規劃跨境詐欺犯罪之偵防作為與建立情資交流平臺，於偵查、預防、宣導與管理機制等面向採取「偵防併舉」策略，期能多管齊下，有效遏止詐欺犯罪，並深化跨境共同打擊犯罪機制，加強查緝跨境電信網路詐欺集團，有效維護國人財產安全。

科技快速進步與民眾消費習慣改變，詐欺犯罪型態亦與時俱進，結合高科技與跨境犯罪模式，透過企業化、國際化經營犯罪組織，以低成本、高報酬之犯罪手法獲取不法利益，使警察機關於偵防詐欺犯罪方面，面臨日益艱鉅的挑戰。因此，強化整體偵查效能，提升查緝犯罪能量，儼然已成為當前重要課題。

然因現今社會消費模式從傳統實體店面轉為網路虛擬賣場，詐欺集團轉而攻擊賣場取得客戶個資，並搭配各種詐騙話術來行騙消費者。故針對是類犯罪，初期階段將加強電商資料庫防護，使詐騙集團不易取得交易個資；中期階段以提升民眾反詐意識為主軸，輔以限縮帳號匯款及員警關懷提問，降低民眾被害機率及提升攔阻成效；後期階段則加強取締以竊取電商個資遂行後續犯罪之詐騙集團，以期澈底打擊。

刑事雙月刊第 95 期以「全方位打擊詐欺 阻斷集團犯罪鍊」為主題，探討國內詐欺犯罪查緝現況，並深入研析詐欺車手查緝策略，電信詐欺話務機房演進趨勢，因應新修正洗錢防制法之金流查緝作為，以及研議網路電商等新興詐騙類型之偵防對策，與各界共同研商與分享打擊及防制詐欺犯罪之道。



刑事

雙月刊 中華民國109年4月

CRIMINAL

BIMONTHLY

95



專業·科技·正義·服務·團隊

發行人：黃明昭

副發行人：林炎田、朱宗泰、廖訓誠

總編輯：莊定凱

副總編輯：陳裕琛、黃淑華

主編：黃欣怡、林俊光

執行編輯：游上佳、黃國晉、林本源、施騰凱

設計印刷

人藝印刷藝術國際股份有限公司

地址 | 235新北市中和區中正路788-1號2樓

電話 | 02-3234-0558

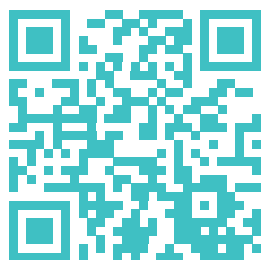
圖片 | 123RF

GPN | 2009305556

ISSN | 2072-4764

封面題字

書畫家 | 樓柏安先生



研討專題

Special Topic

108 年詐欺犯罪查緝成效與策進04

文·圖 | 楊宗霖

108 年詐欺車手查緝量能研析及展望.....09

文·圖 | 邱之伶

新修正洗錢防制法下的金融面向打擊作為 15

文·圖 | 王濟

電信詐欺話務機房之演進與趨勢20

文·圖 | 嚴泓元

遊戲點數詐欺案件現況分析與
偵防策進作為25

文·圖 | 謝政彬

創新預防解除分期付款詐騙策略-
以國內外指標電商成功案例說明30

文·圖 | 林奕辰

電信詐欺恐嚇犯罪趨勢與查處策略.....36

文·圖 | 吳榮修



破案心路

Case Study

運用第三方警政策略阻斷
詐欺集團網路及電信管道40

文·圖 | 王靖欽

偵辦猜猜我是誰手法「數位式移動節費設備」
(Digital Mobile Trunk)
詐欺話務機房案實務研析46

文·圖 | 鄭信良



新知科技

Technology

通訊監察於打擊詐欺犯罪實務之助益..... 50

文・圖 | 楊元宏

郵包炸彈處置與應變..... 54

文・圖 | 蕭雅安

偵查論壇

Forum

警察機關執行防制洗錢作為與未來展望..... 58

文・圖 | 賴建亨

修正刑法打擊聚眾鬥毆..... 63

文・圖 | 鄒至剛

正義拍檔

Visiting

國際交流..... 68

文・圖 | 林本源、施騰凱

寰宇交流

Communication

阻斷跨境電信網路詐欺集團..... 70

文・圖 | 康淳閔

各國《禁蒙面法》的立法源由及刑事偵查意涵. 73

文・圖 | 楊宗新

108 年詐欺犯罪 查緝成效與策進

刑事警察局打擊詐欺犯罪中心偵查員／楊宗霖

壹、前言

當前的詐欺犯罪，因社會經濟型態與民眾消費方式而不斷變形，並運用通訊科技組成跨國犯罪組織，循企業化經營模式，展開跨境犯罪獲取龐大利益，各國執法者無不想方設法力求突破，下文即為我國警方於打詐及防詐的具體成果與未來策進。

貳、108 年詐欺犯罪概況

一、詐欺案件受理、破獲情形

108 年 1 月至 12 月（以下稱本期）詐欺案件受理數計 23,671 件，較 107 年 1 月至 12 月（以下稱去年同期）增加 201 件

（+0.86%）；破獲數計 22,025 件，較去年同期增加 347 件（+1.6%）；破獲率 93.05%，較去年同期增加 0.69 個百分點。

二、主要詐欺案類分析

本期受理案件以「假網路拍賣（購物）」3,720 件（占 15.72%）最多、「一般購物詐欺（偽稱買賣）」3,060 件（占 12.93%）次之、「解除分期付款詐欺（ATM）」2,846 件（占 12.02%）再次之；本期破獲案件以「假網路拍賣（購物）」3,677 件（占 16.69%）最多、「解除分期付款詐欺（ATM）」2,829 件（占 12.84%）次之、「猜猜我是誰」1,915 件（占 8.69%）再次之；本期各詐欺案類破獲率，除「色情應召詐財」破獲率為 39.81%及「假

愛情交友」為 69.46% 較低外，其餘案類破獲率均維持 8 成以上。

三、詐欺犯嫌與被害人分析

本期緝獲詐欺犯嫌計 3 萬 0,089 人，較去年同期增加 2,852 人(+10.47%)，其中以男性犯嫌居多，共計緝獲 2 萬 0,924 人(占 69.54%)；詐欺被害人計 3 萬 4,083 人，較去年同期減少 1,635 人(-4.58%)，其中男性被害人 1 萬 7,151 人及女性被害人 1 萬 6,932 人約各占 5 成。

參、108 年重要工作成效

一、規劃執行「全國同步查緝車手專案行動(斬手行動)」

農曆年前民間現金流通量高，經統計為詐欺案件高發期，且詐欺集團通常於年節前夕將大筆不法所得攜回臺灣，為期先發制人，有效壓制詐欺集團氣焰，並加強查扣不法所得，本署於 108 年 1 月 9 日至 25 日執行第 3 次全國同步查緝車手專案行動，統計專案行動執行期間，共計查獲犯嫌 1,915 人，查扣不法所得合計新臺幣 1 億 0,249 萬餘元。



圖 1：署長出席斬手行動成果記者會(圖為現場贓證物展示)

二、規劃執行「全國同步打擊詐欺專案行動」

暑假期間為青少年從事詐欺車手之高發期，為持續刨根溯源、掃蕩詐欺集團，爰規劃針對詐欺「集團核心」、「詐欺車手」、「查扣不法所得」三大面向進行打擊，於 108 年 7 月 8 日至 12 日規劃執行「全國同步打擊詐欺專案行動」，傾全國警力全面掃蕩詐欺集團，統計本次專案行動執行期間，共計查獲犯嫌總數 2,280 人，另查扣不法所得合計新臺幣 4 億 1,174 萬 3,423 元。

三、研修推動「偵防電信網路詐欺犯罪工作執行計畫」

(一)為推動各警察機關落實執行打擊電信網路詐欺工作，本署除依各階段治安情況機動性調整查緝重點外，並定期針對計畫內容與執行狀況，廣納各警察機關意見，108 年間業已滾動式修正各評核項目與計畫內容，調整相關評核基準項目、提升詐欺承辦人員獎勵，並修正羈押率評項比重，與基準值免納婦幼警察隊刑警數，以減輕同仁執勤負擔，並鼓勵積極溯源查緝。

(二)108 年各警察機關共計查緝詐欺取款車手 9,494 人，較 107 年增加 2,114 件(+28.64%)、偵破國內詐欺話務機房 74 件，較 107 年同期增加 13 件(+21.31%)、偵破電信網路詐欺集團 657 件，較 107 年同期增加 205 件(+45.35%)，整體查緝能量提升。





圖 2：108 年詐欺取款車手、話務機房、詐欺集團查緝情形

四、研修推動「追緝網路購物詐財專案行動計畫」

為鼓勵各警察機關積極偵辦網路購物詐財案件，本署針對各主要網購詐欺類型「交易型網路購物詐騙（放長線釣大魚）」、「三方詐騙」、「典型網路購物詐騙（買空賣空）」，依其特性個別修正核分規定及外勤績效評鑑標準，期能提升各警察機關偵查量能，有效減少是類案件發生。

五、加強詐欺人頭電話卡溯源查緝作為

本署針對「猜猜我是誰」警政停斷話資料與 DMT 案件涉案電話，透過大數據分析，溯源追查人頭卡經銷商與異常銷售通路商，並由刑事警察局電信偵查大隊組成專案小組積極查緝；各單位如有查獲詐欺集團案件，其集團成員所使用之人頭卡門號亦彙整交由電信偵查大隊溯源清查有無不肖經銷商與通路商涉入，藉以斬斷詐騙集團施詐工具。

六、持續掃蕩國內非法話務據點 (DMT)

為打擊各地 DMT(Digital Mobile Trunk, 數

位式移動節費設備) 詐欺話務機房，本署持續分析「猜猜我是誰」案件通聯資料，並篩選比對各地可疑話務機房據點後，即將相關情資交由刑事警察局北區（電信偵查大隊第一隊）、中區（偵查第六大隊第六隊）、南區（偵查第八大隊第六隊）各外勤專責大隊偵處；然 DMT 話務機房據點設置容易、轉移迅速，未來將持續要求各偵辦單位溯源追緝，向上追查集團共犯及幕後主嫌，以澈底截斷其詐騙管道。



圖 3：持續查緝各地 DMT 詐欺話務機房（圖為 DMT 話務設備）



七、研修推動「警示帳戶作業規定與流程」

為確實反映民意，達簡政便民之效，本署業已修訂「民眾解除警示帳戶申請書」及相關作業流程，明定單一窗口原則，並簡化「帳戶如未交付予他人而遭利用」處理流程，及單獨列示「一般商業交易糾紛」項目與加速公司戶之解除流程，除函發各警察機關知照，並協請金融監督管理委員會銀行局、財團法人金融聯合徵信中心函發各金融機構配合辦理。

八、協請網拍業者執行虛擬帳戶案件防制措施

為有效降低虛擬帳戶涉案情形，本署持續與「蝦皮拍賣」與「淘寶網」業者研商，針對虛擬帳戶不同屬性，分別執行各項行政措施，涉案虛擬帳戶數已明顯下降，前揭業者配合執行相關行政措施如下

（一）蝦皮拍賣（境內虛擬帳戶）：

加強用戶認證機制、成立詐欺防制小組，研擬風險控管對策與監看交易平臺異常情形、限縮單筆交易金額（每筆限額新臺幣2萬元）、加強銀行對接，每日接收銀行端訊息，並停權可疑買家帳戶。

（二）淘寶網（境外虛擬帳戶）：

關閉所有經過海外IP認證之帳戶、全面停止平日夜間及假日認證服務、關閉可疑認證手機門號（號碼尾數連號/回撥為空號者）。

九、協請遊戲點數業者執行各項防詐措施

（一）「智冠科技股份有限公司」發行之MyCard點數卡，原為詐騙集團利用遊戲點數取贓之最大宗，經本署持續與該公

司研商實施各項防詐機制，詐騙集團利用該公司遊戲點數情形已明顯降低，該公司配合執行措施如下：

1、「實施國內外會員身分重新驗證機制」：針對該公司所屬會員進行重新驗證，包含電子信箱與聯絡電話等，增加會員帳戶確實為正常玩家使用之比例。

2、「實施黑名單預警機制」：針對國外會員帳號進行交易監控，如有儲值點數交易異常之帳戶，再以人工比對並凍結該帳戶之遊戲點數儲值。

（二）為複製「智冠科技」執行經驗與成功防制模式，本署持續與「遊戲橘子數位科技股份有限公司」研商防制策略，期能降低詐騙集團利用該公司發行之GASH卡遊戲點數銷贓情形，該公司配合本署執行措施如下：

1、「推動會員升級並重新認證帳號」：推動帳號整併之升級服務，比照「智冠科技股份有限公司」模式，全面要求註冊會員重新認證帳號，藉此消弭人頭帳號。

2、「禁止境外IP儲值國內實體遊戲點數卡」：經雙方協商評估可行性後，該公司業已試辦禁止境外IP儲值國內實體遊戲點數卡機制，以降低非法代儲情形。

肆、未來策進

詐欺集團分工細緻，且製造組織各分層斷點，規避警方查緝並增加偵辦難度，本署未來將秉持阻斷詐欺犯罪結構鍊、向上溯源、向下刨根及分享情資、協作偵查與共享成果

等理念，針對詐欺集團上、中、下游分別執行各項打擊策略，以有效壓制詐欺犯罪：

一、截斷通信網絡

持續與各電信業者研商建立詐騙電話預防攔阻機制，落實執行斷源專案工作，向上溯源追查人頭卡經銷商與異常銷售通路商，提高追緝非法業者量能，截斷詐欺集團通信網絡。

二、阻斷金流管道

人頭帳戶為詐欺集團獲取被害者財物之重要工具，本署將持續精進收購人頭帳戶犯嫌打擊作為，除提高查緝取簿犯嫌之專案核分權重，激勵同仁積極偵辦涉人頭帳戶案件外，並指定專責查緝大隊即時整合情資，以阻斷詐欺上游獲取金流管道。

三、防制個資外洩

持續配合經濟部工業局強化電商業者管理機制，落實執行行政檢查及裁罰，定期統計各賣場案件數與公布高風險賣場，除製作防詐宣導包供電商業者參處，並利用多元管道加強宣導，協請各大網路賣場加設警示標語，強化民眾網路購物安全意識。

四、打擊轉接話務

近期「猜猜我是誰」詐騙話務已漸轉由VoWiFi(可於境外透過WiFi撥打國際電話，費率與國內電話相同)撥打之現象，本署將持續研析犯嫌使用話務之異常表徵，與電信業者研擬篩選機制，以利執行後續停斷話作為，精進打擊轉接話務管道。

五、加強高風險對象監控

考量通緝犯嫌如棄保潛逃至國外，極可能於第三地以詐欺犯罪謀生，並結合當地國民詐騙他國民眾，本署將持續清查前揭犯嫌，以利後續溯源追緝；另為打擊國人赴海外從事詐欺犯罪，本署亦將持續利用大數據分析及情資蒐集，掌握核心成員出境動態，並針對境外犯罪建立合作窗口，共同打擊詐欺犯罪。

六、落實防詐宣導攔阻被害款項

持續要求各警察局分析轄內詐騙手法類型與高風險被害族群，運用分齡分眾與主題式反詐宣導模式，提升防詐宣導效果，並強化與轄內金融機構之聯繫機制，以增加線上攔阻成效。

伍、結語

詐欺犯罪戕害民眾財產安全甚鉅，且影響政府施政威信與金融體系穩定，本署將廣續推展跨部會、跨機關及跨領域合作，統合各警察機關查緝量能，持續執行各項打擊詐騙工作，以有效瓦解犯罪集團組織，減少詐騙犯罪發生。





108 年詐欺車手查緝量能 研析及展望

刑事警察局打擊詐欺犯罪中心偵查員／邱之伶

壹、前言

打擊詐欺犯罪為本署當前治安工作重點，而查緝詐欺車手為近年掃蕩詐欺集團重要推行項目之一，現就 108 年查緝詐欺車手相關數據進行研析，以持續精進偵防作為，提升查緝成效，減少民眾被害。

貳、108 年查緝詐欺車手概況

一、108 年查獲詐欺車手 9,494 人次（唯一化人數為 4,450 人），較 107 年增加 2,114 人次（+28.64%），其中查獲現行犯和拘

提人數為 3,481 人次，占整體查獲人次 36.67%，復經法院裁定羈押人數為 1,191 人次，羈押率為 34.21%。

二、各直轄市、縣（市）政府警察局查獲詐欺車手人次，直轄市以臺北市政府警察局查獲人次最多、臺中市政府警察局次之、新北市政府警察局再次之，縣市以彰化縣警察局查獲人次最多、新竹市警察局次之、新竹縣政府警察局再次之。

三、108 年查緝詐欺車手總人次較 107 年有顯著成長，顯見警方查緝詐欺車手量能提升，持續壓制詐欺集團氣燄！

參、108 年詐欺車手數據研析

一、詐欺車手「年齡」分析：

查獲詐欺車手年齡以 30 歲以下為大宗，約占整體緝獲比例 72.61%，其中以 18 至 30 歲為主（占 59.08%）。

108 年詐欺車手年齡分析		
級距	人數	比例
18 歲以下	602	13.53%
18 至 30 歲	2,629	59.08%
30 至 50 歲	1,035	23.26%
50 歲以上	184	4.13%
總計	4,450	100%

二、詐欺車手「戶籍」分析：

查獲詐欺車手戶籍地前 5 名分別係新北市板橋區、桃園市中壢區、新北市新莊區、三重區及中和區，均分布在新北市西區居多。

108 年詐欺車手戶籍分析					
戶籍地（鄉鎮市區）	18 歲以下	18 至 30 歲	30 至 50 歲	50 歲以上	合計
新北市板橋區	18	60	32	8	118
桃園市中壢區	19	63	26	3	111
新北市新莊區	14	61	25	7	107
新北市三重區	13	50	32	7	102
新北市中和區	23	43	15	8	89
桃園市桃園區	17	45	19	2	83
桃園市平鎮區	25	36	12	1	74
臺中市北屯區	7	44	14	3	68
新北市汐止區	5	51	9	3	68
新北市新店區	7	31	20	4	62

三、詐欺車手「刑案紀錄」分析：

（一）108 年查獲詐欺車手 4,450 人，其中：

- 1、有毒品刑案紀錄者共計 928 人。
- 2、有三、四級毒品行政裁罰紀錄者共計 885 人。
- 3、有竊盜（含汽、機車竊盜）刑案紀錄者共計 468 人。
- 4、有組織犯罪防制條例刑案紀錄者共計 303 人。

5、有槍砲彈藥刀械刑案紀錄者共計 114 人。

6、有賭博刑案紀錄者共計 106 人。

7、有重大刑案紀錄（含故意殺人、強盜或海盜、搶奪、擄人勒贖、強制性交等）者共計 180 人。



108 年詐欺車手涉及其他刑案紀錄分析

案類	毒品刑案	毒品行政裁罰	竊盜	組織犯罪	槍砲	賭博	重大刑案
人數	928	885	468	303	114	106	180

(二) 詐欺車手「犯案次數」分析：統計分析詐欺車手每半年度累積犯案達 2 次者共計 933 人、達 3 次者共計 359 人、達 4

次者共計 123 人、達 5 次者共計 55 人、達 6 次者共計 16 人、達 7 次者計 4 人、達 8 次者計 2 人、達 13 次者計 1 人。

108 年詐欺車手犯案次數分析

犯案數	2 次	3 次	4 次	5 次	6 次	7 次	8 次	13 次
人數	933	359	123	55	16	4	2	1

四、詐欺車手「幫派」身分及「聚眾鬥毆」涉案分析

- (一) 108 年查獲詐欺車手 4,450 人，經分析具幫派列管註記者共計 135 人，占整體查獲人數 3.03%；曾參與聚眾鬥毆情事者共計 179 人，占整體查獲人數 4.02%。
- (二) 深入分析具幫派列管註記者，以具天道盟、竹聯幫及四海幫身分為多數，其中又以天道盟太陽會與天道盟正義會較多。
- (三) 深入分析有聚眾鬥毆紀錄並具幫派列管註記者，以具天道盟、竹聯幫、四海幫身分較多。

(-52.23%) 次之、屏東縣政府警察局減少 1,867 次 (-67.64%) 再次之。

- (二) 108 年查獲詐欺車手總人次較 107 年增加 2,114 人次 (+28.64%)，各直轄市、縣(市)政府警察局查獲詐欺車手人次以新北市政府警察局增加 501 人次 (+51.92%) 最多、臺北市府警察局增加 474 人次 (+38.73%) 次之、臺中市政府警察局增加 291 人次 (+23.72%) 再次之。
- (三) 108 年詐欺車手提款總次數較 107 年減少，查獲總人次則較 107 年增加，顯見警方偵防詐欺犯罪作為已見成效！

肆、提款次數及查緝量能研析

一、108 年與 107 年各直轄市、縣(市)政府警察局詐欺車手「提款次數」與「查緝量能」之比較分析：

- (一) 108 年詐欺車手提款總次數較 107 年減少 7,240 次 (-10.09%)，各直轄市、縣(市)政府警察局詐欺車手提款次數以臺中市政府警察局減少 5,477 次 (-33.16%) 最多、高雄市政府警察局減少 3,147 次

二、108 年與 107 年詐欺車手「提款時段」之比較分析：

108 年與 107 年詐欺車手提款時段高峰多分布於 0 至 1 時及 12 至 16 時，0 至 1 時提款次數較高可能與車手受限於每日提款金額上限，急於隔日再次提款有關；另檢視 108 年提款時段，1 至 4 時及 17 至 21 時之提款次數較 107 年上升，推論係因詐欺集團為分散風險而改變提款時段，本署將滾動式調整勤務，持續加強可疑人車盤查，防制詐欺車手刻意規避查緝！

詐欺車手「提款時段」比較				
提款時段	107 年 提款次數	提款時段	108 年 提款次數	增減率
0 至 1 時	6,215	0 至 1 時	5,239	-15.70%
1 至 2 時	833	1 至 2 時	1,016	21.97%
2 至 3 時	270	2 至 3 時	283	4.81%
3 至 4 時	94	3 至 4 時	104	10.64%
4 至 5 時	80	4 至 5 時	29	-63.75%
5 至 6 時	85	5 至 6 時	57	-32.94%
6 至 7 時	131	6 至 7 時	103	-21.37%
7 至 8 時	231	7 至 8 時	156	-32.47%
8 至 9 時	413	8 至 9 時	365	-11.62%
9 至 10 時	776	9 至 10 時	589	-24.10%
10 至 11 時	1,208	10 至 11 時	938	-22.35%
11 至 12 時	3,730	11 至 12 時	2,888	-22.57%
12 至 13 時	6,336	12 至 13 時	5,226	-17.52%
13 至 14 時	7,620	13 至 14 時	6,098	-19.97%
14 至 15 時	7,725	14 至 15 時	5,783	-25.14%
15 至 16 時	6,688	15 至 16 時	5,295	-20.83%
16 至 17 時	3,942	16 至 17 時	3,781	-4.08%
17 至 18 時	3,087	17 至 18 時	3,483	12.83%
18 至 19 時	4,341	18 至 19 時	4,800	10.57%
19 至 20 時	4,427	19 至 20 時	4,782	8.02%
20 至 21 時	4,602	20 至 21 時	4,750	3.22%
21 至 22 時	4,432	21 至 22 時	4,322	-2.48%
22 至 23 時	3,084	22 至 23 時	3,076	-0.26%
23 至 24 時	1,437	23 至 24 時	1,384	-3.69%
總計	71,787	總計	64,547	-10.09%



三、108 年詐欺車手提款地點分析：

檢視 108 年詐欺車手提款地點以銀行、便利商店及郵局為主，銀行共計遭提款 2 萬 5,449 次，占整體 39.43%、便利商店共計遭提款 2 萬 863 次，占整體 32.32%、郵局共計遭提款 1 萬 601 次，占整體 16.42%，其中銀行以合庫商銀、彰化銀行及華南銀行最多，便利商店則以統一超商及全家超商最多。

地點	次數
統一超商	9,715
全家超商	7,621
萊爾富超商	2,182
OK 超商	1,345
總計	20,863

地點	次數
合庫商銀	2,938
彰化銀行	1,955
華南銀行	1,714
第一銀行	1,480
玉山銀行	1,369
台灣銀行	1,344
國泰世華	1,234
土地銀行	1,147
中國信託	1,073
台北富邦銀行	975
總計	15,229

地點	次數
銀行	25,449
便利商店	20,863
郵局	10,601
農漁會	1,995
超市量販店	1,612
百貨公司	938
其他	792
醫院	749
捷運站	554
學校	408
政府機關	250
中華電信	110
遊樂場	88
火車站	72
高鐵站	57
休息站	8
機場	1
總計	64,547

伍、策進展望

一、針對詐欺車手集團案件加強溯源打擊

查緝車手可斬斷詐欺集團左右臂，防止民眾被害款項流向境外，為刨根溯源澈底掃蕩，遏止詐欺犯罪持續發生，本署將以查緝詐欺車手為基礎，向上溯源發展至集團核心幹部及幕後集團操控者，以強化打擊詐欺效能，根除詐欺集團。

二、攔阻金融帳戶以降低被害案件發生

詐欺車手取得金融卡並提領款項之時，即代表民眾已遭詐欺集團誑騙並將被害款項匯入詐欺集團指定金融帳戶，為阻斷詐欺車手取得此類金融帳戶，避免帳戶淪為車手提領贓款工具，本署逐步調整打詐行動方針，將詐騙、收購金融帳戶嫌犯及收簿手列為重點查緝工作，並與轄內超商、物流業者等建立聯繫管道加強配合，以提升偵破收簿集團量能，有效斷絕民眾匯入款項機會，降低詐欺案件發生。

三、掌控設籍轄內車手名冊預防再犯

詐欺屬高再犯性之犯罪型態，經分析 108 年查獲詐欺車手 4,450 人之犯案次數，犯案 2 次至 4 次間者共計 1,415 人、犯案達 5 次以上者共計 78 人，顯見詐欺車手有反覆實施詐欺犯罪之可能，本署將綜合分析車手間之相關性據以偵辦，並適時派員了解其動態以預防及約制再犯。

四、未成年及年長車手加強預防宣導

經分析 108 年查獲詐欺車手年齡 18 歲以下者共計 602 人，占整體緝獲比例 13.53%；年齡 50 歲以上者共計 184 人，占整體緝獲比例 4.13%，相較於 107 年查獲詐欺車手年齡 18 歲以下者共計 519 人，年齡 50 歲以上者共計 95 人，皆有些微增加趨勢；本署將針對利用假求職廣告誑稱工作內容為代收包裹或提領款項等相關涉犯刑法詐欺罪案例，透過勤區查察、社區治安座談會等面對面接觸方式實施宣導、關懷及犯罪預防，並持續呼籲青少年勿受金錢誘惑而遭詐欺集團吸收擔任車手，提醒年長者慎選工作內容避免遭詐欺集團利用，強調涉犯刑

法將面臨之刑責及高額賠償，以提高民眾警覺心，減少誤入歧途機會。

陸、結語

透過全體警察同仁一整年的辛勞努力，108 年查獲詐欺車手之成效有顯著成長，為持續壓制詐欺集團氣燄，本署將強化執行「偵防電信網路詐欺犯罪工作執行計畫」，除針對詐欺車手集團案件加強溯源以根除詐欺集團，並調整打詐行動方針，將詐騙、收購金融帳戶嫌犯及收簿手列為重點查緝工作，以遏制詐欺犯罪，降低詐欺案件發生，保障人民財產安全。





新修正洗錢防制法下的金融面向打擊作為

刑事警察局打擊詐欺犯罪中心警務正／王濟

壹、前言

我國於 85 年間即制定洗錢防制法，為亞洲地區率先通過洗錢防制法專法之國家。惟二十年來犯罪集團洗錢態樣不斷推陳出新，洗錢管道除金融機構外，更可利用不動產、保險、訴訟管道等方式洗錢，且歷次修正均以後階段之追訴犯罪為核心，未能建置完善洗錢防制體制，強化洗錢防制作為，建立透明化之金流軌跡與可疑金流通報機制等國際規範標準，致我國雖有專法，防制成效仍大幅受限。

隨著各國對於洗錢防制之重視日增，國際間金融活動往來日益密切，非法金流利用層層複雜的各種名目、態樣而移轉、分散至跨國不同據點，以形式上合法來躲避查緝，執法單位所面臨的被告，已非傳統個人被告，而係擁有龐大資金、法律專業團隊為後盾之犯罪集團。故國際間一再強調打擊犯罪除需查緝犯罪不法外，更應自阻斷金流著手，藉由金流透明化之管制及強化洗錢犯罪之追訴，才能澈底杜絕犯罪。

貳、刑法沒收新制之效益

過往舊刑法關於沒收之規定，對於沒收僅限於違禁物及被告犯罪所生、所用、所得及預備犯罪之物，適用之範圍極其狹窄，有關於犯罪所得之贓款查扣微乎其微，審判實務上亦常見法官將犯罪所得之返回視為量刑之重要依據；惟就歐美先進國家之沒收制度而言，犯罪所得本就應由國家所追償，並非犯罪嫌疑人可據以對國家刑期喊價之籌碼。

另囿於舊刑法之沒收規定，除違禁物之外，沒收之客體僅限於犯罪行為人本身，歹徒可以輕易藏匿犯罪所得至第三人處，躲避司法查扣與沒收。然而，105年7月1日實施之刑法沒收新制，可單獨對物宣告沒收，並可及於第三人，可有效防杜歹徒之藏匿資金行為，針對渠等所為之犯罪所得加以追徵抵償，似可大大提升追贓返回成效。

惟就當前偵辦實務而言，詐欺集團皆係以極細緻之分工，且從詐欺成員、金融帳戶、資通共犯至集團核心成員等處廣設斷點，各犯嫌間幾乎不認識，且僅以代號或通訊軟體聯絡，縱查獲直接從事詐欺犯行之正犯，並清查相對應之被害人連結指認，仍無法向上連結幕後核心成員，縱有些微之證據連結至集團幕後金主，亦難以證明其所詐騙之所有被害人之關聯性，就新施行之沒收新制，恐怕力有未逮，成效有限。

綜上，雖近年針對沒收不法財產及利得大幅修正相關法律，仍需靠警方突破偵查斷點、連結犯罪證據使得適用前開法律規定遏止犯罪。

參、金融帳戶為主要取財管道

目前電信網路詐欺案件受理數仍以ATM取款案件（主要犯罪類型為「取消分期付款設定」、「假網拍」、「猜猜我是誰」）為大宗。以近3年ATM取款案類受理比例分析，106年電信網路詐欺案件共受理12679件、ATM取款案件占11619件（91.63%）、107電信網路詐欺案件共受理12579件、ATM取款案件占11424件（90.82%）、108年電信網路詐欺案件共受理13246件、ATM取款案件占8418件（63.55%），足見人頭金融帳戶仍為電信網路詐欺案類主要取財途徑。如能致力降低歹徒得使用之金融帳戶數量，應可有效減少詐騙國人管道。

肆、人頭金融帳戶來源分析

目前人頭帳戶類型主要區分為「自願性人頭帳戶」及「非自願性人頭帳戶」性質分述如下：

一、自願性人頭帳戶

所謂自願性人頭帳戶，係詐欺集團以金錢或其他利益，向人頭帳戶申辦人買斷或租借帳戶，進而用於供被害人匯款之用，此類人頭帳戶，通常具有幫助詐欺之不確定故意，且成立「詐欺幫助犯」需負擔刑事責任，多係由車手集團自行向熟識之人，私下收購；被收購者多為經濟上較為弱勢者，雖知出賣帳戶之行為可能成立刑事犯罪，仍欲藉此換取現金，亦通常有多筆詐欺刑案資料紀錄，此類帳戶申辦人多係遭熟識朋友介紹或收購，可利用筆錄技巧使帳戶申辦人供出上手。



二、非自願性人頭帳戶

詐欺集團先於各大社群或報章雜誌，以「求職」、「代辦貸款」等名義散布消息，吸引不特定被害人，再以「辦理薪資轉帳」或「製造金流紀錄、提升信用額度」等話術，誘騙被害人將存摺、提款卡、密碼等，寄送至特定地點，進而提供詐騙集團使用，此類人頭帳戶提供者，因欠缺幫助詐欺之故意，並不會構成刑事犯罪，雖有財務之需求，亦不致多次遭此類手法詐騙，通常較無詐欺刑案資料，其詐騙金融帳戶模式如下：

- (一) 於 LINE、FACEBOOK 等社交群組，散布訊息並留下「LINE ID」。
- (二) 俟被害人加入詐欺集團的 LINE 群組後，以話術誘騙被害人，將存摺、提款卡、密碼等寄出至詐欺集團指定之處所（超商或物流公司收貨站），並回報詐騙集團。
- (三) 詐騙集團接收被害人回報後，遂指示「取簿交通」人員，前往領取包裹，並放置指定處所，賺取報酬。
- (四) 帳戶由騙簿之集團轉入提款車手集團，開始進行提領現金等後續行動。

另「租借帳戶」類型，歹徒係誣稱經營賭博網站，須向不特定多數人租借帳戶，以進行避稅，並約定每星期支付高額租金吸引不特定多數人將帳戶寄交予犯罪集團利用，歹徒取得帳戶後旋即利用於詐騙犯罪，此類帳戶申辦人多抱持租借帳戶予他人使用並非洗錢行為，俟帳戶遭警示後始向警方報案。

就目前警示帳戶通報設定速度及衍生性帳戶連動警示等機制觀之，縱同一申辦人將名下數筆帳戶提供車手集團作為犯罪之用，其

存活時間亦應短暫，然 ATM 取款案件仍屬大宗，除少數自願性販售金融帳戶犯嫌外，詐欺集團應係使用非自願性金融帳戶為主，就目前偵辦現況歹徒多係以「假貸款」、「租借帳戶」或「求職詐騙」等詐騙手法方式取得金融帳戶。

伍、預防作為

一、縮短通報設定警示帳戶時程

為能更有效率彙整 ATM 提款熱點資料，即時提供各單位查詢運用，目前將「受理案件至審核確認警示帳戶之時程」，列入「偵防電信網路詐欺犯罪工作執行計畫」，要求各單位落實辦理，以縮短彙整時效。經統計 106 年下半年，時效自前期的 4.69 天縮短至約 1 天。

二、建立詐欺案件金流異常指標

為即時防制民眾受騙，爰由刑事警察局分析相關詐騙案件之金流等特徵，並建立「異常交易指標參數」，於 106 年 9 月 19 日函請金管會及各金融機構配合辦理，對於帳戶交易行為符合前揭指標參數者，採取必要因應措施，以減少民眾受害損失。

三、強化防制「人頭金融帳戶」宣導

防制人頭金融帳戶宣導部分，主要推廣預防民眾交付存摺、提款卡給予詐騙集團做為人頭帳戶，於 105、106 年各警察機關即利用宣導活動、電子媒體、平面媒體、付費管道及警廣「防騙金鐘罩」、「安全停看聽」、「琇如十時樂」及「內政部空中服務處」等單元推廣反詐騙觀念，也製作淺顯易懂之圖檔透過 165 反詐騙 APP 等

管道宣導，呼籲民眾求職、借貸時遇詐騙集團利用話術騙取民眾交付存摺、提款卡等重要文件時，應提高警覺並嚴正拒絕，以期提升民眾防詐知識、降低被害案件發生；另於 107、108 年陸續製作假借貸及假求職等詐騙手法之宣導素材（例如警語、影音、廣播及新聞稿等），廣續運用各宣導管道（電子媒體、平面媒體、付費管道及警用管道等）託播，持續強化民眾對人頭帳戶刑責及詐騙集團取得手法之認識。

陸、查緝作為

目前查緝收簿手、攔阻金融帳戶業已列入 109 年上半年「偵防電信網路詐欺犯罪工作執行計畫」評核項目，各警察機關均依單位屬性，分配查處任務如下：

一、派出所、分局—攔截金融帳戶

深入轄區超商及物流公司收貨站，於第一時間掌握可能為金融帳戶之包裹，並通知寄件人釐清內容物，如確實為金融帳戶，即通知寄件人到場領回，避免淪為詐欺所用，並進一步詢問寄件原因（是否欲「辦理貸款」或「出租帳戶」）、廣告來源，以查知訊息散布管道、釐清是否為自願提供。

二、警察局、分局—查緝取簿交通、清查涉案帳戶申辦人

「取簿交通」犯嫌，同一人通常多次前往固定物流站領取包裹，警方僅能依前述非自願性人頭帳戶寄送地，調閱監視錄影畫面，循線查獲「取簿交通」犯嫌，以進一步釐清取得金融帳戶之上手共犯。

分局偵辦涉及帳戶詐騙案件，通知涉案帳戶申辦人到案說明時，應確實釐清是否為自願性提供，如為自願性人頭帳戶，應利用偵訊技巧使其供出收購上手、掮客及訊息散布管道，並向上追查實際出資收購者。

三、刑事警察局—查緝收購詐騙人頭帳戶者

詐騙人頭帳戶者皆係利用網路或社交軟體散布相關廣告訊息，如前述地區警察機關能盡速攔截金融帳戶釐清廣告來源、查獲取簿交通，即能於第一時間利用相關情資，擴大偵辦，查知詐騙人頭帳戶者。

柒、結語與建議

過往洗錢防制法，僅針對特定犯罪且涉案金額達新臺幣五百萬元以上之情形，始有適用，於現今斷點分明、分工縝密之犯罪模式下，殊難想像執法機關得由個案犯罪事實舉證符合前開構成要件；新修正洗錢防制法，除放寬前開本法適用限制外，更針對諸多金融機構、專業人士、特定行業課予洗錢防制通報義務，逐步修補我國防制洗錢機制，殊值肯定。

過往警察機關受理民眾遭詐騙金融帳戶，往往告知民眾「等帳戶遭警示後再來報案」，待數日後民眾帳戶遭歹徒用於詐騙他人，由其他警察機關為通報「警示帳戶」，民眾向原報案機關求助時，旋即以「詐欺犯罪嫌疑人」移送該報案民眾，完全忽略該民眾遭詐騙金融帳戶為刑法第 339 條第 2 項「詐欺得利罪」之被害人，明顯混淆民眾前階段遭詐騙帳戶及後階段民眾帳戶詐騙他人

之情形，民眾遭詐騙帳戶之情形，亦未獲警察機關之重視。

基此，藉由本次洗錢防制法之修正，分析我國詐欺犯罪之根源，嘗試提出因應對策，希藉全國警察機關量能大力截斷詐欺集團人頭帳戶來源，並宣導民眾如自願提供其所申辦之金融帳戶，供詐欺集團處理不法贓款使用以躲避警方查緝，即屬提供帳戶掩飾不法所得去向，而該當新修正條文第2條第2款之情形（洗錢防制法第2條立法理由三、（四）參照），以嚇阻民眾販賣自身帳戶之情形，冀能從源頭剷除不法。



電信詐欺話務機房之演進與趨勢

刑事警察局打擊詐欺犯罪中心偵查員／嚴泓元

壹、前言

電信詐欺犯罪擾亂國內金融秩序已久，綜觀近年電信詐欺犯罪案件及財損數雖已獲有效控制，惟仍無明顯下降趨勢。其中電信詐欺案類中以假冒機構（公務員）詐騙手法造成財產損失最鉅，主要透過詐欺話務機房搭配 VOS 或群撥系統行使詐騙話術，並以一、二、三線人員為基底架構，惟近期部分電信詐欺機房已轉向複合型詐騙方式、分散式機房等模式經營，以增加詐騙成功及降低遭查獲風險概率，摘要分析如下。

貳、演進與趨勢

一、複合型詐欺話務機房：

分析國內近期查獲詐欺機房案件，發現除了占大宗的假冒機構（公務員）詐騙手法外，部分假交友機房詐騙手法有轉型趨勢，犯嫌透過「賭博機房」及「金融平臺」（投資虛擬貨幣）等 2 種型式偽裝從事傳統話務詐欺機房之實，藉以規避詐欺罪責。

（一）架構剖析：

1. 通常由一線犯嫌（前端）擔任話務機房成員，盜用俊男美女圖片藉由交友軟體（網

站)或通訊軟體(LINE、FACEBOOK)結識被害人,透過溫情攻勢與被害人建立信賴或情侶關係。

- 嗣後由一線犯嫌介紹被害人加入賭博網站會員或投資平臺(虛擬貨幣),並引薦偽裝為職業投顧之二線犯嫌(後端),積極遊說被害人充值賭博網站或投資虛擬貨幣,俟被害人欲領回款項遭犯嫌迴避時方知受騙。
- 前揭話務機房遭警方查獲時,機房現場多佈置為從事博弈、投資之偽裝環境,犯嫌筆錄亦多供稱無從事詐欺情事,僅為受雇參與線上博弈或投資網站,規避刑法詐欺罪責。

(二) 案例說明：

以刑事警察局偵查第二大隊第一隊於 108 年 6 月 3 日偵破劉○軒等人涉嫌從事假交友詐欺機房為例。

1. 案情摘要：

(1) 機房組成：

本案係由嫌犯劉○源承租花蓮縣新城鄉 1 處民宅,並由嫌犯吳○航(金主)出資並申請前揭民宅之中華電信網路成立詐欺機房據點,分由一、二線成員(每線含幹部 1 名,成員 3 名)計 8 人進行假愛情交友話務詐欺機房。

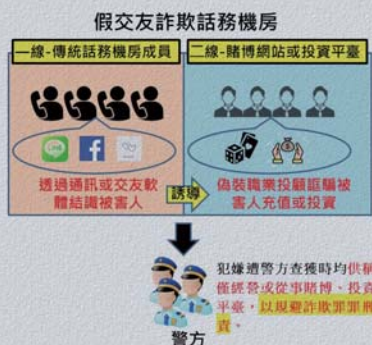


圖 1：複合（轉）型詐欺話務機房示意圖

(2) 犯罪手法：

A、詐欺機房一線話務成員透過「吾聊」、「FACEBOOK」、「LINE」等通訊軟體,以盜用俊男美女圖進行交友、戀愛徵婚(假愛情交友)等方式誘騙臺灣地區不特定被害人至 12BET 網站 (<https://b20.12-bet.com.tw/>)(<https://b26.12-bet.com.tw/>) 註冊會員,佯稱可投資獲利,並儲值新臺幣 1,000 元以上不等之金額至機房所有之虛擬帳戶內(以超商儲值或網銀轉帳)。



圖 2：12BET 網站截圖(為合法成立於亞太地區體育博彩、商城娛樂之線上博弈網站)

B、由詐欺機房二線成員擔任帶牌老師取信被害人，佯稱保證獲利誘騙被害人持續加碼儲值，俟被害人欲領回網站儲值或獲利金錢時，機房人員即以 LINE 訊息告知「洗碼量不足」等話術，或以對訊息已讀不回、不讀不回等方式致被害人獲知受騙並求償無門。

(3) 偵辦概況：

本案源於民眾向本局偵查第二大隊第一隊舉報友人在花蓮縣新城鄉工作賺錢，惟週間行蹤不明又難以聯繫，疑似為詐欺機房工作云云，經該隊現場勘查後發現該工作民宅確有諸多從事詐欺機房癥候，爰立案偵辦。

經長期蒐證，於 108 年 6 月 3 日持臺灣花蓮地方法院核發之搜索票執行搜索，現場查獲 7 名詐欺集團犯嫌，及後續清查約 20 名臺籍被害人，全案依刑法第 339 條、339 條之 4、組織犯罪防制條例第 3 條第 1 項及洗錢防制法第 14 條等罪嫌移請臺灣花蓮地方檢察署偵辦。

2. 建議應處作為

(1) 情資佈建

成立假交友詐欺話務機房仍需含括傳統之機房話務成員，因此機房處所成員必定具備一定數量，勘查機房現場仍具傳統詐欺機房癥候（如監視器眾多、窗簾緊閉、常由一人採買大量餐點或生活用品、極少人員出入、WiFi 流量大等），可透過宣導加強民眾認知對可疑鄰里進行舉報，建立警民聯防機制；或由轄區員警巡邏查訪進行情

資佈建。

(2) 專業支援

為避免犯嫌湮滅電腦數位跡證，偵辦詐欺機房屬本局主辦案件，執行搜索前應依行政流程會簽科技研發科；屬各縣市警察局刑事警察大隊偵辦案件，執行搜索前應會簽科技犯罪偵查組（隊）支援現場數位證物蒐證工作。

(3) 保全證據

A、電腦、隨身碟和行動電話等數位設備皆要編號造冊，以免遺漏。

B、電腦如裝有還原程式，未完成蒐證前請勿關機；另關機電腦切勿重啟，避免啟動還原程式致電腦資料遭刪除無法復原。

C、即時完成詐騙平臺（賭博網站、投資網站）內相關資料取證工作，避免遭遠端遙控關閉。

D、現場嫌犯持用行動電話必須先行開啟飛航模式，避免手機遭遠端刪除。

(4) 突破心防

經審視是類案件犯嫌筆錄，均以「負責推廣博弈平臺、不知在做詐欺機房」等語搪塞，規避事前從事假交友話務機房犯行，爰偵辦員警應著重詢問犯嫌實際從事一、二線等話務端之關鍵事證，俾供檢方據以起訴詐欺犯行；另可將現場嫌犯分別帶至旁邊單獨詢問，各個擊破，尋找關鍵幕後人物。

二、分散式詐欺話務機房：

傳統詐欺話務機房之話機須透過 Gateway 設備連結 VOS 系統，故均係採單一據點、集中管理模式經營。然隨科技進步，智慧



型手機 APP 即能取代 Gateway 功能，透過 SIP(Session Initiation Protocol) 設定使個人手機得以連線至 VOS 系統，機房經營者亦利用上開技術，採分散據點、縮小單點機房人數模式經營，以降低查獲風險及營運成本。

(一) 架構剖析：

1. 招募方式：

由掮客或詐欺機手仲介，藉加入 skype 或 Telegram 等通訊群組談論工作條件，後續加入由幹部（電腦手）開立之聊天群組開始工作。

2. 運行模式：

幹部（電腦手）每日傳送當天系統之 IP 和密碼，由居於自身住所或車上之詐欺機手自行設定座席，一線機手詐騙成功後按 #2 轉到二線機手，並用通訊軟體向群組內幹部報告，達成分散據點管控。

(二) 案例說明：

以刑事警察局偵查第六大隊第五隊於 109 年 1 月 14 日偵破蕭○儒等人涉嫌從事詐騙英國及澳洲華人機房為例。

1. 案情摘要：

(1) 機房組成：

本案係由嫌犯鍾○軒招募詐欺機手，於

臺中市及高雄市公寓大樓、屏東縣及南投縣民宿間游走，以一個禮拜為單位快速遷移躲避查緝，本案計查緝分散於 4 處之從事假冒機構（公務員）詐欺話務機房據點，各據點詐欺機手僅持用 1 支工作手機及私人手機，共計 5 名。

(2) 分散式機房特性：

- A、詐欺群組內幹部與機手間，均毋須碰面，未必知道彼此真實身分，查獲某一成員時，難以續行追查其他共犯。
- B、無集中管理及餐食問題，各自居住，外顯特徵與一般人無異。
- C、獲利由轉帳機房公司派人交付，集團幹部毋須出面。
- D、設備及網卡由詐欺機手自行準備，無統一購置。
- E、工作時間及地點彈性，甚至詐欺機手可以一次接兩個不同群組之詐欺工作。
- F、可能規避組織犯罪之刑責。

(3) 偵辦概況：

- A、本案源於刑事警察局偵查第六大隊第五隊偵破他案詐欺話務機房案，經該案落網嫌犯交保舉證指認後，爰立案偵辦。



圖 3：分散式詐欺話務機房示意圖

B、經長達 10 個月之跟監蒐證及通訊監察，於 108 年 1 月 14 日持臺灣南投地方法院核發之搜索票同步搜索 4 處詐欺話務機房據點，計查獲犯嫌 5 名及保全員 1 名。

2. 後續偵辦方向

由嫌犯扣案手機進行解譯，因分散式詐欺話務機房之電腦手（幹部）常透過 skype 等通訊軟體聯繫各處詐欺機手或傳遞被害人基本資料，爰應透過 WIRESHARK 軟體解析通訊軟體之聯絡人 IP，由 IP 續行追查遠端犯嫌位置；另是類詐欺話務機房常使用 Bria 軟體連線 VOS 系統竄改顯號詐騙民眾，可透過開啟 Bria 軟體之 SIP 設定確認連結

VOS 系統之 IP 位址，以 IP 反求其他連線至 VOS 系統之話務裝置擴大偵辦。

參、結語

伴隨資通科技演進，詐欺話務機房型態亦趨向細緻化分工執行，並盡可能規避詐欺罪、組織犯罪條例等罪刑，大幅提升警方偵辦是類詐欺機房案件之偵蒐難度，辦案人員除須與時俱進，時刻精進偵查技巧，亦仰賴第一時間控制犯罪現場之電腦雲端、手機硬碟等證據保全工作，俾後續解析及獲取數位證據提供檢方起訴參據，循序溯源提升案件質量，同步消弭詐欺機房產業鏈存續。



圖 4：分散式詐欺話務機房後續偵辦方向



遊戲點數詐欺案件 現況分析與偵防策進作為

刑事警察局打擊詐欺犯罪中心偵查員／謝政彬

壹、前言

近年來網路世界及手機科技的發展，帶動遊戲產業蓬勃發展，人手一機發展出人人均有遊戲帳號之現狀，但由於遊戲點數會員公司帳號管理未臻完畢，申請會員帳號僅以綁定個人電子信箱或聯絡電話等方式，未落實

使用實名制之申請方式，導致交付遊戲點數成為詐欺集團新興之取贓方式，以下就此案類之被害及財損數據、遊戲點數公司經營模式、犯罪手法與洗錢方式、現行預防機制及偵處困境、預行之策進作為等提出分析。

貳、被害及財損數據分析

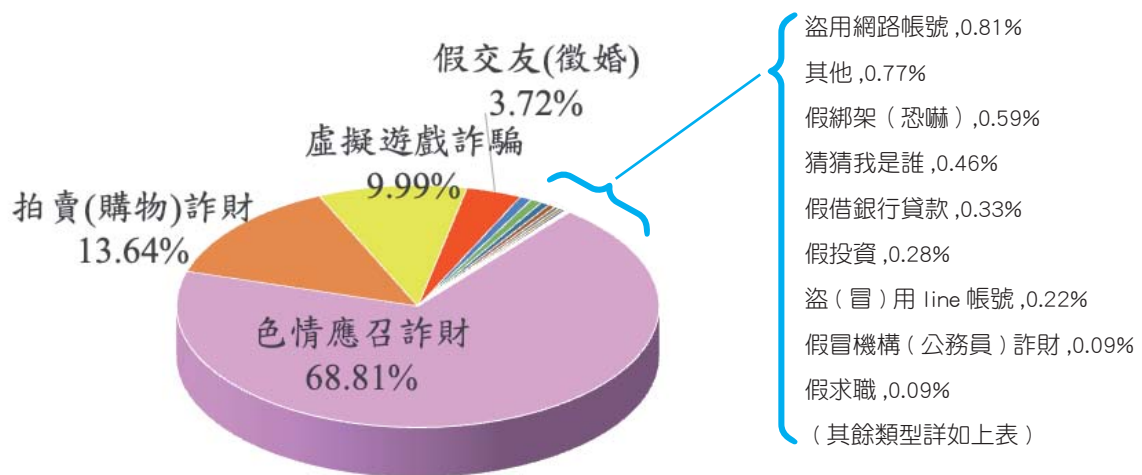
一、交付遊戲點數之詐欺案件發生數與財損數，顯示年年上升之趨勢

	106 年	占總案件 比例	107 年	占總案件 比例	108 年 上半年	占總案件 比例
件數	1,776	7.83%	2,356	10.04%	1,552	14.15%
財損	8,986 萬 3,202 元	2.22%	1 億 994 萬 5,230 元	2.77%	6,914 萬 9,824 元	3.93%

二、交付遊戲點數之詐欺案件手法中，以色情應召詐財為最大宗，拍賣（購物）詐財次之。

107 年	色情應召 詐財	拍賣（購物） 詐財	虛擬遊戲 詐騙	假交友 （徵婚）	盜用網路 帳號	其他
實體遊戲點數卡	3142	623	456	170	37	35
	68.81%	13.64%	9.99%	3.72%	0.81%	0.77%
假綁架 （恐嚇）詐財	猜猜我是誰	假借銀行 貸款詐財	假投資	盜（冒）用 line 帳號	假冒機構 （公務員）詐財	假求職
27	21	15	13	10	4	4
0.59%	0.46%	0.33%	0.28%	0.22%	0.09%	0.09%
假預付型消費詐財	中獎通知	假廣告	金光黨	假推銷		
3	2	2	1	1		
0.07%	0.04%	0.04%	0.02%	0.02%		

三、交付遊戲點數之重大詐欺案件中，以利用國外電子信箱申請遊戲帳號為主



統計 107 年被害人財損金額逾百萬元案件計有 7 件，此 7 件被害人共儲值 1,498 筆遊戲點數，除 2 筆直接儲值遊戲帳號外，其

餘 1,496 筆（占 99.03%）均儲值於 7 個境外電子信箱所申請之遊戲點數會員帳號，致使我國司法調查難伸。



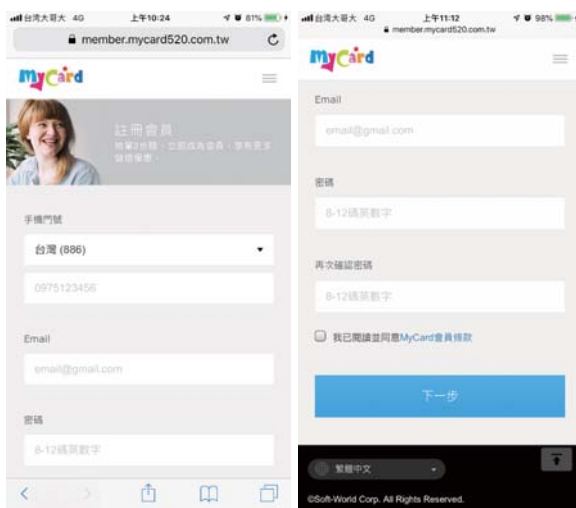
境外電子信箱	儲值筆數
****@126.com	235
****@163.com	1205
****@chacuo.net	39
****@qq.com	1
****@sina.com	11
****@sohu.com	4
****@yeah.net	1
直接儲值遊戲	2
總計	1498

參、遊戲點數公司經營模式

一、遊戲點數公司會員申請方式

以目前市面上最大通路之遊戲點數公司（智冠科技股份有限公司）為例（如下圖）

- （一）會員申請僅需留有收信功能之電子信箱、聯絡電話及建立密碼。
- （二）經申請後，系統會寄送確認信件至申請會員之電子信箱內。
- （三）點擊確認信件之連結網址即可開通會員帳號。



二、遊戲點數儲值方式

- （一）至超商或通路購買可儲值之遊戲點數卡儲值至遊戲點數公司之會員帳號。
- （二）線上信用卡刷卡付費儲值遊戲點數至遊戲點數公司之會員帳號。
- （三）透過遊戲公司提供之虛擬金融帳戶匯款繳費儲值。
- （四）目前各大超商及通路所銷售之遊戲點數卡，有智冠公司 Mycard、遊戲橘子公司 GASH 卡、紅心辣椒卡、台灣勁舞貝殼幣…等，經統計在各超商、賣場之通路所銷售的遊戲點數卡，以智冠科技股份有限公司的產品 Mycard 為最大宗，遊戲橘子數位科技股份有限公司的產品 GASH 卡次之。

三、可兌換為虛寶、金幣之遊戲平臺

遊戲點數公司統整目前市面上各種線上遊戲、單機遊戲、網頁遊戲、手機遊戲、影音娛樂、博奕休閒、數位加值、星座命理、交友社群、FACEBOOK 等，均可以扣除遊戲點數方式兌換該遊戲平臺之虛寶、金幣。

肆、犯罪手法與洗錢方式

一、以色情應召詐財手法為例，說明如下

- （一）詐欺集團成員利用美女圖像化名，利用網際網路在臉書、IG、LINE 等社群（通訊）軟體結識被害人。
- （二）詐欺集團成員透過聊天向被害人表示有兼職援交，並向被害人要求購買遊戲點數卡，拍照序號及密碼充當保證金。
- （三）詐騙集團成員於收到點數儲值序號時，再告知被害人為避免警察釣魚辦案，要求被害人再購買遊戲點數確認身分並完

成交易即可退回保證金，並持續要求開房費等費用。

(四) 被害人驚覺遭詐騙時，詐欺集團甚至冒充是幫派分子，致使被害人心生畏懼，而被迫持續買點數予以儲值。

(五) 警方於接受報案後，向遊戲點數公司調閱會員個資，僅有虛假個資及國外 IP 位址。

二、以網路拍賣詐財手法為例，說明如下

(一) 詐騙集團先以國外 IP 及虛假個人資料申請電子信箱，並向遊戲點數公司申請會員帳號及對應之虛擬匯款帳號。

(二) 詐騙集團在拍賣網站或 FACEBOOK 等社群交友網站佯稱拍賣商品，並以低於市價之方式吸引被害人。

(三) 詐騙集團提供遊戲點數虛擬帳號給予被害人匯款，被害人經匯款後，遊戲公司收到款項即將對應之點數儲值至詐騙集團申請之會員帳號內。

(四) 被害人收不到網路購買商品，向警方報案並提供當初匯款之虛擬帳號，警方經比對該虛擬帳號對應之遊戲點數會員資料僅有虛假個資及國外 IP 位址。

三、洗錢方式

(一) 遊戲點數代儲

詐騙集團自被害人騙取遊戲點數儲值序號後，即儲值至其利用境外電子信箱所創立之遊戲點數公司會員帳號內，再於網路購物平臺以折扣代儲遊戲點數之方式販售給予不知情之遊戲玩家，藉以將非法所得之遊戲點數轉為與不知情玩家間之合法交易現金。

(二) 購買遊戲平臺金幣、虛寶

詐騙集團於取得遊戲點數後，即在點數公司所配合之遊戲平臺內扣點購買虛寶、金幣，再透過遊戲玩家之間私下交易，藉以換取現金。

伍、現行預防機制及偵處困境

一、預防機制

本局預防科為加強防制遊戲點數詐騙案件，目前已實施下列相關反詐騙措施。

(一) e-PLAY 平臺銷售監控系統(108 年 1 月 14 日上線)

透過與智冠公司協商，建立 e-PLAY 智遊網數位銷售平臺，讓商家與該公司建立連線，針對購買點數情況異常之買家進行監控，並即時回傳智冠公司，該公司再聯繫店家與警方，攔阻遭詐騙之款項。

(二) 國內外會員身分重新驗證(108 年 2 月 18 日起實施)

針對所有遊戲點數公司會員進行重新驗證電子信箱及聯絡電話，增加帳戶確為正常玩家使用之比例。

(三) 黑名單預警機制(108 年 2 月 18 日起實施)

由遊戲點數公司針對國外會員帳號進行交易監控，若有儲值點數異常之帳戶，再實施人工比對，加以凍結該帳戶之遊戲點數儲值。

(四) 關懷提問彈跳視窗(108 年 4 月 8 日上線)

銷售通路店家於使用智冠公司 e-PLAY 智遊網數位銷售平臺結帳時，若有買家購買點數情況異常時，畫面上即彈跳顯



示關懷提問視窗，提供店員詢問買家購買點數之用途及反詐騙宣導。

經統計上揭關懷提問彈跳視窗上線後一個月，涉及智冠公司 Mycard 點數詐騙件數下降達 31.33%，顯示該公司所採相關作為，確見初步成效。

(五) 統一超商多媒體機臺及交易聯單提高反詐騙警語識別度(108 年 5 月 14 日上線)

被害人在使用超商多媒體銷售平臺購買點數時，在機器購買畫面上及條碼帳單上，顯示反詐騙警語視窗或打印警語在紙上，確保民眾能及時回心轉意，免受詐騙。

二、偵查困境 - 遊戲點數公司會員無實名制

縱然本署針對以交付遊戲點數詐欺犯罪實施相關之預防措施，然而犯罪發生數仍無法抑制，探討警方於查緝此類案件，均礙於遊戲公司對於申請會員方式，僅以電子信箱及電話註冊，詐騙集團只需要虛造個資利用境外 IP 申請註冊境外電子信箱，即造成警方查緝上極大困難。

陸、策進作為及成效

一、透過院級跨部會平臺會議，將遊戲點數納入洗錢防制範疇，建立會員帳號實名制

依據洗錢防制法第 5 條第 3 項第 5 款規定「其他業務特性或交易型態易為洗錢犯罪利用之事業或從業人員」，遊戲點數公司所發行之遊戲點數確有易為詐騙集團利用為洗錢犯罪之工具，實有納入規範之。

鑑此本局打擊詐欺犯罪中心已向法務部檢察司提出將遊戲點數業者納入洗錢防制法之範疇，使遊戲點數公司對於會員申請及點數交易，負有客戶實名登記審查、交易紀錄保存及申報疑似洗錢或資恐交易案件等義務，藉以阻卻詐騙集團洗錢管道，增加其犯罪成本，並強化警方偵查上游之能量，迫使詐騙集團不再選擇以被害人交付遊戲點數的方式進行詐騙，方有效根絕此類詐欺案件。

二、與主管機關經濟部工業局及遊戲點數業者研商差別化儲值機制，禁止境外會員帳號儲值國內實體遊戲點數卡

經本局 165 詐欺被害數據統計涉及交付遊戲點數之詐欺案件，99% 係被害人購買國內通路所販售之遊戲點數卡儲值境外會員帳號，本局打擊詐欺犯罪中心與遊戲業者兩大龍頭智冠科技公司、遊戲橘子公司接洽研商，針對儲值國內發行點數卡之境外帳戶實施重新認證及停權等作為，108 年下半年起被害數據逐步下降中。

柒、結語

交付購買遊戲點數已成為詐騙集團取代現金轉帳交付之新興犯罪工具，亦造成被害人極大財產損失，本局除持續推行管理法制化外，並積極與遊戲業者研商防制作為，方能有效遏止此類詐欺犯罪之發生，還給正當遊戲玩家一個優質乾淨的網路遊戲空間。



創新預防解除分期付款 詐騙策略 - 以國內外指標電商成功案例說明

刑事警察局預防科偵查員／林奕辰

壹、前言

依據 2018 年資策會 (MIC) 調查顯示，臺灣使用智慧型手機或平板電腦進行網購的民眾高達 64.9%，其中更有高達 95.5% 的網友習慣透過電商平台網路購物；且依據經濟部 108 年統計，網路電子購物業在上半年營業額為 970 億元、年增率高達 6.6%，顯示電子商務產業的蓬勃發展，一旦電子商務業者蓬勃發展後，詐騙集團可以竊取用來進行解除分期付款詐騙的資料來源也跟著增加，是故解除分期付款詐騙手法為將來防制詐騙之重點項目。

刑事警察局（以下簡稱本局）165 反詐騙諮詢專線（以下簡稱 165 專線）統計，自 103 年起，「解除分期付款」件數呈現逐年上升趨勢，案件發生數自 1 萬,1445 件，逐年上升至 105 年為最高峰之案件發生數 1 萬,5220 件，但經本局多年努力，解除分期付款件數逐年下降，至去 (108) 年已下降至 6,954 件，顯見本局之防制作為奏效（如圖 1）。



圖 1：解除分期付款歷年案件數

貳、現況分析

一、手法分析

165 反詐騙諮詢專線統計分析被害人調查筆錄，被害人均稱接獲客服人員來電，因內部作業人員疏失誤設定成批發商、團購或分期付款，如要變更設定須前往自動櫃員機(ATM)解除，俟被害人聽從指示前往操作後方始驚覺受騙。依被害人所言，歹

徒明確掌握其所購買之商品、金額、付款方式以及連絡電話，故研判歹徒先行取得各拍賣購物平臺消費者資料後，再施以詐騙詐騙被害人。

二、問題現況

因解除分期付款案件層出不窮，經分析目前問題如下：

(一) 僅顧商譽不願坦承漏洞

業者雖增加網站資安維護成本，惟作業系統(瀏覽器)的漏洞、程序撰寫的錯誤或管理人員的疏忽，及民眾所使用個人電腦或智慧型手機未能即時更新或遭植入後門程式，均為資料外洩之因素。另業者通常為維護自身商譽，一般不願對外公開坦承，網站或簡訊之反詐騙宣導內容仍多以宣示性宣導內容為主，恐未能有效提高民眾警覺(如圖 2)。



圖 2：本局函業者反詐騙宣導範例內容與業者實際刊登內容差異

（二）歹徒隨機攻擊應變不足

歹徒以隨機方式對不特定網路賣場資安漏洞實施攻擊並竊取個資，業者經常以個案看待且因應時間短暫，失去防範未然之先機。

（三）物流管道多元素質不一

因現今物流管道多樣且競爭，而勞力密集之工作型態使從業人員素質參差，於貨品配送過程中可能故意或過失致使民眾個資外洩。

（四）民眾依舊欠缺反詐意識

經訪談多數被害人表示，多因歹徒能夠詳述其所購買物品之時間、金額及配送方式等，使其誤信確為客服人員而前往操作 ATM；另問是否曾接獲反詐騙相關訊息，民眾表示曾有接觸過，但因當下未留意，導致接獲電話時仍遭詐騙，顯見仍有不少民眾欠缺防詐意識。

三、執行策略

本局積極整合各方資源，提升偵防能力，針對當前解除分期付款詐騙手法，透過下列措施積極創新改善，藉以降低民眾被害損失：

（一）新增公布系統商

彙整高風險電商業者解除分期付款詐騙案件，透過官網（內政部警政署 165 全民防騙網）、臉書粉絲專頁（165 反詐騙宣導）、LINE（165 防騙宣導）及警政服務 APP（闢謠專區）發布「民眾通報高風險賣場平臺」，讓消費者知悉，接到詐騙集團假冒平臺中公布之電商業者來電時，應慎防詐騙；另自 108 年 4 月起除每週公布電商業者外，更公布系統商業者讓民眾知悉。

（二）修正簡訊及郵件範例

將原先寄送電商業者參考之提醒簡訊及電子郵件範例修正，彙整各類詐騙話術

及微調內容以符合各電商業者之需要。

（三）訂單完成簡訊宣導同步

主動函發國內主要電商業者，落實完成交易後，由系統寄送提醒簡訊或電子郵件予交易完成之客戶，並彙整各詐騙話術提供各電商業者之參考依據，藉以強化提醒消費者慎防詐騙之成效。

（四）出貨遮蔽個資及提醒

要求各電商業者除在出貨包裹遮蔽個人資訊外，亦於出貨包裹上加註提醒防詐騙警語，以減少民眾被害情形。

（五）出席公會防詐叮嚀

主動出席中華民國電子商務領袖早餐會議及中華民國無店面零售公會舉辦之「新舊時代下的詐騙、個資外洩因應策略」座談會，會議中要求參與電商業者落實內部資安防護。

（六）精簡作為表以符需要

就寄送電商業者之「電子商務業者防制詐欺作為自檢表」進行修正，並把類似措施合併、精簡或刪除不合時宜的措施。

（七）確立聯繫窗口避免混淆

修正由權責所需單位與電商業者聯繫，假若業者質疑各縣市警察局員警身分真實性等問題，本局會協助查證，並作為他單位聯繫確認之窗口。

（八）強化受理詐騙案件建檔

新 165 受理系統中，將受理「解除分期付款詐騙案件」的「冒用機構」列為必填輸欄位，更通報各縣市警察局，要求於系統中「案情描述」欄位登載被害人購買區間。

（九）新增電商個資判決案例

將違反個資法判例（勝訴及敗訴判決）製作成案例說明及圖表提供電商公會參辦，由電商公會提醒所屬業者。（如圖 3）

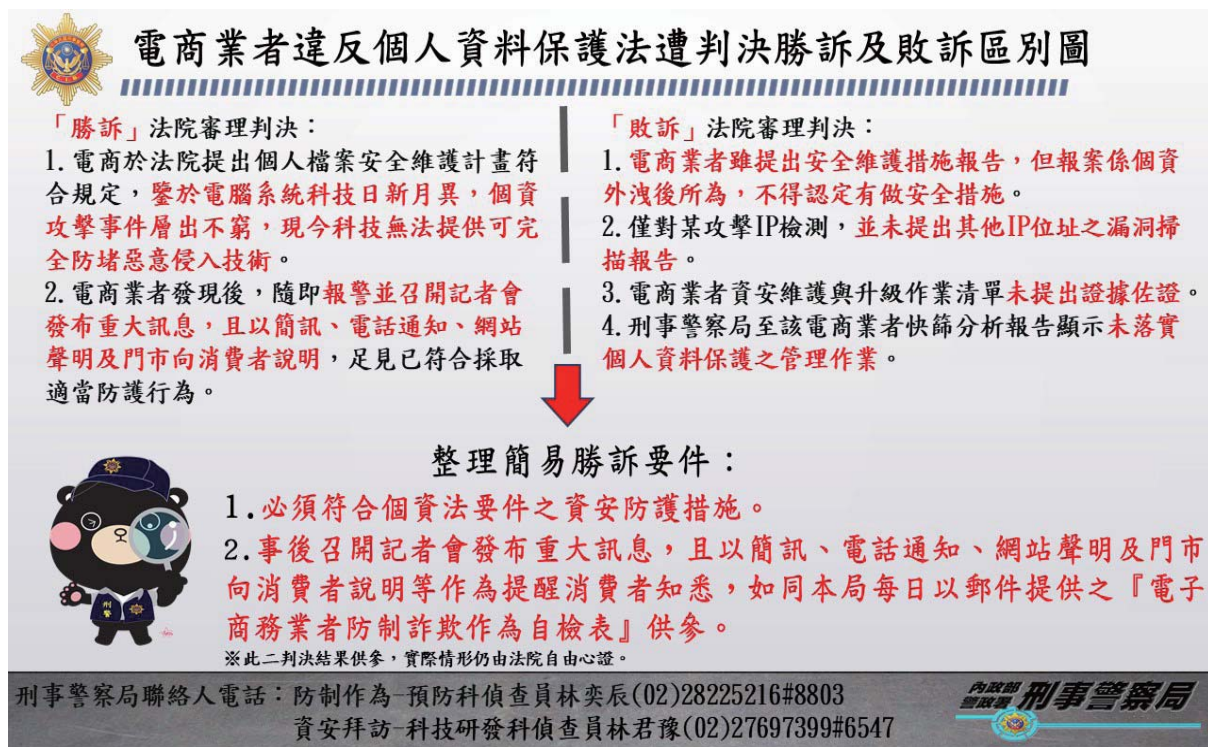


圖 3：本局函業者違反個資判例簡述圖

(十) 發布新聞約束電商

針對不配合防制措施之業者，使用發布新聞稿之方式，透過媒體力量，期以約束相關電商業者。

參、國內外電商指標案例分享

特別介紹國內指標電商業者（錢櫃 KTV）及國外指標電商業者（Booking 訂房網），經本局配合該公司特性，研擬及採取創新防制作為，具有顯著成效，分享如下（如圖 4、5）：

一、國內指標電商案例（錢櫃 KTV）

(一) 問題說明

自 108 年 10 月起，本局發現全國受理「解除分期付款」詐欺案類，該電商有急遽升高之趨勢，旋即密切關注並與業者保持聯繫，惟經業者於官方網頁放置反詐騙文宣及發送 4 萬封會員通知信

後，10 月份被害發生數仍未趨緩。究其原因，由於該電子商務業者寄送電子報或會員通知信過於頻繁，民眾多將上開信件直接移至垃圾信件區，甚至直接封鎖來自電商業者之信件，致使未能充分發揮提醒功能，效果不彰。

(二) 執行策略

1. 訴諸媒體

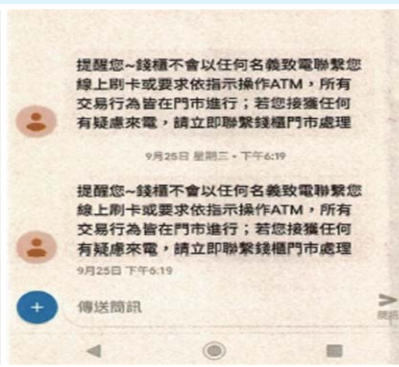
為遏止被害案件數發生並強化民眾防詐意識，本局於 108 年 11 月 18 日主動發布新聞稿並接受媒體採訪，以喚起國人防詐意識；錢櫃公司亦參照本局所提供之建議，針對個資被害區間再次寄出提醒簡訊及透過 APP 推播（寄出提醒之前後時段避免寄送廣告信件，以免影響提醒效果），該公司日後另行開發新型 EDM 系統，由系統自動判讀未開啟提醒防詐通知之被害客戶，再度發送提醒簡訊以達到提醒之效果。

錢櫃 KTV 防詐宣導作為

宣導圖文



提醒簡訊



宣導影片



圖 4：錢櫃業者防詐宣導作為

2. 視業者營業特性規劃宣導

本次與錢櫃公司密切聯繫溝通並採行多元化防制管道後，該業者在本局之建議下，充分利用該公司之特性，於訂位系統中彈跳巨型視窗提醒顧客，更於顧客至各門市消費時，於包廂歌曲影片中播放宣導影片，當該業者實施上述防制作為後，經觀察被害發生數趨勢，發現自隔月起案件開始下降，顯見相關因應對策已漸收成效，然而，後續效果仍為觀察重點。

二、國外指標電商案例 (Booking 訂房網)

(一) 問題說明

本局於 108 年 4 月透過民眾檢舉、諮詢及被害後，就立即以電子郵件、電話聯絡 Booking (訂房網) 公司均未獲積極回應，於 5 月起多次函文 Booking (訂房網) 公司臺灣分公司，建議 Booking (訂房網) 臺灣分公司善盡企業責任，並於網站首頁明顯處加註具體之反詐騙宣導標語及客服聯繫電話，延長客服接聽時間，以簡訊及電子郵件等方式通知

貴公司之消費者注意防範，並針對消費者個人資料安全維護 (含系統商) 進行重複檢測，但均未獲該公司立即回應。

(二) 新創處置策略

因 Booking (訂房網) 公司為外國公司，經專人聯繫臺灣分公司，該分公司表示在臺灣之據點僅為客服中心，故本局採用創新作為，透過第三方警政之力量，於 108 年 10 月 6 日主動發布「知名訂房網疑資料外洩，會員慘淪詐騙集團提款機」新聞稿後，獲聯合報、蘋果日報、自由時報 3 家平面媒體，台視、TVBS、中視、中天等 4 家電子媒體及 14 家網路媒體報導，總計 21 家媒體報導，呼籲民眾慎選資安防護機制完善之電商業者，保障民眾個資安全，深獲民眾響應，而迫使該公司主動透過駐外警察官協助聯繫本局，並與該公司透過視訊會議之方式進行討論，針對網站提出「遮蔽個資安全機制」、「確認外洩來源」及「防詐宣導」等 3 大面向之改善建議，如下所述 (如圖 5)：

Booking(訂房網)防詐宣導作為

宣導圖文



圖 5：Booking(訂房網)業者防詐宣導作為

召開視訊會議



1. 遮蔽個資安全機制

Booking(訂房網)公司於視訊會議後表示已於108年10月17日停止提供系統商消費者個人資料及電話號碼，以防止詐騙集團竊取冒用，本局將賡續追蹤各縣市警察局陸續陳報之案件是否有依規定登輸及調查相關資料後，後續彙整提供該公司協助調查個資外洩來源。

2. 動員警力調查外洩源

本局整理所有被害案件，並請各縣市警察局補足調查被害人之訂房序號、電子郵件等資料，去識別化後交由Booking(訂房網)公司協助分析後，該公司以電子郵件回復本局表示，個資外洩來源為臺灣系統串接商「Traiwan」。

3. 彙整情資以利偵辦

本局協調整合Booking總公司、臺灣系統串接商「Traiwan」及「LINE PAY」，彙整出18組IP及123組虛擬帳號(對應實體帳號46人)移送偵查第九大隊偵辦，以利瓦解幕後詐騙集團。

4. 個資外洩防詐宣導

本局除協助系統串接商「Traiwan」至本局報案追查幕後詐騙集團，更要求該串接商針對個資被害人寄出提醒簡訊6萬9,594封，以提醒被害人，避免後續被害。

肆、結語

現行科技日新月異，電子商務業者如雨後春筍般蓬勃發展，然而所伴隨衍生之詐騙案件亦層出不窮，未來除賡續透過「媒體」、「廣告」、「專題演講」、「活動」及「網路」等5大宣導管道，並運用分眾宣導之策略，強化反詐騙宣導深度及廣度外，另為機先預防詐騙案件發生，參照108年之創新預防解除分期付款作為(前述「錢櫃KTV」及「Booking(訂房網)」之案件偵處及防制措施)，推廣至各大電商，俾利業者標竿學習，即時啟動防詐機制，以提升公司資安，維護民眾權益。



電信詐欺恐嚇犯罪趨勢 與查處策略

法務部調查局經濟犯罪防制處犯罪預防科科长／吳榮修

壹、查處現況

電信詐欺恐嚇犯罪案件，雖經執法機關強力查緝，但不法集團仍持續招募無知年輕人加入及擴大其勢力，傳授經驗技術，並轉移陣地流竄於境外，向世界各地不特定民眾施詐，此種不法犯罪模式輸出，引起國際關注，遭諷稱另類不名譽的「臺灣之光」¹。

為有效遏阻電信詐欺恐嚇犯罪，法務部將其列為「檢察機關排怨計畫」優先查緝案件，要求全力打擊及掃蕩，並與內政部、金融監督管理委員會等機關組成「反詐騙聯防平臺」，跨部會密切合作查緝、宣導及預防²。臺灣高等檢察署於106年9月26日召開「如何強化偵辦跨境電信詐欺犯罪案件」專案會議，達成「偵辦此類犯罪，應採系統

1 參見105年4月19日聯合報A14版民意論壇，作者游其昌暗諷，臺灣的電信詐欺集團1年可創下5百億元「業績」，是傲人的「臺灣之光」；106年5月29日聯合報A2版焦點新聞，有檢察官接受媒體採訪時，痛批跨境電信詐騙集團犯案不斷，使臺灣淪為詐騙王國，嚴重損害國際形象。



附表 103-107 年各地方檢察署辦理電信詐欺恐嚇案件統計情形

項目別		103	104	105	106	107	年
新收案件數		8,287	10,981	18,152	27,182	35,100	件
偵查終 結人數	起訴被告人數 a	6,739	8,024	13,351	17,738	20,659	人
	不起訴處分被告人數 b	5,464	6,940	9,187	12,868	15,916	人
	其他 c	4,870	6,024	10,934	16,152	21,298	人
	合計 a+b+c	17,073	20,988	33,472	46,758	57,873	人
	起訴人數比率	38.8	37.7	39.5	37.5	35.3	%
裁判確 定人數	被告判決有罪確定人數	4,964	4,961	5,660	9,509	11,369	人
	被告判決無罪確定人數	294	297	438	531	654	人
	其他	115	73	108	195	305	人
	定罪率	94.4	94.4	92.8	94.7	94.6	%

性連結，朝組織性犯罪偵辦，並藉由各單位通力合作，向上溯源，加強查緝贓款流向，以瓦解犯罪集團³」之共識。依 107 年法務統計年報資料顯示，各地方檢察署 103 年至 107 年間，每年新收電信詐欺犯罪案件數、起訴被告人數，均以 107 年為最多，分別為新收案件數 35,100 件，較 106 年增加 7,918 件，增加率高達 29.1%；起訴（含緩起訴處分）被告人數 20,659 人，較 106 年增加 2,921 人，增加率達 16.5%。（如附表）⁴至於 108 年 1 月至 11 月之統計資料則為新收案件 32,512 件，起訴被告人數 19,612 人。⁵

貳、犯罪演進趨勢

參酌近期電信詐欺恐嚇案件犯罪模式，發現不法集團自行研擬因應查緝對策，其機房、帳務水房之設置更具機動性，甚至轉向境外，並以新式通訊軟體聯繫各地車手取款。該類犯罪最值得注意的發展趨勢，是朝向更加嚴密的組織，以及更為細緻的分工，檢警調機關之查緝將面臨更嚴峻考驗，茲析述如下：

一、吸收年輕成員，充當基層人力

不法集團利用年輕人涉世未深、亟需經

2 法務部 107 年法務統計年報，法務部統計處，108 年 8 月，iii，頁 4-6。

3 106 年防制經濟犯罪執行會報，臺灣高等檢察署工作報告，參見法務部調查局 106 年經濟犯罪工作年報，107 年 12 月，頁 11-12。

4 同註 2，表 2-2。部分項目數據為筆者參考相關統計資料後，自行加總整理而成。

5 法務部法務統計分析：電信詐欺恐嚇案件辦理情形統計分析，法務部全球資訊網，109 年 1 月 16 日發布，圖一、表 1，頁 1-2，數據為筆者參考相關統計資料後，自行加總整理而成。

濟收入等弱點，透過年輕族群互比炫富等招搖心態，大量招攬成員，以服從即有錢賺之集體行動管理方式，誘騙年輕成員參與，近期查獲之案例中，擔任車手及第一線假冒身分人員，多為年輕人。

二、犯罪分工精細，成員各司其職

電信詐欺恐嚇案件，其集團內部之組織分工，多以單線領導方式，運用層級管理，使不同分工層級成員互不認識，避免曝光被抓風險。大致分為集團首腦、組織核心幹部，下設前端的「電信及網絡組」（主要負責架設通訊設備、移轉機房技術；口條佳或具有特殊語言專長者，則負責撥打電話），以及「金融組」（處理帳戶及各地車手匯回款項、隱匿贓款）與「車手」（多由剛入行者擔任，前往各地領款）。⁶

三、拓點擴張勢力，助長跨域合流

近幾年，臺灣籍與大陸籍不法分子聯手於境外各地設置機房，詐騙臺灣、大陸或機房設置地區人民財產。因為通訊科技快速發達，以及交通往來便捷，加上拓點擴張勢力效應，無形中促進各地不法集團因覬覦共同利益而加速跨域合流⁷。

四、犯罪遍地開花，影響危害加劇

依查獲案例顯示，由於兩岸執法機關強化打擊不法，詐騙集團乃將觸角伸向更多週邊國家、地區如東南亞等地，甚至複製經驗，形成遍地開花⁸。此類跨境犯罪漸成趨勢，不僅危害人民財產，更對政府形象造成無可彌補的傷害。

參、檢警機關因應變革之查處策略

電信詐欺恐嚇集團跨境異地犯罪，涉及與當地國執法人員情資分享、合作及管轄權等爭議，且詐騙機房經常更異地點，其核心領導階層多隱匿幕後，直接證據蒐集不易，又水房處理金流迅速且有斷點，境外追贓困難，成果亦有限，增添許多查處難度。⁹

在檢警機關查處策略方面，宜採行預防與偵辦並重方式。在預防作為方面，充分運用公私部門資源，結合媒體強力傳播宣導，往下扎根至村里及中小學生，並深入民間社會基層，以提醒民眾避免受騙。在偵辦作為方面，添購高科技器材設備，監控特定區域內之電信流通，即時發現異常；精進金流網絡分析能力，針對列管可疑分子行蹤及資金往來不定期查察，從中追查不法及溯源；強化

6 楊士隆、陳順和合著，海峽兩岸電信詐騙機房防制對策之研究，頁 29 三、294；收錄於張凌、袁林主編，國家治理現代化與犯罪防控－中國犯罪學學會年度論文集（2015 年），中國檢察出版社，104 年 10 月。

7 孟維德，組織犯罪跨國蔓延之分析，涉外執法與政策學報第 9 期，中央警察大學外事警察學系暨研究所，108 年 5 月，頁 20、21。作者認為：經由人口遷移、人流增加、資訊與通信科技精進、經濟全球化，為跨國犯罪提供機會，尤其是與當地不法集團合作共同牟利，更有助於犯罪行為之開展。

8 汪子錫，從輿論分析兩岸合作打擊電信詐騙犯罪的成效與今後展望，展望與探索，第 12 卷第 5 期，103 年 5 月，頁 37。

9 時延安、敖博合著，中國大陸跨境電信網路詐騙的現狀及主要法律問題，月旦裁判時報第 87 期，108 年 9 月，頁 98。作者認為，海外追贓主要難題為：1. 快速分贓，去向不明。2. 難以證明錢款屬於電信詐欺所得。3. 與境外金融機構間聯繫管道匱乏。4. 與境外法域權責機構之協調配合尚待加強。



公寓大樓管委會及鄰里區域守望相助觀念，注意地方上進出可疑人車，如運搬大量通訊或資訊設備、臨時住居多人卻門戶深鎖、單純住家卻採購大量食物及民生日用品，或以低負擔、國外旅遊兼打工等招攬年輕族群或失業者等。另外，電信詐欺恐嚇案件被告再犯率高，可運用大數據科技分析模式¹⁰，串連相關資料庫系統¹¹，蒐集歸納該等被告特定時間內之入出境資料、ATM 提款機使用熱點¹²、特定親等內財產增減異動狀況等相關數據資料，從中過濾分析，機先防制犯罪。

肆、結語

筆者認為，不法集團採取人海戰術或是類似游擊戰方式，到處招兵買馬及機動轉移機

房，確實增添許多查緝困難。面對現實環境挑戰，各司法警察、檢察機關及相關政府部門，應暢通指揮體系及加強橫向聯繫，切勿為求績效短利，而有本位主義、搶功等情事，致影響查緝成果。然而，此類狡詐型犯罪集團泯滅人性，只為滿足個人私慾享樂，卻已造成各地民眾鉅大財產損害，形成治安隱憂。因此，世界各國應以查緝海盜、人口販運或毒品之模式，嚴肅面對此問題，共同研擬因應對策。

就筆者所見，加重刑事制裁，研訂合宜的刑事法令，是遏止電信詐欺恐嚇犯罪擴張惡化的良藥，再輔以強力查緝跨境犯罪組織，以及加強兩岸與各法域間互助合作，讓犯罪行為人無法遁逃，則是最有效的防制策略。

10 許華孚、吳吉裕合著，大數據發展趨勢以及在犯罪防制領域之應用，刑事政策與犯罪研究論文集第 18 集，法務部司法官學院，104 年 11 月，頁 361-365。作者認為，運用政府機關相關統計資料，可得知過去幾年犯罪案件、犯罪趨勢、受刑人特性等資訊，藉以預測犯罪者特性，預防可能的犯罪，以減少社會危險，並及時提出最適切的防制對策。

11 臺灣高等檢察署籌建之「反電信詐騙資料庫」，於 107 年 8 月 15 日正式上線。

12 108 年 10 月 17 日聯合報 B2 版高屏澎東要聞：屏東縣警察局利用大數據分析 ATM 提款熱點，在特定時段加強巡查，於 7 月 1 日至 12 日配合專案行動，查獲疑似車手 64 件 127 人。



運用第三方警政策略阻斷 詐欺集團網路及電信管道

刑事警察局偵查第九大隊偵查員／王靖欽

打擊詐欺犯罪一直是刑事司法體系的重點工作，本文從分析詐欺犯罪的手法找出打擊的標的，之後透過 PDCA 的品質管理，改善打擊策略，並結合第三方警政的方式進一步將詐欺犯罪從源頭進行消弭。

眾所周知，刑事司法體系在打擊詐欺犯罪部分，耗費非常多的人力、時間，曾有檢察官說：「車手到處提款、到處犯案，警察動用相關人力抓到車手之後，移送到檢察署，檢察署得配置相對應的人力來偵查，起訴後法院也要配置相對應的人力來審判，但車手是到處提款，所以有可能全國的刑事司法單位都得花費相同的人力、時間來針對同一個車手，所以很容易就將刑事司法體系癱瘓，但詐欺犯罪依舊未見被壓制」。因此找到詐

欺犯罪的「死穴」，從源頭就阻斷詐欺的發生，所耗費的成本將會遠低於在詐欺犯罪發生後才進行的各種刑事司法手段。

壹、現況分析

阻斷詐欺案件的發生，除了透過預防宣導來減少被害外，另一方面就是從加害人端實施相關手段，如提高犯罪成本或減少犯罪工具等著手，但因為各類型的詐欺犯罪手法不盡相同，因此本文先對 108 年 1 月 1 日至 10 月 10 日的詐欺犯罪手法做分析並以圖表方式呈現。從圖 1 可見，「假網拍」類型的詐欺犯罪佔了約 24%，在各類型詐欺犯罪中排名第一位。

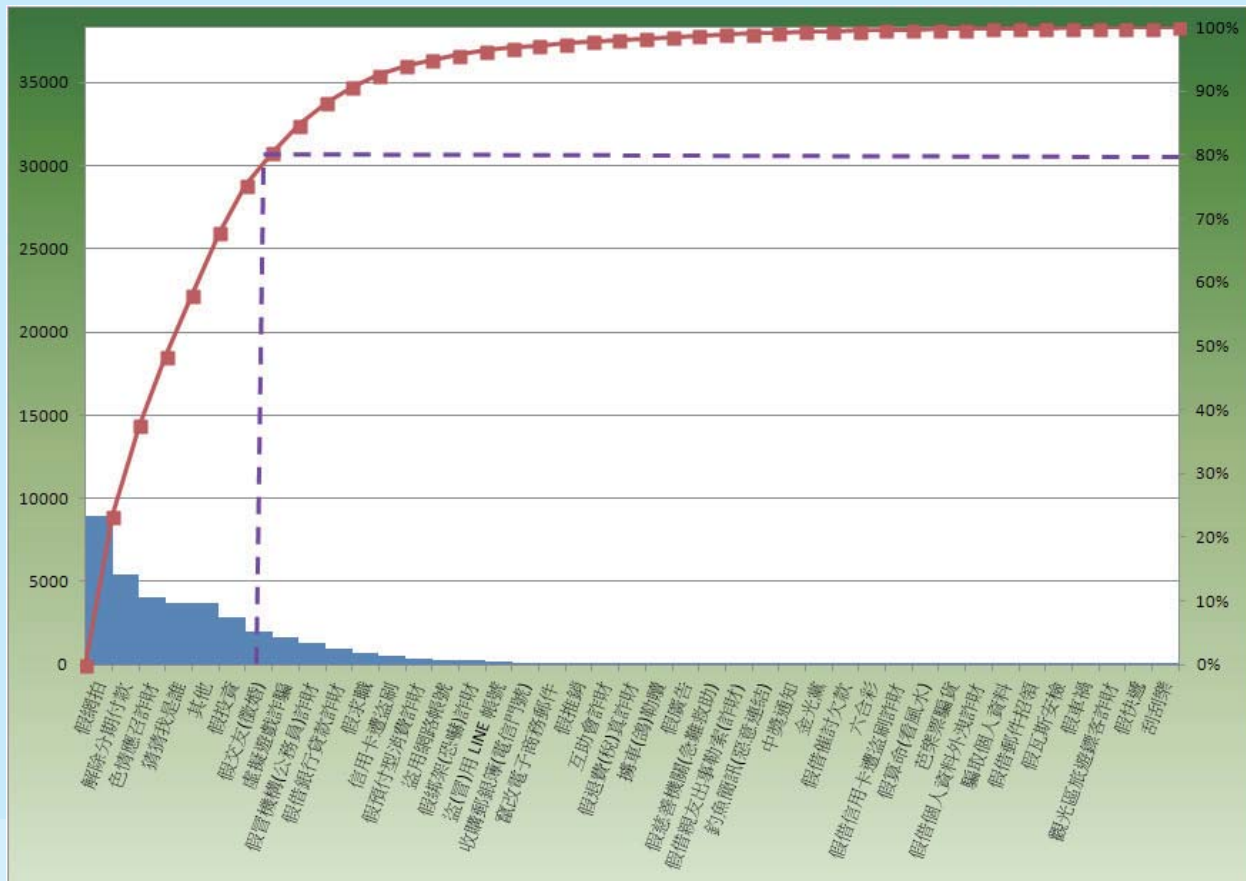


圖 1：各類型詐欺犯罪所佔比例 (108年1月1日至10月10日)

從「假網拍」類型的詐欺犯罪再進行拆解，發現這類犯罪一定有個「帳號」來參與並實施詐騙行為，這個「帳號」可能是「網拍網站」的帳號、「通訊軟體」的帳號或是「社群網站」的帳號，這些帳號均有一個特點，除了使用一個名稱或電子郵件註冊後，還需要提供一個行動電話門號，目的是讓網站發送包含認證碼簡訊到該用於註冊的行動電話門號，讓註冊者在網站上輸入認證碼來核實身份。對網站或 APP 而言，這樣的認證方式除可以減少個資的收集，同時也方便進行會員管理，一般而言，註冊自己的帳號當然是用自己申辦的行動電話門號，因為後續的帳號管理等都與此門號有關。舉例而言，我們

不會跟隔壁同事借他的門號來註冊一個社群網站，隱私是一個問題，日後萬一忘記網站密碼，需要門號接收臨時密碼，便得向當初借用門號的人詢問，這非常不合常理，想當然地，也不會有人願意出借自己的門號來協助他人做這樣的認證。

承前所述，借門號進行註冊帳號是很不合理的事，但在偵辦「假網拍」的案件中，我們發現這些參與犯罪的帳號所綁定的門號可能是「外籍人士」申辦（俗稱外勞卡），或是來臺旅遊的陸客所辦，但最大宗的卻是以公司名義申辦的門號，因此深入探討「門號」跟「詐欺犯罪」之間的關係。當一般民眾覺

得借「門號」給他人認證很奇怪，卻是犯罪者認為最好的「斷點」。分析帳號註冊流程可發現，很多註冊資料都可以捏造，例如隨意申請電子郵件信箱，假造相關個資，但到最後一個步驟用門號收取認證碼時，卻無法任意編造出一個門號來，因為編造出來的門號無法收到認證簡訊，因此犯罪者就會結合「簡訊認證商」來協助完成註冊帳號。

「簡訊認證商」通常是資本額不高的公司，申請註冊成立公司後，便以企業名義向電信公司申請「企業門號」，能申辦門號的數量基本上是依照公司資本額來限制，但如果客戶能預繳資費時，電信公司便可能放寬能申請門號的上限，因此一家資本額極低的公司便能申請上千個門號。當犯罪者想註冊用來犯案的帳號時，就向簡訊認證商申請門號來做綁定，簡訊認證商就會代替犯罪者收取網站發送的簡訊，並回傳簡訊，讓犯罪者完成帳號註冊，日後該帳號犯案，警方循線查到門號申請人時就會查到門號所屬的公司，如果警方查調相關資料，差一點的公司會說當初不知道是誰買的註冊服務，好一點的公司會回復簡單的個人資料，但警方無法核實這些資料的正確性。「簡訊認證商」就此成為犯案帳號的保護傘，也是最佳的防火牆。

「帳號」在「假網拍」等詐欺犯罪裡扮演很重要的角色，而「門號」是產出「帳號」的關鍵，圖2係以心智圖方式呈現「門號」衍生出的各類詐欺犯罪。先從圖2的「網拍詐騙」說起，使用行動電話門號註冊網拍帳號後，犯罪者便可以開始張貼銷售物品等被害人上鉤，或者在貼文上留下「加LINE：(ID)詳聊」等語，俟被害人加LINE後便在LINE上實施詐騙；另外當有兩個以上的假網拍帳號時，犯罪者就以「左手賣給右手」的方式製造假交易，目的是為了產生出貨用的「交貨便」條碼，這些條碼在日後會提供給「自願」寄出存摺、提款卡等的被害人，讓他們到超商的機臺印出「交貨便」條碼後寄送，這就是「取簿交通」的上游。而當門號註冊了遊戲平台的帳號，這個遊戲帳號就能拿來儲存透過各種方式騙來的「遊戲點數」，帳號儲存了點數再透過相關平台出售變現，或是利用帳號進行虛擬寶物的交易詐騙。而各式通訊軟體也需要綁定一個門號，所以當透過簡訊認證商認證一個通訊軟體後，即可使用該服務，例如註冊了一個LINE帳號，這個LINE帳號就能拿來實施詐騙，當詐騙得手後還能刻意將相關訊息回收讓被害人無從舉證。最後門號還能拿來註冊社群平台，例如：FACEBOOK，這樣的社群帳號除了用來張貼販售商品的「釣餌」文章外，也能在平台上實施詐騙，更甚者拿這些大量的假帳號來按

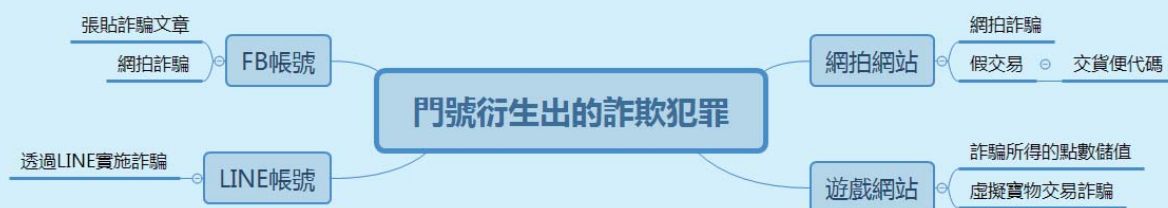


圖2：門號與各類詐欺間的關係

讚、發文，美其名叫「衝人氣」，實際上就是帶動輿論風向。而當一個門號「竭盡」註冊帳號的價值，將能註冊的帳號都註冊完畢後，下場有兩種，人頭卡的部分轉到「猜猜我是誰」的詐騙，俟門號被通報詐騙後停話，門號就完成參與整個詐欺的生命週期，而企業門號的部分，就會被「簡訊認證商」向電信公司要求換號，待取得新門號之後，又開始實施相關帳號的註冊。由此可知，一個「門號」其實和很多種樣態的詐欺案件息息相關，反過來說，我們只要設法斬斷門號與帳號之間的關係，相關的詐欺便有可能被抑制。

透過「簡訊認證商」取得註冊帳號，建立資訊面的斷點後，詐欺集團再把目標轉向建立通訊面的斷點。因為帳號的使用還是得透過網路來實現，倘若使用過程暴露所使用的網路(IP)位址，還是有可能遭緝獲，因此詐欺集團開始使用各式種類的VPN(虛擬私人網路，俗稱「翻牆」)，有的使用APP版本，有的為求穩定向「網路公司」購買類似的服務，透過VPN就能隱藏所使用的網路位址，增加警方追查的難度；而警方向這些服務商調閱相關資料時，也都無法確認、核實這些資料的正確性。所以，詐欺集團在資訊面、通訊面上建立斷點後，讓警方的查緝更顯困難。

貳、擬訂計畫(Plan)

根據上述分析能發現「門號」與「VPN」是網拍詐欺中的關鍵，也是詐欺環節中最易被警方掌握之處，因此犯罪者才需要大費周章地想辦法設置斷點，所以只要將這層斷點除去，犯罪者將失去「門號」所建構出來的各類型詐欺犯罪，而因為「VPN」的中斷，

則必須暫時停止相關的詐欺活動，直到找到新的「VPN」服務為止。

然而，盤點警方針對「門號」與「VPN」所能使用的法令，實在少得可憐，似乎也欠缺明確的「主管機關」來加以管制、約束，即使警方針對這類公司聲請搜索票、拘票，但移送檢方後，大多數是以「不起訴處分」作結，縱然獲得「起訴」處分，卻無主管機關可以實施後續相關管制作為。

所以，除了採取「刑事手段」來查緝外，後續作為應該再引入其他行政、私人公司等等的支援，以第三方警政的方式一起來打斷詐欺所依賴使用的「門號」及「VPN」服務，方能從源頭阻斷，讓詐欺案件不再發生。

參、執行(Do)

在偵辦網拍詐欺案的過程中，本大隊從查調的資料裡找到兩家公司，一家名稱為「立○科技」專門提供「VPN」服務，另一家名稱為「銳○資訊」專門提供簡訊認證，這兩家公司在案件紀錄裡均排名第一，意味著當前發生的網拍詐欺大都透過這兩家公司來製造資訊面、通訊面的斷點。和以往相同，本大隊透過實施強制處分查扣相關設備，當時查扣狀況如表1。

先前多數案件都止於搜索並查扣完相關犯案工具，進一步能做的頂多是將人頭卡停話，但透過這些門號註冊的帳號依舊能夠活動；在發現該種情況後，本大隊在刑事相關作為實施後，開始透過第三方警政的方式以澈底去除犯罪工具。

斷源專案	執行時程	
	第一波	第二波
時間	5月28日	6月17日
地點	臺中市	嘉義鄉
嫌疑人	林○○	李○○
公司名稱/資本額	立○網路科技公司 50,000元	銳○資訊公司 100,000元
查扣物品	查扣電腦6臺、行動電話2支、筆記型電腦1臺、網路交換器9臺、金融卡1張及光纖網路等證物	行動電話SIM卡3713張、手機16支、存簿1本、電腦主機5臺、筆記型電腦1臺及數據機池8臺等證物

表 1：強制處分執行成果

在提供「VPN」服務的部分，本大隊依照相關的會議決議函請「國家通訊傳播委員會」來認定「立○科技」是否有「非二類電信事業但卻實際從事二類電信業務」之情況，加以審查、裁罰。

而從事簡訊認證的「銳○資訊」，本大隊依據該公司的門號管制表，清查出門號曾註冊過的網站、遊戲、社群平台，隨後發文至前述公司，請渠等針對綁定查扣門號的帳號進行「重新認證」，目前多數網站都有「重新認證」機制，如使用者忘記密碼透過「重新認證」以簡訊發送暫時使用的密碼，或是帳號更換綁定的門號亦需要重新認證、或是臉書發現使用者登入異常，會要求使用者接收認證簡訊並到平臺上輸入以完成驗證。簡言之，「重新認證」就是讓網站再發送一次簡訊到帳號當初認證的門號，並要求帳號持有人回傳簡訊內容，藉此核對身分的過程。

根據前述機制，能夠完成「重新認證」的帳號，表示帳號持有人同時也擁有這個門號，因此這部分不會有爭議；反之無法認證者，表示帳號持有人當初應是找「簡訊認證商」

代為認證，這部分的帳號就會因為無法取得認證而失效。

在進行「重新認證」的過程，本大隊獲得所有網站的支持，這些公司也苦於函復大量的查調函件，但卻想不出方法來有效降低龐大的查調數量，甚至得僱請更多人力來回應警方等調查單位的函查，因此獲得遭查扣門號資料後，各公司便立即實施「重新認證」，也希望能除去潛在的「查調對象」，降低公司的人力成本。最後，本大隊於 108 年 7 月底前完成與相關行政部門及私人公司的合作。

肆、效果確認 (Check)

為了確認「透過第三方警政策略打詐」的成效，便以 165 反詐騙系統中的「被害件數」當作是觀察指標，預期在相關的作為實施後，每天遭網拍詐騙的件數應該逐漸減少。

根據實際數據顯示（圖 3），5 月 28 日搜索「立○科技」後，假網拍被害件數微幅下降，但很快就恢復之前的水平，推測應是有很多替代廠商或軟體可提供相同的「VPN」服務，詐欺集團可以馬上找到備援方案。



圖 3：108 年 5 月到 8 月詐欺（假網拍）被害件數

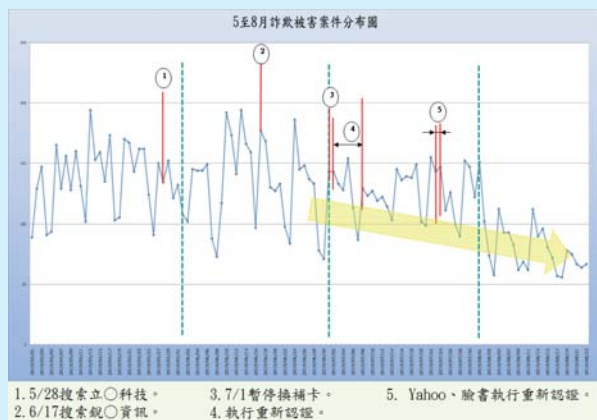


圖 4：108 年 5 月至 8 月 詐欺被害案件分布圖

同時，可以發現在實施「重新認證」的措施後，7 月的被害件數和前兩個月相比，已經收斂到每天 30 件以下，而到 8 月更降低到每天 23 件不到的狀況，顯見相關的作為具有成效。

另外從詐欺被害案件分布圖（圖 4）來分析，7 月的被害件數和前兩個月相比，已經收斂到每天 150 件以下，而到 8 月更收斂到每天 100 件以下，顯見除了假網拍詐欺案件數下降，一些與「門號」有關的其他類型詐欺犯罪也隨之下降，證明了透過第三方警政方式，從源頭打擊詐欺犯罪，的確能獲得實際成效。

伍、後續行動 (Action)

從實際案件進行分析，發現「門號」、「VPN 服務」是某些詐欺犯罪，尤其是網拍詐欺的「死穴」。而實施一連串的防制措施後，也確實讓詐欺案件發生數下降，但可能僅限於個案。原因是多數時候，偵查人員不會知道發函查調回來的企業門號，係來自「簡訊認證商」或是「VPN 服務供應商」，而且縱使查知，也暫無相關法令能予以管制。

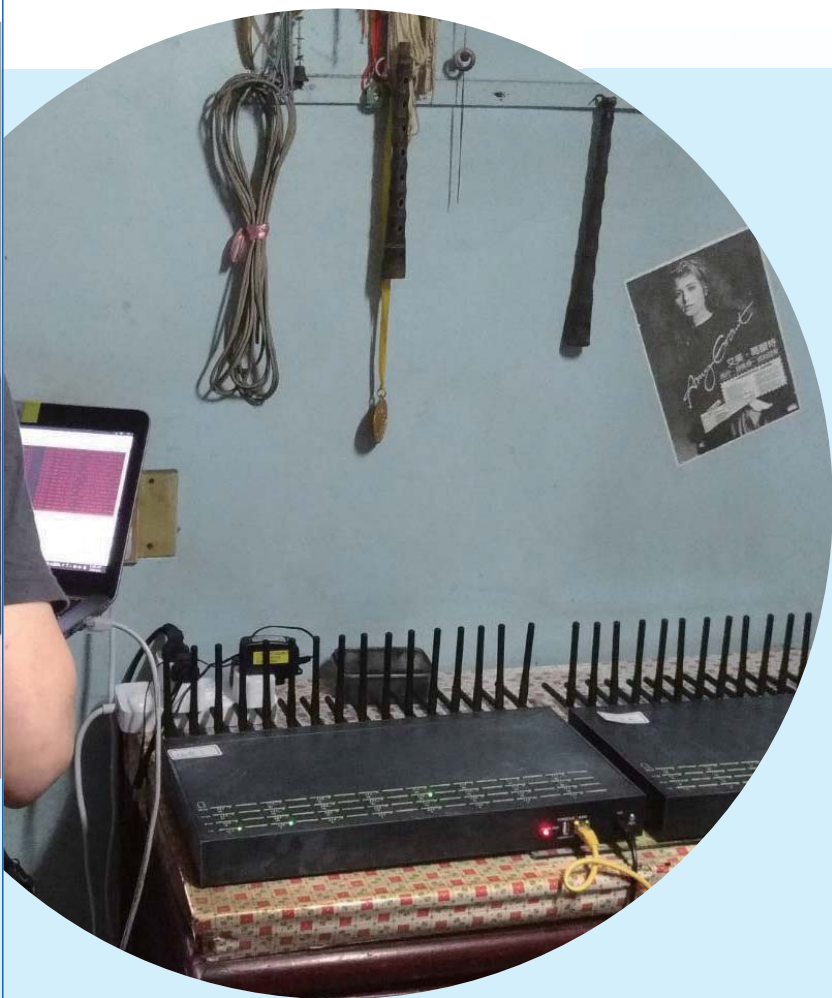
此外，前述願意協助「重新認證」的公司，

即是參與「第三方警政」的伙伴，如有意願續實施「重新認證」，目前也缺乏相關平臺或機制可供運用，倘若能建立類似平臺或機制，警方等調查人員於日後查扣人頭電話後即能上傳，願意加入「重新認證」平臺的公司就能收到相關的資料，主動執行「重新認證」，同時這些公司也能藉由相關數據加強會員帳號管理，如同銀行管理金融帳戶般，將帳號分成各種風險等級，依據不同風險等級實施不同頻率的「重新認證」，若能落實執行是項作為，相信能更進一步將「門號」有關的詐欺犯罪予以消滅。

陸、結語

以「第三方警政策略」來打擊詐欺的作法雖然奏效，也意味著相關法令的不健全，好比「VPN」服務至今尚未有明確的主管機關，任何人願意花錢租用電信公司網路服務後再加以包裝就能販賣「VPN」服務，讓這些販賣 VPN 服務的公司或個人就像網路裡的雜草，氾濫蔓生而成為滋生犯罪的溫床。

至於門號管理的相關規定也付之闕如，目前大多數的網站要求會員註冊時提供門號，是因為這些網站都認為門號就是代表著會員本身，好比使用信用卡消費時，銀行會發送「OTP」，(One Time Password) 到當初申辦信用卡所留存的門號，目的是希望透過門號來核實使用者，而「簡訊認證商」的出現及存在卻讓這種認證機制形同虛設，甚至還大放厥詞地以「服務」為由，企圖掩飾其行為所衍生的後續亂象。唯有從管理面及法制面著手，刑事司法體系才不至於繼續耗費更多資源，亦可避免相關的詐欺犯罪不斷循環發生。



偵辦猜猜我是誰手法「數位式移動節費設備」 (Digital Mobile Trunk) 詐欺話務機房案實務研析

刑事警察局電信偵查大隊偵查正／鄭信良

壹、前言

隨著科技進步、行動網路速度變快及網路電話普及，詐欺集團犯罪模式演變為網路遠端監控、境外化及隱匿性更高等特性。本局分析國內近期發生之「猜猜我是誰」詐騙案件，犯嫌以亂槍打鳥方式撥打電話給國人，佯裝成多時不見好友或親人，並以生病、周轉不靈…等短期間內急需借款等話術進行詐騙，根據 165 反詐騙諮詢專線（以下稱 165 專線）受理民眾報案（諮詢）猜猜我是誰手法詐騙案件犯罪模式分析，並以民眾進線檢舉犯

嫌發話詐騙所用且尚未遭斷話之門號，調閱分析門號通信紀錄，發現詐欺集團指揮在臺犯嫌承租日租套房或旅館，做為設置非法「數位式移動節費設備 (Digital Mobile Trunk，以下簡稱 DMT)」場所，由境外詐騙集團收購國內人頭門號插入 SIM 卡管理器設備後，用網路電話方式撥入在臺 DMT 設備，就能以國內行動門號顯示發話取信國人，再以猜猜我是誰手法詐騙民眾匯款，後續民眾回撥詐欺集團持用門號時，發現已經停話始知受騙報案，使得眾多國人蒙受財產損失。

貳、詐欺機房演變趨勢及犯罪模式

詐欺集團一開始以人工親自撥打電話予詐欺被害人，後為規避警方查緝，開始將詐欺話務機房設置於境外，以招待出國旅遊、償還債務及打工賺錢…等為由，誘騙或招募機手至境外機房，並以 VOS 網路電話將門號竄改成政府機關或金融機構（中華電信、地檢署、健保局…等）代表號後撥打，將話務送至國內以詐欺國人匯款或面交款項給車手。

除將話務機房設於境外，另因科技發展及行動上網速度提升，亦有至當地招募犯嫌尋找日租套房或商務旅館，架設 DMT 設備透過寬頻網路或 4G 行動網卡使用臺灣之行動電話門號為主叫號碼，但實際的發話者位置在境外，被害人接聽電話後回撥求證時，會透過 DMT 設備將話務以網際網路傳送至境外機房接聽以躲避查緝；另亦發現有將 DMT 設備設置於自小客車上定時移動，企圖增加警方查緝困難。

詐欺集團使用 DMT 設備發送詐欺話務用意在於下列各點：

- 一、提高詐騙成功率：詐騙機房假冒被害人親友詐財，會先向被害人謊稱已更換電話號碼，使用 DMT 設備發送詐欺話務時，可供回撥電話取信被害人。
- 二、製造國內發話假象：政府為保護國人協調電信業者將自境外送至國內之網路電話號碼開頭強制顯示「+」，藉以提醒民眾提高警覺；詐欺集團為取信國人及降低警覺性，取得人頭門號後在境外發話透過 DMT 設備顯示號碼，形同在臺灣以行動電話發送話務一樣，民眾根本難以察覺。

三、降低詐騙成本：因詐騙國人的機房多設置於境外，跨境發話費用較高，利用 DMT 設備發送之詐欺話務，跨境時以網路語音技術傳遞話務，可節省犯罪成本。

近來猜猜我是誰手法犯罪模式，大多是由詐欺集團負責電信話務的主嫌以社群媒體、報紙徵才…等管道刊登工作機會，以協助大陸電信業者代管電信設備或伺服器為由，招募急需金錢或工作之人，將 DMT 等相關設備透過國際貨運寄送給求職者，主嫌再以通訊軟體指揮求職者至預訂好的日租套房擺放設備，再用遠端軟體設定網路環境及 DMT 設備，確認正常運作後，便提供詐騙機房開始從境外發話詐欺國人，主嫌大約 2 至 3 天後會請求職者取回設備至下一個日租套房或商業旅館，再重覆上述犯行。

參、偵辦手段

以偵辦葉姓嫌犯 DMT 詐欺話務機房案為例，先報請檢察官專案指揮偵辦，並分析調閱 165 專線受理通報國人遭猜猜我是誰手法詐欺案件之發話門號通信紀錄，依據門號發話基地台位置、發射角等資訊，先確認話務機房在新竹市後，並輔以行動電話即時定位搭配偵搜器材，發現 DMT 訊號來自於一棟大樓內，警方原地埋伏觀察出入人員，發現進入人員進入前大多看著手機確認並拖著行李箱，判斷該棟大樓為日租套房，屋主到場以為警方要查緝日租套房，還一直否認，辯稱是正常租屋；經過一番溝通後屋主才坦誠整棟是知名租屋網的日租套房，最後找到確切 DMT 設備發話訊號源，再循監視器畫面調得葉嫌駕駛車輛確認身分，但葉嫌才剛於 1 天前架設好相關設備，因此，警

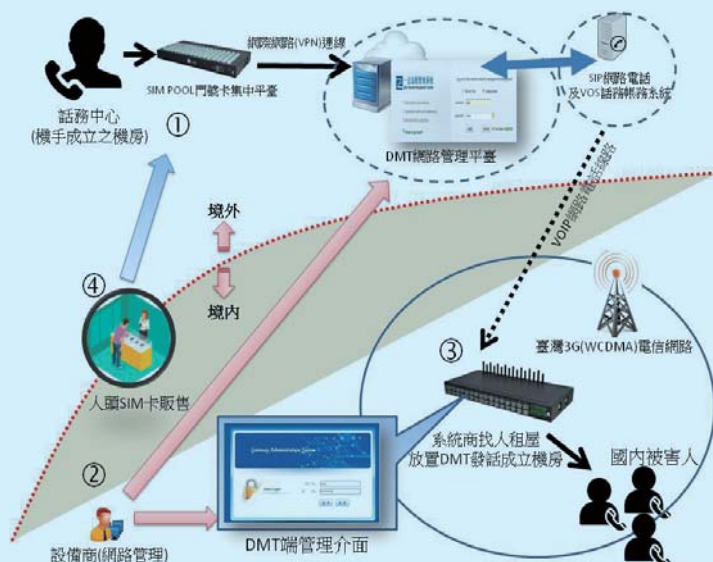
方向屋主承租隔壁房間，經埋伏 3 天才等到葉嫌來取回 DMT 設備，準備前往臺中另一處日租套房架設，警方當場查獲並扣押 DMT 設備等犯罪證據，並根據行車紀錄循線破獲葉嫌在桃園架設之 DMT 機房。

此外，偵辦彰化縣李姓嫌犯 DMT 詐欺話務機房案，進入 DMT 詐欺話務機房時，發現 DMT 設備正在運轉，尚有一個遠端監視器正對著門口，第一反應是先用布直接蓋上鏡頭，因為貿然斷電可能會讓主嫌起疑滅證，同時發現屋內所有設備插座皆搭配智能插座 WIFI 版，為防止主嫌從遠端斷開電源，先將智能插座移除，並儘速側錄網路封包並嘗試蒐集主嫌遠端操作時留下之 IP 位址作為日後溯源上手之用，再請鑑識人員採集物理性跡證。如此謹慎行事係根據近期查獲 DMT 設備案件，從通信紀錄發現，部分主嫌會從遠端竄改 DMT 設備發話 IMEI，增加警方蒐證及分析通信紀錄難度。另外根據目前已查獲案件並破解 DMT 管理介面密碼取得主嫌遠端設定留下之 IP 資料，發現大多位於境外，未來將持續透過協查合作有效打擊境外詐欺話務機房。

肆、偵辦困境

一、DMT 設備輕盈、安裝快速，密集移動犯罪處所

隨著 DMT 話務機房逐一為警方查獲後，詐欺集團開始縮短 DMT 機房停留在同一處所時間，以跨縣市的方式移動機房位置，以致警方才剛分析完資料後，機房可能已移至下一個處所，造成警方舉證及蒐集犯罪證據困難，使得查緝此類案件難度日益漸增。



二、利用外國人註冊訂房網承租日租套房

犯嫌發現住宿商務旅館容易被警方查獲，後期便改以外國人身分註冊某國際知名訂房網站，快速找尋合適地點，並以國外信用卡付款承租日租套房，增加查訪住宿者及訂房者資料難度。

三、招募求職者架設機房，透過通訊軟體指揮及面試

犯嫌透過社群媒體及報章雜誌刊登求職訊息，告知應徵者本身為境外電商，協助架設 DMT 設備是為發送廣告簡訊及蒐集使用者數據資料做為大數據分析等話術，誘騙求職者按照犯嫌指示架設 DMT 話務機房。主嫌全程以通訊軟體通話、視訊等方式指揮求職者架設機房及排除故障，並同時要求職者刪除對話紀錄，酬勞發放則透過其他犯嫌以 ATM 現金無摺存款方式匯給求職者，形成斷點增加警方向上溯源困難。

四、電信技術日新月異

目前電信技術可透過遠端 SIM 卡管理器設備將 SIM 卡插在境外，將話務網路化後再透過 DMT 設備跳過當地電信公司漫遊；或以 4G 網路電話技術，無須另行架設 DMT 設備，即可異地發話給被害人，因此讓真實詐騙話務機房得以藏身於境外。

伍、未來方向

一、強化 DMT 設備內容解析

與數位鑑識單位合作並研究 DMT 設備功能，期能從設備本身破解犯罪者工具及找出可歸類之特徵點，更迅速找出 DMT 設備所在處所並加以查緝到案。

二、追溯犯罪共犯架構與事實

透過查緝到案犯嫌供述及聯繫方式，佐以數位鑑識並還原通訊軟體對話紀錄，再以社交工程方式找出上手或主嫌使用 IP、所在地及真實身分。

三、建立犯罪對策與資料庫

從每次偵辦或查緝到案經驗及資料，建立犯罪資料庫並與電信業者研究用於詐欺發話門號之特徵點，建立高風險門號資料庫。

四、增加犯罪成本

電信詐欺需要使用大量人頭門號，目前法規並未禁止使用他人門號，販售門號的行為

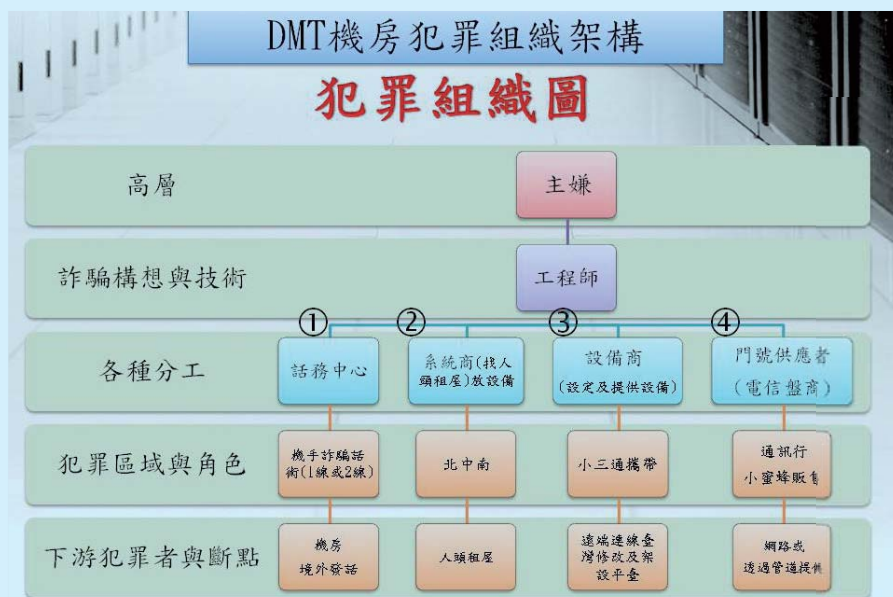
也未入罪，惟門號涉及相關犯罪時，可援用電信法規通知所屬電信公司斷話，並加強查緝涉案人頭門號流向，以減少人頭門號數量為手段，藉以提高詐騙集團犯罪成本。

陸、結語

隨著電信及網路技術發展可將傳統電話話務透過網際網路的方式傳遞，原先美意是讓使用者節省成本及縮短溝通距離，而 DMT 設備為使企業節費或方便民眾使用多個門號發話，朝向縮小設備體積及數位式方式開發。

犯罪集團將上述技術及 DMT 設備，用於跨境發話詐欺國人，利用國人第一時間未能查證發話者身分及善良的天性，使被害人受騙匯款。

本局除規劃專案行動針對是類案件加強查緝外，另透過社群媒體、報章媒體及 165 反詐騙諮詢專線提供諮詢及加強宣導反詐欺資訊，期能降低國人受騙損失。



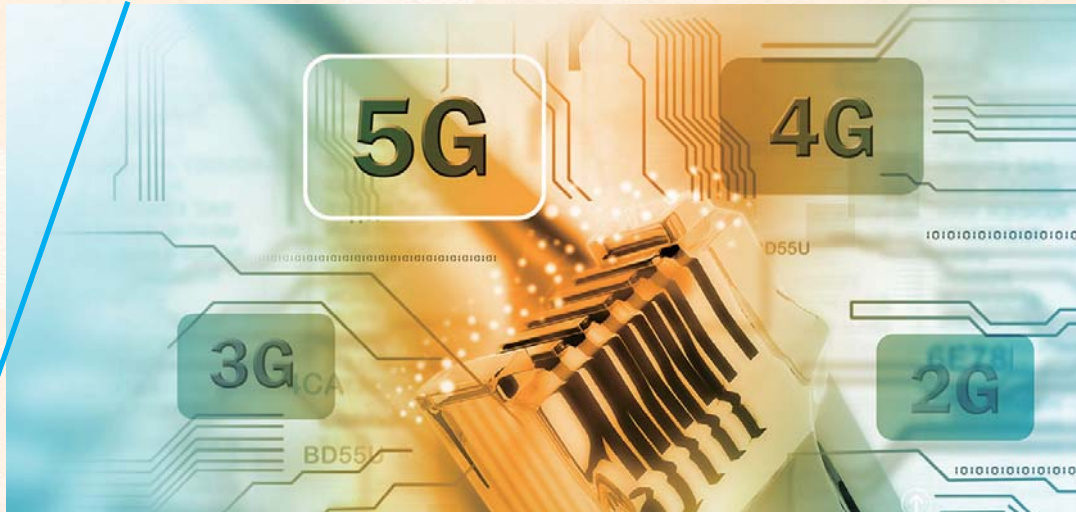


通訊監察於打擊詐欺犯罪實務之助益

刑事警察局通訊監察科偵查員／楊元宏

壹、前言

行動電話的使用人口快速發展，通訊種類、方式日趨多樣化，通訊工具取得也更加容易，通訊監察已是偵查犯罪不可或缺的一環。本科受理全國警察機關，以及國安局、調查局、海巡署、廉政署等治安、國安機關通訊監察投單，協助設定上線監察，並接受各機關通訊監察問題反映，即時予以說明答覆，必要時聯繫維運廠商、居中協調電信業者，協助障礙排除。每年約協助 3 萬件通訊監察案件，對打擊各項犯罪貢獻卓著。



犯罪偵查講究即時性、機動性，能迅速破案的時機稍縱即逝，偵查人員需掌握時效，即時進行偵查工作。為此，本科不自我設限為內勤單位編制，值班台人員 24 小時保持聯繫管道暢通，對於有急迫性之案件，皆能立即協調上線人員、維運人員即時協助處理，以滿足外勤偵查人員對辦案效率的需求。

通訊監察大致可分為一般監察及緊急監察：

一、一般監察：

係由法院核發通訊監察書，經執行機關持通訊監察書投單，由本科審核後予以協助設定上線監察。

二、緊急監察：

係依通訊保障及監察法第六條：「有事實足認被告或犯罪嫌疑人有犯刑法妨害投票罪章、公職人員選舉罷免法、總統副總統選舉罷免法、槍砲彈藥刀械管制條例第七條、第八條、毒品危害防制條例第四條、擄人勒贖罪或以投置炸彈、爆裂物或投放毒物方法犯恐嚇取財罪、組織犯罪條例第三條、洗錢防制法第十一條第一項、第二項、第三項、刑法第二百二十二條、第二百二十六條、第二百七十一條、第三百二十五條、第三百二十六條、第三百二十八條、第三百三十條、第三百三十二條及第三百三十九條，為防止他人生命、

身體、財產之急迫危險；或有事實足信有其他通訊作為前條第一項犯罪連絡而情形急迫者，司法警察機關得報請該管檢察官以口頭通知執行機關先予執行通訊監察。但檢察官應告知執行機關第十一條所定之事項，並於二十四小時內陳報該管法院補發通訊監察書；檢察機關為受理緊急監察案件，應指定專責主任檢察官或檢察官作為緊急聯繫窗口，以利掌握偵辦時效。法院應設置專責窗口受理前項聲請，並應於四十八小時內補發通訊監察書；未於四十八小時內補發者，應即停止監察。」此類監察通常發生於下班後或例假日等勤餘時段，本科編排輪值勤務，以隨時保持與值勤人員聯繫暢通，接獲值勤人員通報檢、警、調等治安或國安機關申請緊急監察，儘速往返辦公處所，協助辦理設定上線緊急監察。

對於辦案人員持法院核發通訊監察書或檢察官同意先予執行之緊急案件通知書，請求協助通訊監察，本科皆能即刻提供協助，協助案件達成率 100%。

貳、108 年度執行通訊監察破獲重大詐欺案件

一、本局電信偵查大隊偵破唐姓主嫌等 20 人假冒公務機構詐欺車手集團案：



(一) 本局電信偵查大隊於 107 年 8 月起偵辦被害人陳○○等人遭假冒公務機構詐欺案，發現境外詐騙機房夥同桃園地區之水房、車手團成員共組電信詐欺集團；經與新竹市警察局第二分局組成專案小組，向法院聲准通訊監察，並經專案小組送驗、比對假公文書指紋，鎖定特定犯嫌，及向銀行調閱車手交、提款畫面，續分析車手行蹤影像，輔以數月跟監、蒐證後，經檢察官指示，陸續查緝車手集團幹部小唐、集團車手頭及車手計 20 人到案，訊後均移送地檢署偵辦，本案仍持續向上溯源，查緝詐欺水房擴大偵辦中。

(二) 本案於拘捕車手張○○時，發現張嫌身上另攜有新臺幣 120 萬元之紙袋，經專案小組就鈔票綑線上所蓋之郵局經辦人印章，向郵局查得提款人（被害人）為一對年逾七旬退休夫妻，經聯繫後順利將詐欺款項即時發還被害人，獲被害人當面致謝，顯見法網恢恢，疏而不漏。

二、本局國際刑警科偵破李○耘等人涉嫌馬來西亞 ANB&M101 吸金案：

(一) 查該集團以投資馬來西亞房地產為幌子，謊稱年報酬率高達 348%，並於國內架設網站供投資人查帳、提現及轉帳使用，復利用境外 OBU 帳戶移轉及隱匿吸金所得，初步清查該集團涉嫌違法吸取將近新臺幣 10 億元資金。李嫌為上開集團帳房，除以上開 OBU 帳戶轉移資金外，另透過名下國內公司帳戶發放獎金給投資人，為擴大業務及吸引民眾投資，更委外製作「WoPay」電子錢包供投資人使用，便利親自管理集團投資人帳務。

(二) 專案小組調查後發現李嫌所為涉犯詐欺、洗錢及銀行法案，於 108 年 3 月 11 日分至臺北市、桃園市、臺中市等地同步搜索 7 個相關處所，拘提主嫌李○耘及通知 3 名犯嫌到案，現場查扣現金新臺幣 190 萬元、手機 14 支、電腦 6 臺及相關書證，另向臺北地方法院聲請扣押新臺幣 1 億 7,600 萬餘元範圍內財產獲准。



圖 2：查扣現金、行動電話、電腦、存簿、投資方案等相關贓證物。



圖3：查扣犯案用手機30支、平板電腦3臺、筆記型電腦3臺、U盾48組、銀聯卡9張，新臺幣50萬9000元等相關贓證物。

三、本局偵查第二大隊偵破白嫌等5人電信詐欺機房案：

本局偵查第二大隊於日前接獲情資，掌握白嫌等5人涉嫌結合電信詐欺機房，以假冒公署名義行使詐騙，復利用人頭金融帳戶透過網路銀行層層轉帳至第三方支付平台轉換現金，藉以替詐欺集團轉帳洗錢，初估受害者達十餘人，轉帳金額高達新臺幣數千萬元。

本局迅與臺北市政府警察局、臺中市政府警察局與嘉義市政府警察局組成專案小組展開追查，在鎖定犯嫌經營水房之處所後，專案小組進行攻堅，當場查獲5名犯嫌及查扣上述犯案用手機等贓證物，全案依刑法詐欺罪及違反洗錢防制法罪嫌解送臺灣臺中地方檢察署偵辦，並持續向上溯源。

參、結語

從上述案件可歸結以下四點防詐心得，希能與社會大眾共勉之：

一、民眾應提高自我防詐警覺，凡遇不明或可疑電話，不論手機或市話，都要「冷靜」、「查證」、「報警」，

並可撥打「165反詐騙諮詢專線」，以適時得到員警協助與諮詢服務，維護自身財產安全。

二、另外，暑（寒）假期間，青少年打工不能為貪圖暴利，替詐欺集團從事轉帳洗錢，即便不知道轉帳金錢來源為何，同樣必須面臨牢獄之災，得不償失；家長亦應關心子女打工之情形，避免誤觸法網淪為詐欺集團之共犯。

三、凡接獲以電信業者、法官、檢察官、警察等身分來電告知：「你的身分證、健保卡被冒用並涉及洗錢、綁架、擄車勒贖、欠電話費等，要凍結你的帳戶（財產）或交付保證金或監管你的銀行存款且不得對外洩露，不從就羈（收）押你」等語，或聲稱子女向錢莊借貸、與人作保現被綁架等情況，十之八九為詐騙話術。因此，於接到身分不明之陌生電話時，應即刻掛斷電話，並查核通話資訊是否屬實，並善加利用「165反詐騙諮詢專線」、「0911-511111反簡訊詐騙特碼」或「110」提出檢舉、諮詢，遇事遵行「停」、「聽」、「看」守則，勿急、勿躁、多思考，全民投入防詐騙行列，讓歹徒再無可乘之機！

四、至於國人對於海外投資環境及投資項目，應謹慎評估，勿因短期優厚紅利及高額獎金貿然投入鉅資，以免受騙上當血本無歸；如因海外投資案遭到詐欺及蒙受財產損失，可提供相關資料向警察機關尋求協助。為維護金融秩序以及打擊海外投資詐欺，本局亦將持續追查幕後主嫌以及可疑金流，以保障民眾財產安全。





郵包炸彈處置與應變

刑事警察局偵查第五大隊偵查員／蕭雅安

壹、前言

郵包炸彈多是透過不知情的郵務人員或公司大樓的物管人員，進入目標物建築內部或直達特定個人，以造成建築物本體的損害、人身傷害甚至死亡，同時製造混亂、恐慌等情狀為目的。有別於一般爆裂物，置放或寄送郵包炸彈的嫌疑人，利用郵務、快遞人員及其系統，運送外觀偽裝成信件或包裹的爆裂物，一可躲避建築保全警衛盤查，達到一般外人無法進入的公



司組織建築物內部，再者當爆炸發生時，炸彈客仍可於安全的暗處躲藏觀望，甚至趁機計畫著下一次行動。因郵包炸彈所循途徑，與日常生活的密切度高，且容易造成重大損傷，一旦發生，莫不引起社會高度關注。

是類案件在我國雖屬罕見，仍曾發生且致人傷殘，相關案例略述如下：

- 一、民國 65 年前立委王幸男製作郵包炸彈，炸傷時任省主席謝東閔手臂及時任革命實踐研究院主任李煥手指，為典型郵包炸彈案例。
- 二、民國 81 年花蓮縣某補習班收到不明可疑包裹，經當事人將郵包拿到派出所騎樓欲報警時，郵包突然爆炸，現場三人嚴重受傷，其中包含派出所值班員警官大增。
- 三、民國 102 年，苗栗縣卓蘭鎮某鵝肉店，一個可疑的包裹被置於店家門口停放的車輛上，上面寫有店家少東的名字，少東方打開即引爆內部炸藥，致渠頭手遭到炸傷送醫。
- 四、民國 108 年 5 月，於高雄鼓山亦發生郵包炸彈案，該案嫌疑人因與被害人債務糾紛而在被害人家門前置放偽裝為包裹之炸彈，被害人不疑有他直接打開，致爆炸傷重，而案發當下爆炸威力驚人，周圍民眾均擔憂遭受波及而心惶不安。

鑒此，特蒐集英、美、日等先進國家有關郵包炸彈辨識、處理及緊急應變流

程，提供國內各基礎建設警衛保全單位、收發單位、郵務單位、警政單位乃至於一般民眾，瞭解基本辨識之特徵、應對之要領，方能於危機發生時做好萬全的準備，並防患於未然。

貳、郵包炸彈種類

郵政和快遞服務經常被利用來向目標接收者提供危險物品，必須正確進行風險評估了解組織面臨的威脅，並提出對應預防措施。郵包炸彈主要有信件、包裹和快遞等形式，包含以下種類：

- 一、爆炸性或燃燒裝置
- 二、銳器或刀片
- 三、令人反感的材料
- 四、核生化(CBRN)物質(散裝或小型/離散量)或裝置。於國外案例中常聽到“白色粉末”，可能是具危險性的化學物質(爆炸性或麻醉性)，生物或放射性材料，也可能是無害材料。這些材料可能不是“白色”、也可能不是“粉末”而可能是結晶的(例如糖)，油性或蠟狀殘膏，或黏稠液體。

任何收到可疑包裹的人都不太可能知道它確切是哪種類型，因此安檢程序應須一體通用於各種可能情形。郵務人員經常以拋扔方式轉運包裹，然而鮮少因此觸發內部爆裂物裝置，但任何打開它的嘗試都可能引爆。值得注意的是，含有核生化物質之包裹，

即使小心溫和處理，也可能導致內部危險物質釋放。

郵包形狀和尺寸各有不同，包裝精美的郵件看似無害，仍有些指標可判斷其是否危險。

參、可疑包裹特徵

下列特徵中的一般性指標為一般性特徵，僅憑單一特徵不一定能正確判斷，應做全面性的風險評估、多方分析後研判。

一、一般性指標

- (一) 非預期中的包裹，特別是親送的
- (二) 厚信封袋
- (三) 額外的包裝
- (四) 標示指定某側開啟
- (五) 形狀特殊或重量不平衡
- (六) 信封封口完全密封嚴實（通常塗膠的信封封口在邊緣留有一些翹起縫隙）
- (七) 標示某人親展、機密、私人等（或某組織或某職位者收）
- (八) 郵戳顯示來源可疑
- (九) 沒有寄件地址或寄件地址可疑（如錯字或印刷草率）
- (十) 筆跡陌生
- (十一) 過多的郵資
- (十二) 包裝油漬外溢
- (十三) 散發特殊氣味
- (十四) 外觀破損

二、爆裂物或可燃物特殊指標

- (一) 重量不平均
- (二) 信封或包裝外觀有小洞
- (三) 發燙

三、核生化物特殊指標

- (一) 粉末、液體外露
- (二) 包裝外觀有液體滲漏
- (三) 打開時有異味、或忽然間皮膚、眼睛或鼻子有刺激感、或內容物為粉末、結晶體、黏稠物等

簡單來說，至關重要的是收發人員的細心與敏銳度，藉由收發人員的眼觀、耳聽、鼻嗅、手觸，以發掘可疑包裹之不尋常處，從而進行更嚴謹之偵檢和危機處理。

肆、可疑郵包處置作為

一、避免不必要的接觸或 X 光

- (一) 如果正拿著，慢慢置放於平坦桌面上
- (二) 標識警示、避免不知情者誤拿
- (三) 不再移動、亦不拍攝 X 光
- (四) 若在 X 光機內，留在裡面不再移動

二、立即隔離

- (一) 立即疏散人員、包含上下樓層人員
- (二) 若為核生化物包裹，立即隔離已接觸人員與其他未接觸人員
- (三) 避免其他人再進入或接近已遭汙染地點
- (四) 避免於可疑包裹 15 公尺內使用手機或對講機

三、報警

- (一) 若包裹已被打開、半打開，要立即告知警方
- (二) 目擊者或知情者應立即向警方簡要說明情況，最好能寫下人事時地物等不尋常之細節，也避免在



警方抵達前與其他非相關人員討論案情。

伍、收發室政策

- 一、除了收發郵件外，收發室應做為安全檢查篩選郵件的處所。讓所有進入組織建築物內的包裹郵件均於收發室先行安檢。
- 二、收發人員對可疑包裹的敏感度及處置方式至關重要。逐個目檢包裹外觀是基本作為，如有核生化物質如郵包炸彈之疑慮，收發人員應落實洗手，戴口罩及手套。
- 三、檢測過關的包裹可以特殊膠帶標示，以提高區分及辨識的工作效率。收發室應與主建物分開，如此可降低可疑包裹發生事故時之風險，包含收發室的空調系統，應分別建置於不同管線。
- 四、另外針對特殊大尺寸、數量多的包裹（例如辦公設備，文具和餐飲用品等）可透過以下措施降低風險：
 - （一）檢核訂單內容。
 - （二）只接受預期的投遞，盡可能使用值得信賴的供應商。
 - （三）開箱檢查交貨內容。
- 五、採用 X 光監測系統
 - （一）X 光可穿透包裹偵測內部物質：如金屬銳器、爆裂物、可燃物或核生化物等。

（二）X 光具有多種等級，可提供不同的檢測能力，能同時對多個物品進行檢查。

陸、結語：培養安全意識，防患於未然

- 一、在恐怖攻擊事件發生率較高的國家，例如英美和歐洲等國，於各大城市裡，民眾聚集、人潮洶湧的地鐵、車站等公共空間，為防止恐怖攻擊造成大規模的傷亡，多有利用定時廣播、張貼海報及短片廣告，強化民眾公共安全危機意識，察覺異樣迅速報警，以收降低危害與傷亡之效。
- 二、辦公大樓或公家機關收發室，可張貼相關宣導傳單或海報於收發室、出入口等，達到提醒與培養安全意識之目的。
- 三、定期舉辦員工教育訓練，針對郵務人員、收發人員施予年度定期安全意識課程，使收發人員於工作中對可疑包裹郵件維持高度敏銳度。
- 四、主管機關可舉辦不定期演練，以製作外觀可疑之假爆裂物包裹，無預警參雜於一般日常收發郵件之中，考驗收發人員檢驗包裹安全的敏銳度，或可從隨機演習中重新審視收發室郵件安檢流程優缺點，再於後續教育訓練中改進強化。



警察機關執行 防制洗錢作為與未來展望

刑事警察局經濟科警務正 / 賴建亨

壹、前言

2016 年前，我國洗錢罪的成罪門檻相當高，平均一年起訴約僅 20 案。警察機關雖然精於各類型傳統刑案之偵查技巧，惟對於「洗錢」多僅止於表面的認知。然而在法務部努力下，在法制面有了重大突破，首先是 2016 年 7 月 1 日刑法沒收新制及刑事訴訟法扣押新制施行，強調「任何人都不得保有犯罪所得之原則」，繼於同年 12 月 28 日修正通過洗錢防制法新制，加上 2018 年不間斷的修法微調，我國洗錢防制工作所需法制基礎已漸趨完備，對執法機關偵辦案件更是強力後盾。

貳、警察機關作為

2016 年既是我國洗錢防制工作的一個重大轉折，警察機關亦緊隨著法制面的修正，自 2016 年 7 月 1 日的沒收扣押新制開始，逐步擴大防制洗錢工作，茲以「政策面之強化」、「執行面之成果」及「外部合作」等三大面向分述如下：

一、政策面之強化

偵查犯罪所需掌握之線索包括：「人流」、「物流」、「金流」、「資訊與通訊匯流」等四面向。惟在 2016 年時，警察機關對於各種金融資料之保管機關、調取方式、分析運用技巧，乃至扣押不法所得之重要性等，尚未能系統化的進行全般性整合與認知。基此，為配合上述四面向，警察機關逐步訂定並修正相關行政規則，提供第一線偵查人員明確、完整之指引。此外並注重新型態洗錢犯罪之研究，加強教育訓練，藉以建立金流追查觀念，提高偵查效率。相關強化措施包括：

（一）訂定「警察機關使用金融帳戶開戶查詢系統管理規定」

金融帳戶開戶查詢系統為法務部委請財金資訊股份有限公司所建置，法務部訂有「金融帳戶開戶查詢系統使用管理要點」。為符合實務需要，警察機關已參考上開要點，另訂管理規定，詳細規定查詢、保密、稽核等工作事項。

（二）訂定「警察機關使用大額通貨交易查詢系統管理規定」

金融機構依洗錢防制法第 9 條規定向法務部調查局申報的大額通貨交易報

告（Currency Transaction Report, CTR），包括新臺幣 50 萬元以上現金存、提、兌之資料，為追查金流的利器。過去警察機關僅能以公文方式調閱，效率不彰。後因法務部調查局洗錢防制處建置新系統，並與警政署資訊部門聯結，始提供警察機關得不受公文往返時效之限制而得即時查詢 CTR，本項系統管理規定訂有相關作業處理流程。

（三）訂定「警察機關處理可疑洗錢交易情資注意事項」

金融機構依洗錢防制法第 10 條規定，負有向法務部調查局申報可疑洗錢交易報告（Suspicious Transaction Report, STR）之義務，此報告亦為追查金流的利器之一。法務部調查局洗錢防制處自 2018 年起新設置調閱 STR 系統，提供警政署資訊部門聯結申請，本注意事項訂有相關作業處理流程。

另法務部調查局洗錢防制處針對上述 STR，經分析金流及關係人前科背景資料後，進一步形成「加值 STR」，即所謂金融情資，於調查階段具高度參考價值，目前均依案類分送各執法機關運用。依本注意事項之規定，各警察機關運用金融情資須適時回報刑事警察局，目前所有分送警察機關的金融情資在程序上均經審核納管。

（四）訂定「警察機關執行扣押處分獎勵規定」

刑法沒收新制及刑事訴訟法配套修正的保全扣押制度，主要目的係為根絕高額利潤之犯罪誘因、有效追訴犯罪。其中，詐欺犯罪、毒品犯罪（製造、運輸、販賣）、組織犯罪等三類犯罪，不但是警察機關一貫的治安重點工作，也是國家風險報告中所揭示具有非常高洗錢風險的前置犯罪。經由澈底查明犯罪者之財產及資金，依法扣押移送司法機關偵查審判，並依法沒收，實為打擊此三類犯罪之關鍵。

刑事訴訟法扣押本為查緝各類犯罪案件重要工作之一，在警察機關內部的獎勵措施上，原未許可於案件破獲移送外，單獨就扣押犯罪所得部分敘獎；惟為配合刑法沒收、刑事訴訟法扣押新制，督促激勵警察人員積極執行扣押處分，乃針對扣押特別訂定本獎勵規定，扣押不法所得達新臺幣一千萬元者，首功人員併本案獎勵得記一大功。

（五）強化教育訓練

1. 各警察機關常年訓練及全國刑事人員講習班
為重視洗錢防制之教育訓練，警政署編訂教材「洗錢防制法偵查實務暨案例討論」，列入各年度全國各警察機關常年訓練之必訓課程，對全國警察人員施教及測驗。

另外，就第一線偵查人員而言，最重要的訓練為每年舉辦之「全國刑事人員講習班」，其訓練科目諸如「洗錢防制及金融調查」、「經濟犯罪偵查—偵辦刑案追查金流實務」、「偵辦詐欺案類實務案例分享」、「查緝跨境毒品案例分享」、「檢肅黑道幫派工作執行要領」、「跨境犯罪與涉外案件偵查要領」等及其金流追查技巧，已涵蓋我國國家洗錢風險評估報告（NRA）中所列「詐欺」、「毒

品販運」、「組織犯罪」等具有非常高洗錢風險的前置犯罪類型。相關師資來源除資深刑事警察幹部外，亦商請法務部調查局洗錢防制處支援。

2. 法務部洗錢防制座談會

法務部針對檢察機關、執法機關，於每年度辦理「洗錢防制實務座談會」，邀請法界、學界專家學者進行洗錢防制專題講座，針對目前實務現況或困境深入探討。警察機關均指派實際偵辦案件的員警與會，提供實務偵辦經驗進行現場意見交換，藉以提升偵查技巧。

二、執行面之成果

以往詐欺集團使用人頭帳戶情形嚴重，偵辦時多能發現大宗人頭帳戶收受詐欺款項之事證；惟洗錢防制法新制實施後，自願性提供金融帳戶供詐欺集團處理不法贓款使用之行為（即人頭帳戶），已納入洗錢態樣，目前各警察機關偵辦集團性詐欺案件時，於查獲犯嫌自願性提供其所申辦之金融帳戶以掩飾不法所得去向時，均能以該當洗錢防制法第2條第1項第2款之構成要件，引據同法第14條罰則（包括未遂犯）辦理移送。

另外，我國提領犯罪所得的車手十分猖獗，以往查獲當時之相關事證不足以認定其涉犯特定犯罪，例如：在攔檢車輛的後車廂有數百萬現金與數百本人頭帳戶存簿；又如某重要政治人物之友人，一天內頻繁出入各大金

融機構，從事接近大額通貨申報金額上限之匯款合計達上億元，雖無法認定涉犯特定犯罪，惟現依洗錢防制法新制規定，其行為明顯與金融活動交易常態顯相悖反，且持有、使用之金額與其收入顯不相當，可成立新增之特殊洗錢罪（「車手條款」或「洗錢教父條款」）。警察機關如查獲犯嫌係向無特殊信賴關係之他人租用、購買或施用詐術取得金融帳戶，用以收受、持有或使用之財物或財產上利益，而無合理來源且與收入顯不相當者（如詐欺集團車手），即屬「以不正方法取得他人向金融機構申請開立之帳戶」收受、持有或使用疑似不法所得之特殊洗錢態樣，均能以該當第 15 條第 1 項第 2 款之構成要件辦理移送（同條文訂有罰則，包括未遂犯）。

在上述二類常見犯罪態樣，均全面適用洗錢防制法新制之後，警察機關查緝洗錢犯罪成效已獲顯著提升，近年查獲績效為：2017 年僅 53 件、2018 年 549 件、2019 年已達 1,350 件。

三、外部合作

（一）跨機關合作加強犯罪宣導

警察機關目前就行政院提供之相關電子及書面海報、懶人包、常見問答集、廣播短語、跑馬燈文字等資料，登載於所屬官網、臉書、LED 電子看板或其他適當地點，並利用向其他機關、學校接洽辦理犯罪預防宣導時機，共同合作向所屬員工、師生擴大宣導作為，以加深全民對於洗錢防制法新制之認知與觀念。

（二）與法務部調查局之合作

除與調查局建立調閱 STR、CTR 聯繫合作機制外，警察機關亦不定期派員參加調查局舉辦之「資金調查實務與犯罪態樣研討會」，如 2018 年 4 月 24 日於調查局科技大樓大簡報室所舉辦之場次，刑事警察局亦同時指派具備「組織犯罪」偵查專業與實務經驗之幹部擔任講座，與在場檢察官、調查官共同研討追查犯罪金流技巧與交換實務心得。

參、未來展望

一、開發多方教育訓練管道

警察機關除自行針對內部進行教育訓練外，亦應聯繫外部機關就其所開設相關研討會、講座，主動協調爭取適當出席名額，藉由吸收外部機關專業知識，提升警察人員偵查技巧。未來也將透過國際組織，如：亞太防制洗錢組織（APG）、國際刑警組織（INTERPOL）、歐洲刑警組織（EUROPOL），多方蒐集其他國家防制洗錢及查緝金流等相關訓練資訊，適時爭取我國派員參與之機會，以拓展不同執法視野，充實警方偵查能量。

二、持續查緝第三方洗錢犯罪

警察機關於 2019 年進行六次「掃蕩地下金融專案」工作，其中三次係配合臺灣高等檢察署規劃「查緝地下通匯專案」辦理，透過對地下通匯業者（第三方洗錢）加強查緝，調查犯罪金流來源或目的地，成效良好。以上專案共計查獲 167 件、執行到案的地下通匯業者 499 人、扣押不法所得 2 億 5,800 萬餘元，另統計查獲帳上匯兌金額達 84 億元，通匯地區遍及大陸、香港、菲律賓、越南、印尼、泰國及澳洲等。警察機關未來除持續配合臺灣高等檢察署專案查緝外，亦應持續不定期規劃掃蕩工作，防止不法金流氾濫。

三、追查境外不法所得

追查境外不法所得，向來為我國偵辦洗錢案件之困境，主要因目前國際政治因素，我國雖無法與大多數國家建立外交關係或簽訂司法互助協定，但仍積極尋求各種形式之國際合作互助，如警察機關近年拓增派駐美國等 12 國及澳門共 13 位警察聯絡官及簽署多個合作備忘錄、透過國際刑警組織日本東京總部等請求外國對等機關協助、並積極派員參加國際組織相關會議，拓展合作網絡。即便在執法合作上處境艱困，警察機關仍設法與外國執法機關進行跨境毒品、詐騙等案件之聯合調查，對於大多數未與我國簽訂司法互助協定之國家，亦積極不斷地請求合作，設法追回已被移往外國之犯罪收益。

未來警察機關應持續拓展多元國際合作途徑，如：利用國際會議等場合及機會，適時分享我國偵辦各類重大犯罪案件之經驗，提倡與各國建立跨境偵查犯罪之夥伴關係與機制；或是與各類國際組織在現有的互動基礎上，建立暢通的聯繫管道及窗口，分享追查跨境金流情資，強化互助合作。

肆、結語

洗錢防制工作是否可以持續改善以提高成效，關鍵在於「觀念常新、精益求精」。以警察機關而言，過去查緝案件的重點在人、在毒品、在槍枝，但金流面的追查不足；然而現在各警察機關訂定計畫、偵辦刑案，均已將追查不法金流、扣押犯罪所得等列為首要工作，洗錢防制成效已明顯得到提升。而觀念常新是一個長期的過程，包括基層人員、中階幹部及高階領導人員，都需要不斷地學習正確的洗錢防制觀念，隨時掌握最新相關資訊，紮實、持之以恆地做下去，才能發揮懲奸除惡的效果。



修正刑法 打擊聚眾鬥毆

刑事警察局司法科偵查員／鄒至剛

FORUM | 偵查論壇

壹、修法緣由

隨著科技進步，群眾如透過社群通訊軟體（如 LINE、微信、網路直播等）進行串連集結，時間快速、人數眾多且流動性高，不易先期預防，致使聚眾鬥毆案件規模擴大，易波及無辜。

然由於司法實務向來對於刑法第 149 條聚眾不解散罪及第 150 條聚眾強暴脅迫罪認定過於狹隘，導致聚眾鬥毆未致死或重傷，而當事人均不提告時，僅能依社會秩序維護法裁處，嚇阻力顯然不足，實有必要修法，以因應方興未艾之街頭聚眾鬥毆案件。

貳、現行法之實務見解

現行刑法第 150 條「公然聚眾，施強暴、脅迫者，在場助勢之人，處…；首謀及下手實施強暴脅迫者，處…。」，字面上的構成要件其實就只有「公然聚眾」及「施強暴、脅迫」而已，然司法實務卻為其設下隱形的四大門檻，導致本條形同具文，析述如下：

- 一、「公然聚眾」一詞應解為「一群人在公然之狀態下聚集」較為合理，但司法實務卻認為必須在「公然」之狀態下聚集多數人，如透過社群通訊軟體呼朋引伴、糾集群眾，因為並非在「公然」的情況下聚集群眾，縱使雙方人馬大打出手，亦不構成本罪。
- 二、「聚眾」指參與之多數人有隨時可以增加之狀況，若參與之人均係事前約定，人數既已確定，便無隨時可增加之狀況，自與聚眾之情形不合。據此，雙方人馬約好在街頭打群架，但因人數已確定，即非隨時可增加之狀況，縱使是 10 打 10 人數眾多且秩序混亂，或路人勸架、圍觀，亦不構成本罪。
- 三、必須有首謀者公然發起召集群眾，如果是一群一言不合或互看不順眼的偶然性群毆，因為沒有一個發起人，所以也不構成本罪。
- 四、必須行為人主觀上有妨害秩序之故意，始成立本罪，如公然聚眾施強暴脅迫，其目的係在另犯他罪，並非意圖妨害秩序，除應成立其他相當罪名外，不能論以妨害秩序罪。但其實本罪重在安寧秩序之維持，只要客觀上足以破壞社會秩序即為已足，不應以行為人主觀上是否具備妨害秩序故意為判斷標準。

參、相關統計數據

據統計近兩年（107、108 年度）的聚眾鬥毆案件，警察機關依刑法第 150 條移送者計 2,672 人次，遭起訴者計 10 人，起訴率為 0.3%，遭有罪判決者 0 人，有罪率為 0%。又因構成要件過於嚴苛，且解散命令難以實施，故未有依刑法第 149 條聚眾不解散罪移送、偵查、判決者。

另警察機關依社會秩序維護法第 87 條第 2 款互相鬥毆及第 3 款意圖鬥毆而聚眾移送法院簡易庭者計 511 件，2,047 人次；不罰計 561 人次，佔 27.4%；裁罰計 1,486 人次，佔 72.6%。其中裁處罰鍰計 1,479 人次，佔 72.3%，罰鍰金額以新台幣 2,000 至 6,000 元為大宗，計 1,266 人次，佔所有裁罰案件之 85.1%；裁處拘留共 7 人，均為易以拘留，佔所有裁罰案件之 0.4%。

由此可知，近來聚眾鬥毆案件明明層出不窮，屢屢占據各大新聞媒體版面，破壞社會秩序甚鉅，卻無一人遭到判刑，多以社會秩序維護法裁處罰鍰新台幣 2,000 至 6,000 元，嚇阻力顯然不足，致使行為人肆無忌憚，離開警察機關後繼續糾眾鬥毆，使得警察疲於奔命、抓不勝抓。司法實務所設下隱形的四大門檻極端限縮本罪之成立，招致各界多有批評，已無法符合當前社會需求，所以才必須修法與時俱進。

肆、修法內容與理由

修正條文	現行條文	說明
第一百四十九條 在公共場所或公眾得出入之場所聚集三人以上，意圖為強暴脅迫，已受該管公務員解散命令三次以上，而不解散者，在場助勢之人處六月以下有期徒刑、拘役或八萬元以下罰金。首謀者，處三年以下有期徒刑。	第一百四十九條 公然聚眾，意圖為強暴脅迫，已受該管公務員解散命令三次以上，而不解散者，在場助勢之人處六月以下有期徒刑、拘役或三百元以下罰金。首謀者，處三年以下有期徒刑。	一、隨著科技進步，透過社群通訊軟體（如 LINE、微信等）進行串連集結，時間快速、人數眾多且流動性高，不易先期預防，致使此等以多數人犯妨害秩序案件規模擴大，亦易傷及無辜。 二、現行條文中之「公然聚眾」，司法實務認為必須於「公然」之狀態下聚集多數人，始足當之。是以，現實生活中以社群通訊軟體（如 LINE、微信等）進行串連集結者，即不屬之。亦有實務見解認為，「聚眾」係指參與之多數人有隨時可以增加之狀況，若參與之人均係事前約定，人數既已確定，便無隨時可以增加之狀況，自與聚眾之情形不合（最高法院二十八年上字第六二一號判例、九十二年度台上字第五一九二號判決參照）。此見解認定過於狹隘，學說上多有批評，爰有修正之必要。 三、聚集多少人始屬「聚眾」，恐生疑義，審酌三人以上在公共場所或公眾得出入之場所實施強暴脅迫，就人民安寧之影響及對公共秩序有顯著危害，是將聚集之人數明定為三人以上。另調整文字，並將此等三人以上之人聚集之場所，明定為「於公共場所或公眾得出入之場所」，強調此係指三人以上之人在公共場所或公眾得出入之場所聚集，包括自動與被動聚集之情形，亦不論是否係事前約定或隨時可增加均屬之，以與現行條文區別。 四、提高罰金刑，以符合罰金刑級距之配置。

修正條文	現行條文	說明
第一百五十條 <u>在公共場所或公眾得出入之場所聚集三人以上，施強暴脅迫者，在場助勢之人，處一年以下有期徒刑，拘役或十萬元以下罰金；首謀及下手實施者，處六月以上五年以下有期徒刑。</u> <u>犯前項之罪，而有下列情形之一者，得加重其刑至二分之一：</u> <u>一、意圖供行使之用而攜帶兇器或其他危險物品犯之。</u> <u>二、因而致生公眾或交通往來之危險。</u>	第一百五十條 公然聚眾，施強暴脅迫者，在場助勢之人，處一年以下有期徒刑，拘役或三百元以下罰金。首謀及下手實施強暴脅迫者，處六月以上五年以下有期徒刑。	一、修正現行「公然聚眾」要件，理由同修正條文第一百四十九條說明一至三。倘三人以上，在公共場所或公眾得出入之場所聚集，進而實行強暴脅迫（例如：鬥毆、毀損或恐嚇等行為）者，不論是對於特定人或不特定人為之，已造成公眾或他人之危害、恐懼不安，應即該當犯罪成立之構成要件，以符保護社會治安之刑法功能。另提高罰金刑，以符合罰金刑級距之配置，並酌作文字及標點符號修正，將現行條文列為第一項。 二、實務見解有認本條之妨害秩序罪，須有妨害秩序之故意，始與該條之罪質相符，如公然聚眾施強暴脅迫，其目的係在另犯他罪，並非意圖妨害秩序，除應成立其他相當罪名外，不能論以妨害秩序罪（最高法院三十一年上字第一五一三號、二十八年上字第三四二八號判例參照）。然本罪重在安寧秩序之維持，應解為只要客觀上足以破壞社會秩序即構成本罪。 三、參考我國實務常見之群聚鬥毆危險行為態樣，慮及行為人意圖供行使之用而攜帶兇器或者易燃性、腐蝕性液體，抑或於車輛往來之道路上追逐，對往來公眾所造成之生命身體健康等危險大增，破壞公共秩序之危險程度升高，而有加重處罰之必要，爰增訂第二項。

（註：囿於截稿時效，筆者投稿時尚未經總統公布，且說明欄因篇幅限制亦為節錄，其修正理由仍應以總統公布為準）

伍、修法實效

修正過後對於警察執法上產生實效如下：

一、第 149 條聚眾不解散罪：

- (一) 在執法層面上，通過條文只須證明聚集之眾人於聚集過程中之任一時點具有強暴脅迫之意圖即成立此要件。例如，甲方聚集多人向乙方催討債務，談判過程中甲方情緒升高而有尋釁或威脅舉動時，雖甲方聚集之初並無強暴脅迫之意圖，惟後續聚集過程中之尋釁或威脅舉動即可認為萌生此意圖之時點，而該當本要件，可以本條論處。
- (二) 解散命令次數維持現行條文「三次以上」，警察機關在命令解散三次後即得依法逮捕。然依司法院 76 廳刑一字第 1669 號函等實務見解，聚集之眾人如受超過三次解散命令而終於解散者，並無處罰必要之意旨，如現場群眾已有散去跡象，得以勸離代替逮捕。

- 二、第 150 條聚眾強暴脅迫罪：新增第 2 項加重聚眾強暴脅迫罪，將「攜帶兇器或其他危險物品犯之」及「因而致生公眾或交通往來之危險」之態樣加重其刑至二分之一，提高持械鬥毆及街頭暴力行為之嚇阻力，以降低對於社會秩序之危害。

陸、結語

刑法第 149、150 條將「公然聚眾」一詞修正為「在公共場所或公眾得出入之場所聚集三人以上」，明確定義場所及人數，有利於實務判斷；另第 150 條新增持械或妨害交通之加重規定，防止危害擴大，得以有效壓制於街頭、夜店、KTV 等場所聚眾鬥毆之情形。是以本法修正後，街頭聚眾鬥毆者將不再是罰鍰了事，而是科以刑責，大大提高嚇阻力，預計能夠有效減少街頭聚眾鬥毆案件量，還給民眾安居樂業的生活環境。



108年3月6日國家安全局同仁參訪本局



109 年 3 月 9 日澳洲昆士蘭警察局督察邁可道奇參訪本局

阻斷跨境電信網路 詐欺集團

內政部警政署駐印尼警察聯絡官／康淳閔

壹、前言

蔡總統於 108 年第一次署務會報中肯定警政署反詐工作的努力及成果，同時提及應持續全力貫徹打詐相關作為。刑事警察局各駐外警察聯絡官在各級長官指導、支持下，秉持國際合作、除惡務盡之精神，努力與各國執法單位建立跨境犯罪偵防平台並加強合作廣度、深度。筆者赴任駐印尼警察聯絡官前，於刑事警察局電信偵查大隊服務約 4 年，對於境內、外電信詐欺集團有些許偵查經驗，綜合抵任後於 108 年度在印尼查獲之案件分析，透過本文針對跨境電信詐欺犯罪提出偵防淺見，與各級長官、刑事工作前輩、先進交流，希冀激盪出更有效之偵防策略。



圖 1：筆者於巴淡島警局勘查數位證物

貳、案件成果與偵辦心得

108 年度印尼移民、警察單位查獲我國籍犯嫌涉案之電信詐欺集團案件計有 3 件：

- 一、108 年 4 月 18 日於中爪哇三寶瓏地區查獲 1 處詐欺機房據點，逮捕 40 名犯嫌，其中 12 人為我國籍，其餘為大陸籍。
- 二、108 年 9 月 18 日於巴淡島地區查獲 2 處詐欺機房據點，逮捕 47 名犯嫌，其中 29 人為我國籍，其餘為大陸籍。
- 三、108 年 11 月 25 日於大雅加達地區查獲 5 處詐欺機

房據點，逮捕 85 名犯嫌，其中 5 人為我國籍，其餘為大陸籍。

上述案件查獲後，筆者前往現地取證並進行詢問，發現境外到案嫌犯身分多為現場管理幹部（核心）、電腦手、各線機手，而集團上手多藏身國內遙控並透過地下匯兌等方式取得贓款。經詐欺集團管理幹部（核心）成員供述，多受具幫派背景之上層階級指揮，電腦手、機手則供述遭集團吸收管道多係透過網路遊戲、報紙求職、朋友牽線等，循個案供述脈絡，歸納可行偵防技巧如下：

- 1、依新修組織犯罪條例，針

對牟利性犯罪組織成員加強情資蒐報、列管，並定期查詢成員出、入境活動情形；於偵查個案過程，如見可疑對象即先行通報刑事警察局國際刑警科建立資料庫向移民署設立境管通知，並轉知各駐外警察聯絡官事先因應查緝腹案。



圖 2：筆者與印尼移民局官員押解人犯回台，簽署人犯交接收條

- 2、佈建網路、報紙廣告業者，如見欲刊登薪資待遇優、國外短期打工卻無面試地點、公司地址，僅留單一聯絡電話之廣告資訊，即通報偵查單位追查刊登者以及聯絡電話持機人。
- 3、針對有境內、外電信詐欺刑案資料者設立資料庫，分析日常金流、健保投保等靜態資料，無固定收入者轉列高風險對象，定期查詢渠等出、入境活動情形。

- 4、整合國內偵查單位情資，各單位鎖定對象如具通緝身分且滯留海外多年者，依偵查經驗多為詐欺集團核心成員，轉列為重點查緝對象，透過聯絡官制度與各國建立之跨境犯罪偵防平臺交流相關情資，俾於出、入境時各警察聯絡官駐在國時伺機緝捕、遣返，並透過數位鑑識渠等隨身電磁紀錄擴大偵辦。

參、結語

上述為筆者自身經驗歸納、略述，駐外期間對國內偵查新知、資訊更新相較不及時，有賴先進就國內偵查環境、法規隨機應變及調整應用。未來，為嚇阻是類集團持續招募社會經驗不足青年，遠赴海外從事電信詐欺犯罪，同仁應特別針對查獲並成功取證之境外詐欺機房案件，積極進行溯源偵查，緝捕集團金主、幹部，並聲請查扣不法所得、斬斷集團金流，力求澈底阻斷是項犯罪。





各國《禁蒙面法》的 立法源由及刑事偵查意涵

法務部調查局兩岸情勢研析處調查官 / 楊宗新

壹、前言

近數月來，香港因「反送中」事件陷入動盪，在民眾連續示威抗議下，港府於2019年10月4日，頒布了備受爭議的《禁止蒙面規例》。一時間，「禁止蒙面行為」成為各界高度討論的話題。本文將介紹香港及世界各國對於禁止蒙面之規範，並探討禁止該行為的刑事偵查意涵。

貳、香港的《禁止蒙面規例》

依據港府頒布《禁止蒙面規例》時發布的新聞稿，立法源由為：「激進及蒙面的示威者嚴重破壞公眾安寧，對社會造成廣泛和即時危險…蒙面示威者使用的暴力極端激進，大肆對人和財產投擲汽油彈、嚴重襲擊警務人員、警車和警署，並大規模蓄意破壞港鐵車站和政府合署等…禁止蒙面的行為，有迫切立法需要，以協助警方的刑事調查及蒐證，以及嚇阻暴力和違法行為。」

《禁止蒙面規例》中，將「蒙面」定義為「使用面罩，或者用其他可以遮掩全臉或部分臉龐的物品，例如以顏料畫上難以識別容貌的妝容」，在「經警方批出不反對通知書的集會與遊行；未經批准的集結；非法集結與暴動」等三種狀況中，蒙面者將觸法。違法者將處以最高監禁1年、罰款2.5萬港幣；

警方在這些場合中，也可隨時要求蒙面者拿下面罩，拒絕者另處以最高監禁6個月、罰款1萬港幣。

但若有「從事專業或受僱工作，為其個人人身安全理由，要蒙面在集會遊行現場出現者，如執勤員警；因宗教信仰而遮掩面部者；因先前已存在的醫學或健康理由，而要戴口罩者」等事由，是可以豁免的。

此法雖經香港高等法院於11月18日裁定違反《基本法》，惟《基本法》的制訂機關「中華人民共和國全國人民代表大會」已表示，香港高等法院無權解釋《基本法》。因此，《禁止蒙面規例》究竟是否有效，仍陷於爭議。

參、世界各國的類似立法

其實，香港的《禁止蒙面規例》並非全球首例，在許

多國家，都已行之有年，甚至我國也有類似立法，即《集會遊行法》第14條：「主管機關許可室外集會、遊行時，得就左列事項為必要之限制：…六、關於妨害身份辨識之化裝事項。」該條文雖無明訂禁止蒙面，但要求集會遊行參與者的身分，必須是可供辨識的，背後思維與禁止蒙面並無二致。

美國在20世紀中期，因曾發生數起利用萬聖節等變裝場合進行無差別殺人事件，及為取締「3K黨」、極端政治狂熱者之需，部分州政府開始禁止蒙面行為，目前包括哥倫比亞特區及另外15個



州，都有類似法規。觀察各州規範，可發現有許多較之香港更為嚴格，例如加州禁止在公共場所配戴假鬍鬚、明尼蘇達州禁止在公共場所穿長袍（此二者之原因，可能是許多阿拉伯裔恐怖分子都蓄長鬍、穿長袍）；加拿大則於 2013 年，在警方極力爭取下，通過《C-309 法案》，禁止在騷動或非法集會期間戴口罩或做足以隱瞞身分的裝扮，除非能證明出於宗教或醫療事由。

歐洲國家部分，因地緣上鄰近中東，經常發生恐攻事件，相關國家為求防範，乃禁止穆斯林婦女以全身遮蔽式裝束現身於公共場合。原本有類似立法的國家，多半是社會中有相當比例穆斯林族群者，惟近年來，因歐盟做出要求成員國必須接納敘利亞難民的決議，又多了好幾個社會中原不存在相當數量穆斯林的國家，也開始對即將到來的敘利亞難民預做規範。由此可看出，對比於

香港的《禁止蒙面規例》排除了宗教因素，歐洲國家因長期籠罩於宗教狂熱者發動恐怖攻擊的陰霾下，並不接受以信仰做為豁免事由。

類似立法多見諸於歐美國家，這並不代表這些國家限制人權，相反的，正是出於對人權的尊重，才將此罪刑法定化。相較之下，在其他法治不彰的國家，政府可肆意侵犯民眾權益，反而用不著類似立法。



肆、禁蒙面行為的刑事偵查意涵

犯罪心理學者指出，許多犯罪者都是在確信「不會被人察覺」的心理下，才著手進行犯罪行為，倘若他們明知會被發現，就不敢這麼做了。人在蒙面後，因受外界辨識程度降低，滿足了不易遭到察覺的要件，將使個人的社會責任感降低，行為也會變得更大膽，敢於鋌而走險或做出激烈舉措。

就群體性犯罪而言，當所有人裝束一致時，將因此產生強烈的凝聚意識，從而讓原本理性的活動走向暴力。自2018年年底持續迄今的法國「黃背心」運動，是個典型案例。該運動源起於民眾抗議政府調高油價，因示威者都身著黃背心而得名。活動的初始，採理性抗爭，隨著身著黃背心者蜂擁群集，群眾開始肆無忌憚的焚燒路邊汽車、砸毀周圍店鋪。同樣的，蒙面行為也屬於一種

共同性裝束，當所有抗議者都蒙面時，群情激憤下，場面極可能失控。

而站在執法者的立場，蒙面行為顯然是不利於偵查的。如果蒙面者僅有一人，尚可透過監視器比對行為人蒙面前、後動態，或以蒐集指紋、毛髮等方式驗證身分，然而當蒙面者群體行動時，採用同樣做法不僅難度大增，也喪失偵查經濟性；此外，倘若在同一事件中，有人蒙面、有人未蒙面，則最後可能變成以真面目示人者面臨刑事追訴、蒙面者則僥倖脫責的狀況，讓法律無法做到公平適用。長此以往，所有參與

者在理性抉擇下，都寧可選擇蒙面。屆時，執法者的蒐證難度、參與者之手段劇烈性，均將上升。

伍、結語

站在人權的立場，蒙面與否，是人身自由的一部分，每個人理應有自主選擇權。然而，此行為確實將提升犯罪的可能性及偵查的困難性，故在有條件情況下，仍應予以規範。如何在人權及社會安全之間拿捏恰當分際、避免淪為政治工具，成為政府必須面對的重要課題。





榮耀時刻 CRIMINAL BIMONTHLY



本局109年3月4日週報頒發刑俠仗義茶



本局109年3月18日
週報頒發刑俠仗義茶



本局109年4月8日
週報頒發刑俠仗義茶



局長率副局長、主任秘書，
於109年3月6日預祝女性同仁
婦女節快樂，致贈鮮花及合影(1)



局長率副局長、主任秘書，
於109年3月6日預祝女性同仁
婦女節快樂，致贈鮮花及合影(2)

注意嚴重特殊傳染性肺炎

公共空間請做好左列事項



避免接觸野生
動物、禽鳥



咳嗽戴口罩



肥皂勤洗手



14日內不適
戴口罩儘速就醫



少去傳統市場
醫院等人多場所

發燒者自主管理 不出入公共空間