

## 冒用人頭資料犯罪及相關防制對策

中央警察大學刑事警察學系教授兼主任 廖有祿  
高雄市政府警察局刑警大隊偵查員 江芝迎

### 目次

- 第一章 緒論
- 第二章 相關文獻探討
- 第三章 訪談資料分析
- 第四章 結論與建議

### 摘要

目前許多犯罪利用他人提供的個人證件及資料，申請大量人頭帳戶、人頭電話、人頭公司等，再利用這些工具來遂行犯罪或幫助降低犯罪風險，如擄人勒贖、利用人頭帳戶交付贖款，或是新興的詐欺犯罪集團利用人頭電話及帳戶進行詐騙等，冒用人頭資料的犯罪成為這些犯罪手法的前置作業，或是必要的工具，影響層面甚廣。政府陸續新增許多規定，透過內政部警政署、金融監督管理委員會、國家通訊傳播委員會等相關部門的聯合，希望能藉由更嚴格及周密的規定遏止冒用人頭資料犯罪的現象。

本文首先介紹目前政府防治冒用人頭資料的政策，接著再整合學者對這些政策的看法及建議。再藉由訪談冒用人頭犯罪的犯嫌及偵查人員，瞭解此類資料犯罪的流程及偵查方法，整理分析冒用人頭資料犯罪的特徵，藉此發展出偵查及預防的相關建議。

研究發現偵查此類犯罪需要從金融機構、電信機構調閱大量資料，提高此兩機構的配合度可以大幅強化偵查效率。而冒用人頭資料犯罪之預防，則應加強對民眾的教育宣導，減少提供資料的人頭。同時電信業者也應成立聯徵系統，不讓犯罪集團利用人頭資料申請大量電話，還要研發二類電信和網路電話的監管機制，減少電信安全的死角。此外對於販賣人頭資料行為應該儘速立法，使其單獨成罪，才能使此行為獲得適當的懲處，以嚇阻此類犯罪。

關鍵字：人頭帳戶、人頭電話、詐欺防治

## 第一章 緒論

### 第一節 社會背景

自由貿易的風氣席捲全國，台灣也逐步開放相關產業讓民營企業涉足，其中電信及金融業的自由化對我國影響甚鉅。開放民營企業進入金融、電信市場，自由競爭的情況雖然帶動經濟，卻也衍生出相關的犯罪問題。

電信市場及金融業的開放，讓電信及銀行公司大幅增加，許多業者為了搶佔市場，拓展大量便民措施，對客戶申請的資料未核實確認，衍生出電信金融的安全問題。會有如此情況產生，可能肇因政府為了推動經濟發展，於短期間內開放電信及金融市場，卻未能同時研擬完善的管理機制和配套措施，讓有心人士利用漏洞從事許多不同的犯罪手法，像新興的詐欺犯罪，讓全民人心惶惶，受害人數及金額不計其數。

經濟困難的遊民、貪小便宜者，會將自己的身分資料賣給他人，讓犯罪者利用收購而來的人頭帳戶、人頭電話、人頭證券交易戶等，遂行其他重大的犯罪，逃避警方追緝。歹徒擄人勒贖時，會利用人頭帳戶取款、人頭電話聯絡被害人；詐欺犯罪集團作案時，為避免警方追緝，和共犯也用人頭電話聯絡；還有利用人頭開公司，用以掩護非法交易或進行詐騙，甚至有心人士會利用人頭戶洗錢、炒股票，影響大者甚至有上億的違法資金流動。

新興詐欺犯罪更是其中影響最廣、禍害最深的，據統計詐欺案件的被害金額目前躍升為財產犯罪的第二名<sup>1</sup>，其犯案手法中，人頭帳戶及人頭電話正是不可或缺的必要工具。

如上所述，顯見冒用人頭資料的影響性，當它被歹徒濫用時所造成的犯罪，無論是類型、規模都相當複雜而龐大，也衝擊民眾對治安的信心，並增加偵辦難度。

人頭資料的冒用情形相當多，如人頭帳戶、人頭電話門號、人頭證券交易戶、人頭董事等，不勝枚舉。但目前實際情況中買賣人頭資料之行為，係以人頭帳戶、人頭電話數量較龐大且多用於新興詐欺犯罪，故本文討論重點以販賣收購人頭帳戶<sup>2</sup>及人頭電話為主。

### 第二節 防制冒用人頭資料犯罪之重要性

冒用人頭資料犯罪是指販賣人頭者自願將自己的名義提供收購者使用及犯罪，如人頭帳戶、人頭電話等，藉此換取金錢；而收購者也利用他人名義進行犯罪，躲避警方追查，如人頭帳戶、公司人頭、人頭電話等。

因為冒用人頭資料的手法是許多犯罪的基礎、重要的工具，想要預防犯罪，從源頭加以截堵是必要的作法。尤其是新興詐欺犯罪(用電話指示被害民眾到提款機前操作，藉此將被害者戶頭的金錢轉到人頭帳戶中)，不但受害民眾廣大，

<sup>1</sup> 第一名為竊盜犯罪。

<sup>2</sup> 此指在郵局及銀行等金融機構開立，存提款之用的帳戶，非指證券交易或其他帳戶。

人頭帳戶及人頭電話更是此犯罪手法的必要工具。此類販賣自己資料的行為量刑雖低，法律上甚至無法單獨成罪，但其實牽連甚廣，有加以防範的必要。但是針對此種犯行，國內不論檢警雙方的偵查作為，和政府機構的防制措施，都還有很大的改進空間。

本研究首先蒐集國內外對於人頭資料冒用的防制作為，以及多位學者所提出的防治建議，再根據對販賣、購買人頭資料者及偵查人員的深入訪談，全面理解其犯罪情形、動機、心路歷程，同時藉由整合、比對文獻資料及訪談內容，期能對冒用人頭資料犯罪有具體而完整的瞭解，研擬出法治面、偵查面及制度面更適合的防治對策。

### 第三節 冒用人頭資料的犯罪手法

對於冒用人頭資料的來源，主要可分成三種，一是偽造證件向銀行或公司申請資料，二是向販賣者購買已申請好的名義，如帳戶或電話，或是直接購買身分證件來申辦之。第三則是從非自願提供人頭資料者而來，如用拾獲的證件及用各種藉口騙取他人身分證件者來申辦人頭資料。目前因為身分證剛換新，偽造難度提升，加上申請人頭名義大都需要雙證件方能辦理，所以第一種情形的數量不高，而第三種情形則因為被冒用者多半沒有犯意，不涉及犯罪，所以本文主要討論的情況是以第二種，自願提供人頭資料供他人犯罪之情形。

## 第二章 相關文獻探討

### 第一節 冒用人頭資料犯罪的成因與防制

在此介紹學者認為冒用人頭資料的可能成因，接著再從相關部門：警方、電信、金融三方機構內部所採取的防制對策，深入理解目前人頭犯罪的防制方法及實務運作。

#### 一、冒用人頭資料犯罪的可能原因

冒用人頭資料的犯罪情形已存在許久，近幾年來政府相關部門戮力加強防制作為，實務上偽造或盜取他人資料犯罪之情形已有減少趨勢，但自願性販賣人頭資料仍不在少數，相關學者認為可能原因有以下四點<sup>3</sup>：

#### (一) 販賣人頭資料者缺少法律知識及責任觀

民眾普遍認為販賣人頭資料者對法律知識欠缺，常在責任意識不足的情況下，將人頭戶售予他人使用。

#### (二) 犯罪黑數偏高，人頭販賣者心存僥倖

犯罪黑數包含民眾未報案及警方未知或未登錄的犯罪案件，冒用人頭資料的犯罪如詐欺，常有許多被害人沒報案，使許多人在心存僥倖之

<sup>3</sup> 羅贊興、吳翰明、吳博聰、林宏錦(2007)，證券市場人頭戶之探討—從市場監視觀點評析(上)證交資料，第539期，頁16。

下以身試法。

(三) 司法實務對販售人頭資料者所科刑責過輕

法官於實務判決中，冒用人頭資料犯罪大都判為幫助詐欺取財罪，僅數月的刑期，還可易科罰金，對販售人頭資料犯罪者並無警惕作用。

(四) 金融機構徵信作業不確實，和警方配合度意願低

銀行規定金融機構臨櫃人員有義務對客戶身分、職業等進行徵信等查核作業及拒絕高風險客戶開戶，但因人力不足、工作時間繁忙、民眾會申訴抱怨服務不佳等情事，使人頭申辦帳戶的防制程序無法落實。

二、國內政府的防制措施

政府與詐欺犯罪集團的戰爭已經延續多年，早從 91 年起就開始提出相關政策，企圖減緩詐騙被害情勢，有學者就明確整理出政府為因應新興詐欺犯罪之防制對策，以下列出與冒用人頭資料犯罪的相關措施。

表一 政府防制冒用人頭資料犯罪之措施

| 日期       | 政府措施   |
|----------|--|
| 92.07.14 | 刑事警察局偵七隊及各市、縣警察局刑警隊成立「人頭帳戶犯罪案件專責處理、偵辦窗口」                             |
| 92.07.16 | 正式啟用「人頭資料庫」第一階段功能（警察局刑警隊可查詢）   |
| 92.10.20 | 警政署建置之「人頭資料庫」提供金融機構查詢  |
| 93.01.05 | 正式啟用「人頭資料庫」第二階段功能（分局刑事組亦可查詢）   |
| 93.03.30 | 金融機構落實執行「新開戶留存影像檔案」，並妥善管理該影像檔案，於檢警調機關調閱時，可適時提供                       |
| 93.04.21 | 行政院召集成立「中央跨部會聯合打擊利用電信、金融人頭帳戶犯罪」專案小組                                  |
| 93.04.23 | 召開「反詐騙跨部會協調會議」，針對利用電信、金融人頭帳戶犯罪，提出討論議題，協調解決機制，以有效遏制歹徒氣焰，回應民眾對政府最殷切的期盼 |
| 93.04.29 | 建立電信「雙卡查核機制」   |
| 93.05.01 | 建置「通聯調閱管理系統」，各業者應配合全面實施電子交換處理作業，落實內部管控機制，確保「聯絡窗口」二十四小時暢通             |
| 93.05.10 | 建立金融機構開戶「雙卡查核機制」，除留存該身分證明文件，還要留存影像資料                                 |
| 93.05.20 | 行政院金融監督管理委員會函請財金公司研議增加警示帳戶監察門號數量，由原本十線增加至二十線                         |
| 93.06.01 | 金融機構受理開戶，除客戶要求外，不提供金融卡非約定帳戶轉帳之功能                                     |
| 93.07.14 | 警察機關依警示通報機制，可由分局逕行發文查詢帳戶資金流向   |
| 93.08.01 | 警政署將0800 免付費電話改設置為「165」三碼反詐欺專線，並增加接聽電話之警力配置                          |
| 93.11.17 | 監察院對內政部警政署、行政院金融監督管理委員會銀行局及交通部電信總局提出糾正案（93 年第 146 號糾正文）              |
| 94.03.07 | 「限縮預付卡門號」規定國人及外勞均僅能限辦一個門號，且必須至直營門市辦理手續                               |

|          |  |
|----------|--|
| 95.02.22 | 交通部電信總局業務移交給「國家通訊傳播委員會」簡稱NCC，全力支援全民拼治安等作為                          |
| 95.04.06 | 刑事警察局整合通訊監察中心、資訊室、刑事研究發展室與偵九隊等單位正式成立「科技犯罪防制中心」，有效運用偵防資源，對抗新興型態科技犯罪 |
| 95.05.26 | NCC 正式啟動「電信事業網路總體檢」針對第一及第二類電信業者，分別實施行政檢查，調查違規事項並處分                 |
| 95.07.14 | NCC 成立「電信詐欺技術諮詢小組」針對電信詐騙技術進行研討與防制                                  |
| 95.11.01 | 警政署與金管會聯手啟動「警示帳戶聯防機制」，民眾可就近至金融機構報案，即時阻斷詐騙款項之提領                     |
| 96.03.26 | 金管會函文給中華民國證券商業同業公會，重申證券商應加強落實人頭戶管理                                 |
| 96.11.01 | 成立「聯合服務平台」方案，中華電信公司率先配合實施，全面提供民眾詐騙電話之諮詢服務                          |
| 97.03.11 | 「聯合服務平台」其他七大電信業者跟進投入「聯合服務平台」                                       |
| 98.05.12 | 165反詐騙專屬網站www.165.gov.tw開站，民眾亦可透過網路檢舉及報案                           |

資料來源：盧俊光(2006)，新興詐欺犯罪模式及其偵查作為之研究及本研究整理

為了打擊冒用人頭資料之犯罪，行政院出面結合金融、電信、警方等跨部會單位，以期遏止該類犯罪，雖然詐騙案件數已不再飆高，卻也未見減少，防治政策及相關作為還有改善的空間。

第二節 國外冒用人頭資料之防制政策

針對和我國冒用人頭情況相似的日本，以及近幾年受詐騙集團洗禮的韓國，簡單敘述兩國人頭帳戶防制及處罰規定<sup>4</sup>：

一、日本的防治作為

1. 金融機構防制規定

日本政府鑑於使用人頭帳戶的詐欺在日本日益嚴重，故於 2003 年 1 月 6 日正式施行「關於金融機構客戶之身份確認法」，該法希望可以達到健全金融機構及客戶管理體制之目的，以及確保司法機關針對犯罪組織犯罪收益及資金來源之情報蒐集。該法主要內容可分為以下幾個部分<sup>5</sup>：

(1) 明定「金融機構」之定義：

包括銀行、信用金庫、信用合作社、保險公司、證券公司、貸款業者、金融期貨交易者等。

(2) 確認本人義務及該紀錄之製作、保存：

金融機構受理客戶開立存款帳戶或高額現金（200 萬日幣以上）交易時，必須以當事人提出駕照、護照、健保證、居留證等政府機關發行

<sup>4</sup> 羅贊興、吳翰明、吳博聰、林宏錦（2007），證券市場人頭戶之探討--從市場監視觀點評析(上)，證交資料，第 539 期，頁 18。

<sup>5</sup> 古慧珍（2006），我國網路詐欺防制之研究—以使用人頭帳戶為中心，交通大學科技法律研究所碩士論文，頁 21-24。

之證明書類的方式，確認客戶（自然人）的姓名、住址及其出生年月日；如客戶為法人時其名稱及所在地。

另為防止以空頭公司或人頭冒領的情況發生，授權金融機構在簽訂存款契約（開戶）交易時的自然人（法人公司的代理人、受雇人等）與客戶（法人）有異時，必須對雙方（自然人及法人）均進行確認。另為確保自然人所填寫各種有關確認本人（自然人及法人）資料的真實性，明定禁止虛偽填寫確認本人的事項。又在製作確認本人紀錄後，即使在結清該帳戶後，該相關紀錄仍須保持七年。

(3) 明定金融機構進行金融等業務時，必須製作交易紀錄。同時，自交易之日起，該紀錄必須保存七年。

(4) 處罰規定：

A. 行政當局對違反本法確認本人義務及製作、保存交易紀錄的義務之規定時，得命令其採取改善之必要措施，對違反規定者，處兩年以下有期徒刑，或科或併科三百萬日幣以下罰金。

B. 對未提出與其業務相關報告、資料或提出虛偽的報告、資料者，處一年以下有期徒刑，或科或併科三百萬日幣以下罰金。

鑑於洗錢行為多利用金融機構進行，故日本〈組織犯罪處罰法〉規定疑似洗錢交易之申報制度。疑似洗錢交易申報制度之目的，除犯罪偵查外，亦有防止犯罪者利用金融機構存款之目的。而金融機構申報之可疑交易資料，係由金融廳作統一之整理、分析，如認申報之可疑交易資料足認為有犯罪收益等隱匿罪及其前提犯罪之事實時，得將相關情報提供給檢察官或司法警察機關。

## 2. 刑罰規定

日本的人頭戶問題和我國類似，日本在 2004 年 12 月修正〈本人確認法〉，改為〈本人確認及防止帳戶不當利用法〉，其制訂背景除和國際防制洗錢及反恐立法密切相關外，更受國內販賣人頭帳戶遂行的詐欺犯罪（和台灣所發生的詐欺類型相似）之案件數及受害規模激增有直接影響。以下就簡述該法防制帳戶濫用之部分：

(1) 若有以下行為，得處以五十萬日幣以下罰金，若為常業者，處兩年以下有期徒刑，或科或併科三百萬日幣以下罰金。

A. 若意圖冒充他人，也就是盜用他人帳簿之情形，或使第三人冒充他人的存款帳戶，而受讓、收受或取得與存款契約有關之存款帳簿、存款提領卡。

B. 非通常之商業交易或金融交易或無其他正當理由，而有償受讓、收受或取得存款帳簿等。

C. 明知他人有不正使用之目的，仍轉讓、交付或提供自己所有存款帳簿。

D. 非通常的商業交易或金融交易或無其他正當理由，而有償轉讓、交付或提供存款帳簿等。

(2) 若以勸誘、刊登廣告或其他類似之方法引誘他人犯前述之罪，處五十萬

日幣以下之罰金。

以上處罰之立法理由，是認定為轉讓他人使用而隱匿非為自己使用之意圖，向金融機構申請帳戶，符合詐取金融機構存摺存款的詐欺罪。而受讓自己存款帳戶則為贓物罪或詐欺罪的共犯。但是在「靜止帳戶」之情形，由於開戶時並無將帳戶轉讓他人使用之意，嗣後再轉讓帳戶行為並不構成詐欺罪。再者從實務觀察，存款帳戶自行為人手中取得後，常會經過層層轉手，中間轉手未必會有詐欺罪之共犯或贓物罪之共犯認識。故基於以上理由，將帳戶買賣依詐欺罪處罰其實有實際困難。

## 二、韓國的防治作為

和大多數國家相似，要能證明人頭戶知道購買自己帳戶者之「意圖」或「目的」。如無法證明，人頭戶不會被起訴。但是韓國的真名金融交易法案（Act on Real Name Financial Transactions）中禁止出借/借用帳戶，人頭戶可以因違反真名金融交易法而被起訴<sup>6</sup>。

日韓兩國是少數有針對販售及購買使用他人帳戶的行為加以處罰，作者認為此法可做為借鏡，並生警惕之效。

## 第三節 現有文獻對冒用人頭資料犯罪之防制建議

雖然針對於買賣人頭資料的犯罪研究不多，但是針對新興詐欺犯罪有不少的研究，許多研究都發現人頭帳戶及人頭電話的重要性，以下簡述其中對冒用人頭資料行為的防制建議：

### 一、整體防制建議

#### (一) 花一元，凍結帳戶

警方建議民眾一旦接到詐騙電話，要求從 ATM 轉帳，先花一元匯款後再報案。有匯款的動作，警方才有足夠的依據將匯款帳戶通報為警示帳戶凍結。詐騙集團買一個人頭帳戶大約要花一萬多元，而民眾用一元匯款，即可凍結此帳戶，提高犯罪成本。

#### (二) 加強教育宣導

許多自願性販售人頭者，社會知識水平不高，貪圖數千元蠅頭小利，將證件出售給他人，對之後可能會背負的民事及刑事責任並不清楚，因此應加強宣導販賣人頭資料者可能會有刑責，另外受理開戶的金融行員，也應對高風險之帳戶申請人說明可能責任。

#### (三) 嚴格查辦提供犯罪集團虛設公司行號之代辦商

犯罪集團為取信被害人，會請代辦商代為申辦公司行號及申請公司營利事業登記證，並將人頭登記為負責人，再用公司行號從事詐騙，建議經濟部商業司嚴格監督代辦商申請公司之程序及審核，並於事後追蹤經代辦公司申請核准設立之公司行號的經營情形，以防止犯罪集團利用

<sup>6</sup> 慶啟人（2007），防制人頭帳戶成為洗錢管道芻議，國會月刊，第 35 期，頁 33-35。

代辦商申請公司來從事犯罪行為<sup>7</sup>。

#### (四) 推動兩岸刑事司法互助機制

警方即便付出大量時間及精力向上追查人頭資料犯罪，但難有善果，因為大量的人頭電話及人頭帳戶都被新興詐欺犯罪集團所利用，而該犯罪集團為躲避司法管轄，常將總部置於大陸、越南地區，再以大陸地區之電話層層轉接，遙控指揮在台犯罪成員。但是由於兩岸長期缺乏合作打擊犯罪機制，犯罪集團利用兩岸政治藩籬，難以合作辦案此點，遊走法律漏洞。

台灣地區與大陸地區對打擊犯罪之合作，目前僅侷限在雙方有關偷渡犯及刑事犯遣返之合作，不擴及調查、取證、搜索、扣押等其他方面之刑事合作。但政府目前採取大三通政策，使兩岸經貿往來日益頻繁，故衍生的刑事案件層出不窮，罪犯藉穿梭兩岸逃避法律追緝。以台灣現行之刑事訴訟制度，對於刑事證據力的要求日趨嚴格，故目前對於兩岸跨境犯罪案件取證之要求，台灣比大陸更高，不過相信日後雙方往來更密切時，司法合作將對雙方都有利<sup>8</sup>。

#### (五) 單獨立法處罰提供人頭供他人犯罪之行為

現行法律對於提供自己名義供他人使用僅限於，該名義遭犯罪集團所利用，有被害人產生後；也就是需犯罪者利用名義構成犯罪後，提供者方依幫助犯懲罰。如提供人頭帳戶者尚在收購階段，未被用於犯罪即被發現，提供帳戶雖然收取賣金（已有得利行為），卻無法可罰。

為減少人頭資料不當使用，應仿照日本〈本人確認及防止帳戶不當利用法〉，單獨對提供自己名義供他人使用的行為立法處罰。然而日本立法只能處罰提供人頭帳戶之行為，無法處罰其他種類，如人頭電話、人頭公司、名義負責人等，但社會尚有許多濫用他人名義來犯罪之情形，故我國立法時不應只針對人頭帳戶，而應將要件擴展為提供自己名義供他人犯罪之行為。

## 二、人頭帳戶防制建議

### (一) 建立個人信用評等制度

應仿美、日等國，建立個人信用評等制度，而金融機構在開戶辦理徵信時，亦應比照放款一樣的嚴謹，且必須依據個人信用評等，若有瑕疵或評等不佳，即應拒絕開戶之申請，或經過一段猶豫觀察期間後始可准予開戶，唯有如此才能使每個人愛惜個人信用，有效降低人頭戶之使用及有利商業交易信用制度之建構。目前我國有以下幾種管道可得知個人之信用狀況：

1. 向銀行公會聯合徵信中心查詢大額退票紀錄、授信戶逾期催收呆帳變

<sup>7</sup> 賴添貴 (2005)，台灣地區經濟詐欺狀況處理與防制之實證研究，大葉大學事業經營研究所碩士論文，頁 133-134。

<sup>8</sup> 慶啟人 (2007)，防制人頭帳戶成為洗錢管道芻議，國會月刊，第 35 期，頁 92-94。

動資料查詢。

2. 向票據交換所查詢拒絕往來戶資料，包括信用卡停卡紀錄查詢，支存照會查詢等。

金融聯合徵信中心可比照信用卡等建立金融卡、存戶基本資料之徵信作為，金融機構凡受理開戶申請，應先向聯合徵信中心查詢已開戶數量、有無不良紀錄（如涉嫌詐欺或販賣帳戶供不法使用）或其他可疑狀況（如大量開戶而與身份、職業、所得顯不相當之情事）<sup>9</sup>。不能因貪圖業績或害怕得罪顧客而輕易受理，要建立起嚴格的個人金融信用評估制度，並強化聯合徵信中心資料庫的查詢功能，並對涉及提供或利用人頭帳戶犯罪之正犯，嚴格評估是否拒絕其金融業務往來，促使社會重視個人金融信用，杜絕人頭帳戶。

### (二) 開戶後進行持續性的客戶審查

目前對客戶審查之進行多是在開戶時，但持續性進行審查有助於發現犯罪、防制洗錢，如明顯可知為圖小利而開戶轉讓他人。對可疑交易之客戶應終止業務，製作可疑交易報告。

### (三) 整合查詢金融機構交易資料之平台

由於人頭帳戶交易資料查詢往往曠日費時，為避免延宕警方辦案時效，建議請金管會協調各金融機構，建立全國帳戶電腦連結平台，提供檢警查詢交易資料的單一窗口，讓調閱者可在最快時間取得所有轉帳及匯款流程資料，而不用讓地檢署和金融機構公文來往，耗時費力，並加速偵辦效率。

### (四) 提高相關之刑責

有學者認為依照我國實務之平均刑度，賣帳戶一案刑期約三至四個月，不足以嚇阻想要提供人頭帳戶以牟利之潛在犯罪者。因此應促請法官能同步加重個案之量刑，並能適度運用併科罰金之手段，來提高犯罪者之犯罪成本。

政府正全力遏止冒用人頭資料的犯罪，透過警方、金融業、國家通訊傳播委員會三方的通力合作，採取許多防治措施，並強化警方之偵查，希望能減少犯罪數。同時尚有不少學者都提出防制冒用人頭資料犯罪之相關建議，如鼓勵民眾報案，降低犯罪黑數；或是加重冒用人頭資料犯罪的刑責等，足見冒用人頭資料犯罪對社會風氣的負面影響。

## 第四節 研究方法

本研究首先對冒用人頭資料犯罪的案例加以分析，藉由案件的報案紀錄、筆錄、調查記錄、前科記錄、起訴書等資訊的吸收消化，對買賣資料雙方犯罪者的背景、犯罪過程、事發狀況有整體認識。同時清楚目前實務針對冒用人頭資料犯

<sup>9</sup> 古慧珍 (2006)，我國網路詐欺防制之研究—以使用人頭帳戶為中心，交通大學科技法律研究所碩士論文，頁 87-93。



罪的調查、逮捕、蒐證是如何運作；偵查重點為何，收購人頭者是怎樣利用報紙廣告、夾報來刊登收購消息，都希望能透過內容分析(context analysis)呈現出來。

其次本研究使用實地觀察法(field observation)，希望觀察網路來理解收購人頭資料者，如何利用此管道，暗中找尋有意願之賣家。觀察相關其中聯絡方式、頻率、用語等，來瞭解收購人頭資料的其中一個管道。

最後再根據對販賣、購買人頭資料者的深度訪談(in-depth interview)，對犯罪者特徵、動機、心路歷程、犯罪過程等有透徹的認識，最後透過偵查人員在實務上的分享，冀能導出對冒用人頭資料犯罪有效的預防及解決方針，方能對預防及偵查冒用人頭資料犯罪的政策有所助益。

### 第三章 訪談資料分析

#### 第一節 販賣人頭資料犯罪者特徵

根據對販賣人頭帳戶者的訪談內容發現，販賣人頭資料嫌疑人大都對販賣人頭帳戶的嚴重性及風險一知半解，犯案後也甚少會有罪惡感，還有不少人抱持僥倖的態度，貪圖小利才導致惡果，以下詳細說明之：

##### 一、不清楚販賣人頭帳戶的嚴重性和風險

收購人頭時會有很多說詞來欺騙人頭戶，比如說用於職棒簽賭，不算違法等，但不法份子常利用他人的帳戶及電話，進行犯罪來逃避警方追緝實屬社會常識，故將自己的人頭資料(如存簿、密碼)給陌生人使用並因此獲利，一樣成立幫助犯。但販賣者大都一知半解，缺乏社會常識及人際支援，被他人鼓吹而做了錯誤抉擇。

##### 二、短視近利

販賣人頭者都只考慮到馬上就可以到手的現金，卻不擔心事後的風險。就作者所知，他們並非皆處於經濟極度困頓的情形，只因需要用錢，便不加思索的選擇賣帳戶。

##### 三、犯案後很少有罪惡感

訪談時，全部受訪者對自己被關一事大都感到不值，沒有一位受訪者覺得做錯應受處罰，認為自己也是受害者。據作者分析，可能有以下原因：

##### (一) 不用直接面對被害人

販賣人頭資料者犯罪時，接觸的只是收購者，至於專門仲介人頭資料的犯罪者，也只是將帳戶賣給犯罪集團，沒有和被害人有直接互動，很難體會到被騙者無辜受害，積蓄全無的傷痛。

##### (二) 以自身資料換取金錢

提供自己個人資料來獲得金錢，對許多人而言是以物易物，把用個人資料賺取金錢認定是理所當然。

##### (三) 錯誤的自我角色認知

所有受訪者沒人感到內疚，將自己歸類為詐欺集團的替死鬼。但他

們賣人頭時對資料會被如何利用漠不關心，只想賺取金錢。既然貪圖不義之財的享受，那之後所判的刑期，就是應付代價。販賣人頭不是受害者，而是讓犯罪的幫兇。販賣人頭者應正確認識自身角色，不能將責任推給犯罪集團。

#### (四) 再犯可能性低

有些人因為同一個帳戶被匯進了兩、三位以上被害人的款項，一罪一罰後刑期累計高達一年，再加上許多販賣人頭者不是因山窮水盡才賣帳戶，所以對於被判刑後都相當懊悔，覺得不划算。

### 第二節 收購人頭資料犯罪模式及手法

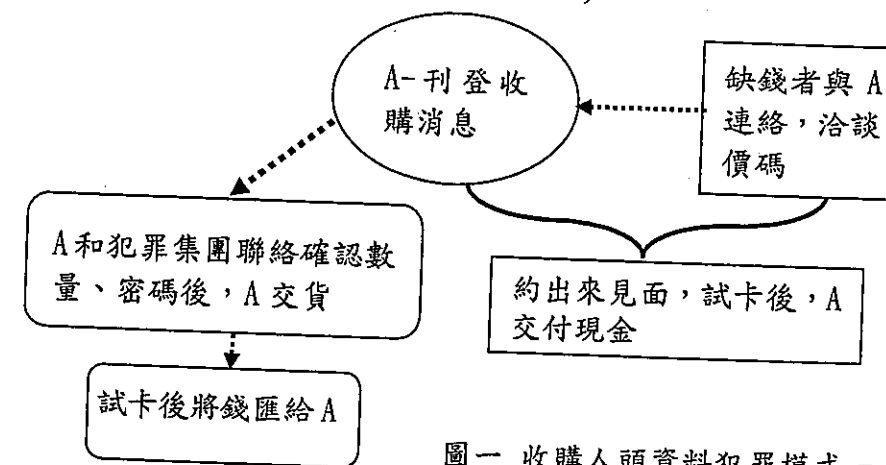
#### 一、收購人頭資料之模式

收購人頭資料早期都是新興詐欺集團因為犯案需要，由集團內部分工來完成，但因為犯罪市場需求量大增，所以近幾年也出現獨立運作的個體戶，本身不屬於任何犯罪集團，專門負責收購人頭資料再轉賣，賺取差價。同時也有主要依靠人頭來賺取金錢的犯罪集團，以下四種模式，即為目前大量收購人頭資料的犯罪方式，也是提供「黑市」人頭帳戶及人頭電話的主要供應來源。

##### (一) 獨立作業

也就是專門負責刊登消息，收購帳戶或電話，再將這些人頭資料轉賣給需要的集團或「公司」(指幫派)，賺取差價。獨立作業的模式如圖一，A為專門收購人頭資料的集團(約1~3人)，要收購帳戶必須先放出訊息，引來缺錢的人出賣自己的帳戶及電話。和對方連絡並談妥價碼後就會約出來交貨，要了解所買的帳戶和電話是否可以使用，所以會當場試卡，確認無誤後即交付現金。

A會透過各種管道，將帳戶或電話寄給犯罪集團，再由犯罪集團匯款給收購者的帳戶。A和詐欺集團只是交易關係，貨用「寄」的，雙方大都只有電話連絡，不曾會面(用虛線表示)。

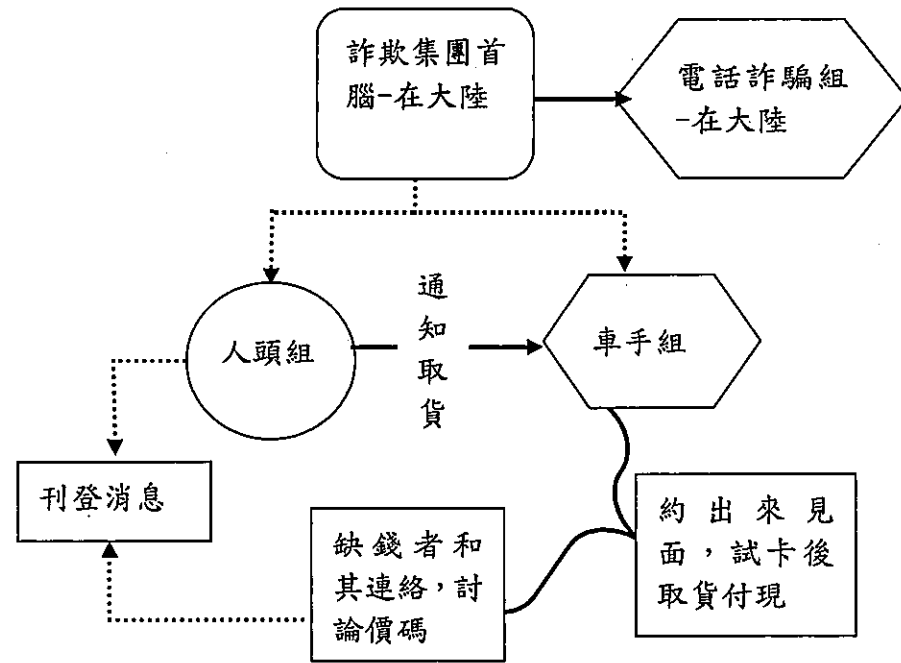


圖一 收購人頭資料犯罪模式一

(二) 新興詐欺犯罪集團內部的收購人頭組

新興詐欺集團裡面，分工細膩，其中首謀一般都在大陸以電話進行操控，只有車手(負責試卡、提領金錢)和車手頭才會留在台灣。對於收購人頭電話和人頭帳戶一般也都有專人負責。人頭組購買帳戶的流程和模式一雷同，最大的差別是改由車手去拿貨付錢。因為車手原本就是負責攜帶提款卡，定時試卡，在有需要時馬上利用 ATM 提錢。所以由他們領貨可以少了再交付的程序，而且人頭組的人也免去直接出面的風險。

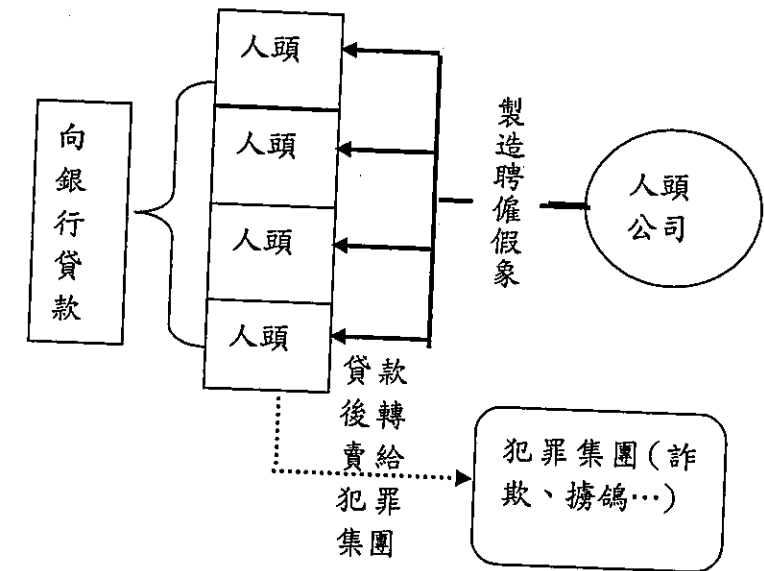
一般而言，人頭組只負責用電話和賣人頭者洽談，彼此不會見面。整個詐欺集團運作模式(如圖二)，在大陸首謀和台灣車手、人頭組也都只用電話連絡(用虛線表示)。



圖二 收購人頭資料犯罪模式二

(三) 以公司名義培養貸款人頭

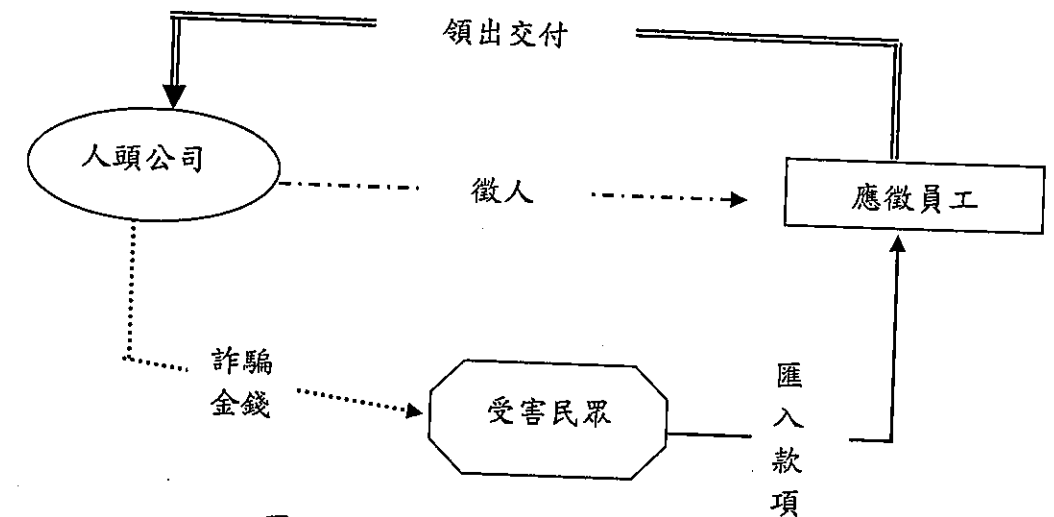
有些犯罪組織會利用「培養」人頭來賺錢。一開始先成立表面合法的營利公司，但負責人也是人頭，並非實際負責人。接著他們會自行培養人頭，找些遊民、吸毒等缺錢的人，帶領他們去辦電話、辦帳戶。同時利用公司名義定時做薪資轉帳、辦勞健保。還從公司戶頭持續定期撥款給這些人頭帳戶，並慢慢提出部分金額，這樣操作數個月，營造這些人頭在公司上班，有薪水的假象(放款和提出的都是同一批人)，達到銀行貸款的門檻後，就開始去貸款，培養一兩年後，過年繳完稅，就可拿完稅證明向銀行高額貸款。貸完款後，公司還會再要這些人申請門號、帳戶轉賣給詐騙集團，可說是利用殆盡(如圖三)。



圖三 收購人頭資料犯罪模式三

(四) 利用員工薪資轉帳帳戶當作人頭帳戶

犯罪集團以人頭公司名義在報紙、網路刊登應徵消息。對前來應徵之人假意任用後，就要求新進員工提供自己帳號，方便公司薪資轉帳。接著此犯罪集團在進行詐騙時，就會讓民眾將金額匯入這些員工帳號，之後再告知帳號本人，其帳戶內大量的金額是因為公司轉帳時操作錯誤，要求員工提領款項後交還公司，不知情的員工就成了犯罪集團的人頭帳戶兼車手。



圖四 收購人頭資料犯罪模式四

二、收購人頭資料之犯罪手法

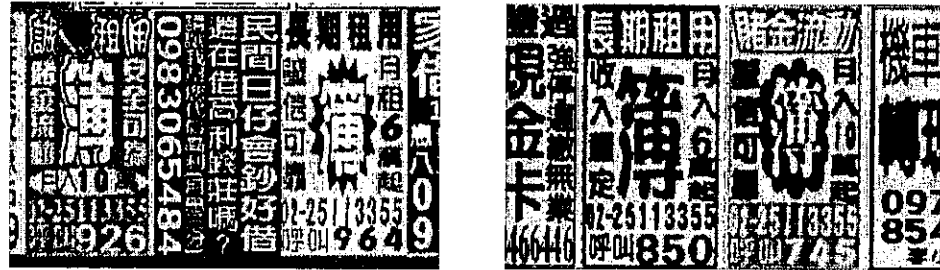
每個犯罪集團的操作模式雖然大致相同，但收購的細節及所用的說詞其實各

有千秋。

(一) 散佈收買人頭資料之管道

1. 刊登報紙廣告：

綜合訪談及筆錄所知，要散佈收買人頭的消息，最多人使用的就是在報上刊登小廣告，如「高收郵銀簿」、「小紅(指銀行存摺)3000，小綠(郵局存摺)5000」、「租用存簿，公司自用」、「簿，長期租用」、「賭金流動」等，如下圖：



自由時報 2009.03.25. 台

自由時報 2009.03.27.

圖五 報上刊登的廣告

收購人頭電話，則有「專收易付卡」，或一些代辦手機、門號的廣告，這類廣告有些是為了賺電信行差價，但也有在辦門號時留下雙證件資料，用申辦者名義多辦一張預付卡。所以有不少犯罪者和電信業者合作(多為二類電信業者)，藉此蒐購大量人頭電話卡，此外以公司名義也可大量申請電話門號。

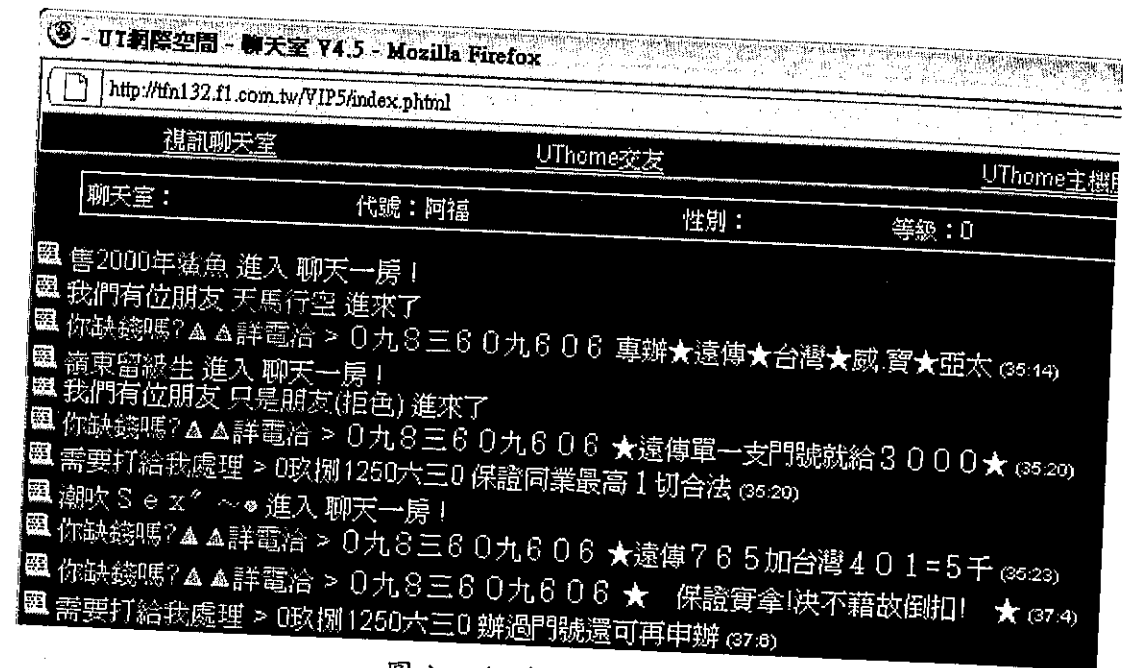
犯罪集團(如詐欺、擄鴿...)要購買人頭電話或帳戶時，只要打廣告上的電話，就可以和收買人頭資料者取得連絡，藉此大量「進貨」。

2. 雜誌及夾報

刊登內容及作法和上述雷同，也會刊登在跳蚤雜誌、報紙夾報裡。還有求職廣告，如小兵立大工的求職廣告，名義可能用「徵人，月入六萬」等，打電話過去後，接洽人表面上請人當車手，要求職者拿存簿、提款卡等，交由「公司」處理，或是請他辦帳戶，公司才能將薪水匯入；用諸如此類的名義，讓不少求職者交出個人的個人資料，成為人頭。

3. 網路聊天室

在網路上有許多免費的聊天室，一天內會有上千個人次進出瀏覽、聊天。有心人就可以藉由上面的暱稱、留言，散發訊息，「缺錢者請密我」、「門號一支三千」，如圖六。主動丟訊息想問詳情時，他就會要求你在 MSN 或 YAHOO 交友以進一步討論，以免在網路上丟公開的訊息而被電信警察盯上。



圖六 網路聊天室散布訊息

(二) 吸收人頭的方式

如犯罪模式三所述，有些人頭不只會提供自己的帳戶、提款卡等，若是要向銀行辦貸款，申辦帳戶、電話，就需要人頭的詳細資料、證件，也會需要本人出面。這時就必須清楚掌握人頭的聯絡方式、住址來確保他們隨傳隨到。而這種多半由公司「業務」來負責，業務有些是地方幫派，他會掌握手底下的新人，業務也有毒品供應者，向他買毒品的人就可以吸收成為人頭。也有的業務之前經營過當舖，就會認識缺錢的人及遊民，如此透過認識的人輾轉介紹、拉人正是人頭公司吸收人頭的主要方式。

(三) 收購人頭帳戶之說詞

為了讓賣人頭資料者放鬆戒心，收購帳戶會用很多名義和說詞，簡單整理如下：

1. 公司自用：假藉公司需要節稅或作外資匯入，不會違法。一位受訪者曾說明，對方不但穿著西裝筆挺，還自稱為經理秘書，備有名片，如此面面俱到，很容易就取得信任。
2. 地下簽賭：偽稱為地下職棒簽賭，需要用他人的戶頭來「洗」賭金，不算違法。
3. 長期租用：號稱租一月一萬，十五天就會先付五千。但出租的戶頭往往兩三天後就會變成警示帳戶，根本不需用到十五天。
4. 貸款需要：也有收購帳戶者一開始的名義是幫助貸款，等見面後再跟人頭解釋，若是申辦貸款需要申請薪資證明等，要求人頭把自己的證件、存摺、提款卡、印章、密碼都給他，才方便辦貸款。販賣者有些



是真的相信，或隱約猜到帳戶可能的用途，但利字當頭下還是同意了。

### 三、收購人頭資料之種類及利潤

對於所收購的人頭帳戶，因為申辦銀行的不同價位會有差異，但平均收購一個帳戶約五千至一萬元，再轉賣可賣一萬至兩萬元，而手機門號分為預付卡門號及月租型門號，價格約如表二，不論人頭帳戶或人頭門號，轉賣的利潤皆相當高。

表二 收購轉賣電話門號之價格

| 門號種類  | 初購(收購價碼)    | 轉賣(賣給犯罪集團價碼) |
|-------|-------------|--------------|
| 月租型門號 | 1000元~2000元 | 3000元        |
| 預付卡門號 | 500元~1000元  | 1500元~1800元  |

資料來源：本研究透過官方案例資料整理

## 第三節 冒用人頭資料犯罪特徵

綜合以上資料分析，統整後發現冒用人頭資料犯罪和其他犯罪相較下，有以下幾項特徵：

### 一、量刑長短差異極大

因為冒用人頭資料犯罪並無單獨成罪，同時在連續犯被刪除後，一罪一罰的規定，讓如今冒用人頭資料犯罪的刑期呈現出很弔詭的情況。如先前所述，就算賣了人頭帳戶，只要買家尚未用於犯罪，或是被害人不出面報案，一樣是無罪名成立。

但如果某人所賣的帳戶，有三筆被害人金額匯入過，那這個帳戶的所有人，就必須被罰三倍的刑期，以初犯約3~4個月乘以三，將近一年。

但是就販賣人頭電話而言，犯罪次數就不會像人頭帳戶一樣因此倍增。同樣的若帳戶被用於詐欺犯罪，犯罪所得又剛好高過五百萬，那此人頭帳戶的所有人，還可依洗錢防制法來論處，和刑法§339「處五年以下有期徒刑、拘役或科或併科一千元以下罰金」相比，洗錢防制法§11規定為「處五年以下有期徒刑，得併科新臺幣三百萬元以下罰金」，更提高了罰金的額度。

同樣是販賣個人資料牟利，但刑期卻是依「運氣好壞」決定，和希望透過法律來實現公平正義的大相逕庭，民眾無法適從，也會對法治安定性造成負面影響。

### 二、供貨量及需求量皆大

本研究一開始就說明，冒用人頭資料是許多如新興詐欺集團、擄鴿勒贖等犯罪的基本「工具」，在「犯罪市場」需求量極大的情形下，使得買人頭資料的價位拉抬得很高。如此吸引眾多短視近利的民眾，在金錢的誘惑下成為犯罪者的幫兇。

此外經濟的不景氣，除了直接讓窮困潦倒的百姓和急需毒品的成癮者，樂意提供自己的資料換取現金；同時也間接提高社會的犯罪率，刺激犯罪增長。在此

惡性循環的趨勢來看，冒用人頭資料犯罪，政府若不出面建立完善的制度加以遏止，恐怕會越演越烈。

### 三、查獲時間長短不一

作者整理資料時發現犯罪後被查獲的時間差異極大，還出現販賣帳戶三五年後方被警查獲的情況，會有如此情形，是因犯罪成立全看人頭買家如何運用這些帳戶及電話而定，若是用在成立人頭公司，那就會比用做詐欺犯罪的洗錢帳戶更晚被發現。因為買家買到會如何運用，何時「犯罪」會成立，都是未知數。也有人頭資料被轉手賣過幾輪(如代辦公司貸款後又賣給詐欺集團)，再被警察查獲。

然而賣人頭資料五年後，才找到嫌疑人處罰，當時犯罪細節多已不復記憶，追查收購者身分更是難上加難，而在犯罪這麼久的期間後才面臨刑期，使刑罰對個人的懲戒性、教育意義也大幅降低。

### 四、犯罪難度低且獲利高

前述收購人頭帳戶之利潤，對某些人而言，賣人頭資料是無本的好交易，因為申請帳戶和電話都是輕而易舉的事，不如竊盜、搶劫需要體力、技術，難度低，犯罪時也沒有風險。因為販賣人頭資料的犯罪性質如此，故犯罪年齡分布廣，男女比例較為平均。

## 第四節 偵查困境

### 一、偵查冒用人頭資料犯罪的意願較低

分析警察對偵查冒用人頭資料犯罪意願較低的原因有：

#### (一) 行政獎勵低

對偵查人員而言，案件偵破最直接的鼓舞就是行政獎勵。早年新興詐欺集團相當猖獗時，對詐欺犯罪的行政獎勵頗高，但是民國九十六年時，獎勵全部砍半，此舉大大影響士氣。尤其詐欺案件偵辦起來相當困難，而犯罪者又懂得與時俱進，善用各類高科技通訊來躲避偵查。在吃力不討好的情況下，願意投入心力偵辦此類犯罪之人必會大為減少。

#### (二) 耗時費力

要偵辦此類犯罪，追查帳戶所有人、使用者、使用記錄等，警方常需至金融機構調閱相關資料。但因為目前銀行業者眾多，要調閱相關資料須透過公文往返、曠日費時。

如要調某犯罪者名下所有帳戶，所需時間可能為二週至一個月，再調閱所有帳戶之交易明細又需二週至一個月，如此類推，可能已過了聲請續監之期限或路口監視器畫面的保存期限。所以從追查到破案，監聽數個月後到分析整理證物，發公文調帳戶，一個案件可能需半年以上才能處理完，甚至更久。

再加上目前警方欲調閱通聯紀錄，需要按日計費，一個門號一日的雙向通聯資料就要120元，然而有時可疑的門號可能多達十幾個，如此累積下來花費的金額相當可觀。破案難度高，花費時間長，行政獎勵又

低，自然警方在面對此類案件時不願投注太多精力。

### (三) 難以斬草除根

案件破獲，成就感也是影響警方意願的要素。在實務上能破獲整個犯罪集團並逮捕主謀的情況並不多。針對人頭帳戶而言，要追查出版賣者較容易，查到收購者比較困難，有很多收購者始終隱身幕後，交代下游的收購者收到存簿後用快遞寄給他，主謀再寄給負責提款的車手，但車手和主謀一來一往間都只用電話聯絡，從未見過面，很難循線上查。

若是詐欺集團中負責收購帳戶者，很多負責人更是身在大陸或越南，警方大都只聞其「聲」，未見其人。無法將犯罪集團全體破獲，只逮捕到下游車手或人頭，令偵辦者心有不甘，士氣低落。

## 二、冒用人頭資料犯罪難以根絕

依目前形勢來看，人頭電話及人頭帳戶，是許多犯罪不可或缺的「工具」，故收購價碼相當高。賣帳戶對很多人而言，尤其部分生活潦倒的遊民，是難以拒絕的選擇。還有就是吸毒者，毒癮發作的痛苦，更讓他們不擇手段地希望能馬上得到金錢買毒品，販賣人頭資料的行為就某種程度上，可謂經濟不景氣的反應，大環境的影響讓此一犯罪難以杜絕。

## 三、偵查冒用人頭資料犯罪之法律問題

### (一) 冒用人頭資料犯罪無法單獨成罪

目前對於購買和販售人頭帳戶的行為，若是沒有用於犯罪即不成罪。曾有警方於購買帳戶的犯罪者家中搜出記載帳號密碼的筆記本，但對尚未有錢匯進去的帳戶所有人，儘管知道有收購和販賣人頭帳戶的情事，卻無法做任何處理。

被害人不願報案的情形也會直接影響到刑期長短，有些帳戶匯了三筆不同被害人的詐騙金額，有些則是一筆。在一罪一罰的情況下，使同一個販賣帳戶的行為，刑期從無到有，產生極大的落差。

### (二) 洗錢防制法

對於販賣人頭帳戶的行為，早期原本可以成立洗錢防制法的幫助犯，由於詐欺得利大都透過地下匯兌的方式把錢匯到對岸，而這些用於地下匯兌的人頭帳戶，也只能透過洗錢防制法加以處罰。目前洗錢防制法§3規定：「下列各款之罪，其犯罪所得在新臺幣五百萬元以上者，亦屬重大犯罪：一、刑法第三百三十六條第二項、第三百三十九條、第三百四十四條之罪。」所以只要詐欺犯罪所得超過五百萬，也能適用洗錢防制法。

但五百萬的所得依高雄地方法院法官曾仁勇認為，不應合併計算。在詐欺犯罪中，常是大量民眾被騙，累計金額達上億，但一次要達五百萬以上的門檻過高，可能會導致詐欺犯罪的洗錢行為無法可罰。

## 第四章 結論與建議

### 第一節 研究發現

本研究對官方案例、質性訪談等資料綜合分析後，對冒用人頭犯罪的特性及概況有一定的了解，以下簡單歸納之：

#### 一、冒用人頭資料犯罪之模式及手法

不同犯罪者會用相異的犯罪方式來達成目的，同時也會施用各種手段逃避警方追緝，如下所述：

##### (一) 犯罪模式

犯罪模式主要有三種，其中獨立作業的手法最原始及粗糙，而詐欺集團和人頭公司的組織型犯罪模式，分工精細，獲利也更高，而首謀大都隱身幕後，難以逮捕。其中可以發現此類犯罪的犯罪者除非必要，不直接碰面，降低警方連帶擊破的風險，因此常利用電話及快遞交貨，而這也成為警方突破案情的關鍵。

##### (二) 犯罪手法

收購人頭的方式主要是透過刊登在報紙、雜誌的廣告，到聊天室散布相關訊息，等有意販售者主動連絡，也會因為認識的人介紹，拉攏成為人頭。同時為了取信於提供人頭者，還會編撰出許多說詞如出租帳簿、公司自用等，讓不少人在懵懂的情況下，為了利益出賣自己的信用。

##### (三) 躲避偵查之方式

為了避免警方追緝，犯罪者不論是刊登廣告、互相聯絡或是交貨取貨時都要大費周章。使用難以追查的通訊方式如地下機房、網路電話。利用間接方式完成犯罪，如廣告上使用電話秘書而不直接留手機；取貨時利用快遞或放置寄物櫃來取代直接面交。其中對警方影響最大的問題為通訊方式，人頭卡及地下機房的使用，已成為電信安全上的死角。

## 二、偵查冒用人頭犯罪的困境

逮捕販賣人頭資料者，困難度不高。但要逮捕收購者以及組織背後的主嫌，就變得相當複雜，需要投入大量時間及精力。在實務上冒用人頭資料犯罪被大舉破獲的情況不多，因為主謀者多不在台灣，向上追查的難度高，且偵辦需要公文往來調閱資料、長期監聽分析內容，耗時又費力，行政獎勵又不高，令許多員警不願投入大量心力偵辦此類型犯罪。

而且就算警方深入追查，此種犯罪的主謀大都躲在外地，難以就逮。就算想要追捕較下游的人頭資料提供者，有時也因受害者不願出面報案，使提供人頭的行為無法成罪。再加上大環境經濟不景氣，使得想要提供人頭資料換錢的民眾源源不絕，犯罪趨勢難以減緩。

## 三、冒用人頭資料犯罪之特徵

本研究分析後得出冒用人頭資料犯罪及嫌疑人的特徵，歸納如下：

### (一) 犯罪者特徵

本研究藉由收集嫌疑人的背景資料，而分析出提供人頭資料的犯罪者特徵，其中因為此種類型犯罪不需要體力，犯罪行為時風險又低，所以提供人頭資料犯罪的男女比率較其他犯罪類型(如搶劫、殺人)接近，年齡層也較為提高。

此外利用販賣人頭資料來獲益者，並非如所預期的是在山窮水盡的情況下才會從事。有不少人居住家裡而且家境小康，或是有工作收入，只因為一時缺錢加上相信收購者的說詞，就同意提供自己的帳戶被用作犯罪。

## (二) 犯罪特徵

針對冒用人頭資料犯罪，有幾項特徵：首先因為提供人頭資料的幫助犯行為，罪名數量依使用者決定，故相同的行為，刑期差異卻頗大；而被發現時間也要視使用者如何利用，查獲時間長短也不甚固定。再來受環境影響，財產犯罪數量居高不下，讓冒用人頭資料犯罪的供貨量和需求量甚為龐大。

此種犯罪難度低，不需要體力或技術，而且不論是販售、收購人頭資料，或是使用這些人頭資料犯罪，利潤都相當高。其中提供人頭資料的嫌疑人，多認為自己只是用個人資料換取金錢，犯案時很少有罪惡感。

理解這些犯罪特徵後，也能明白為何此類的犯罪數量會如此龐大，使警方抓不勝抓。

## 第二節 討論

前曾提及許多學者對冒用人頭資料犯罪提出相關看法，在此和本研究發現互相比較，討論其中異同。

### 一、冒用人頭資料犯罪的可能成因

學者曾提及成因可能有：1.販賣人頭資料者缺少法律知識及責任觀、2.犯罪黑數高，嫌疑人心存僥倖、3.司法實務對販售人頭資料者所科刑責過輕、4.金融機構徵信作業不確實，和警方配合度低。本研究發現，確實有許多嫌疑人在提供人頭資料時根本不知事情的嚴重性，對刑責懵懵懂懂。確實有人因為朋友賣過沒事後心存僥倖，同樣選擇以資料換取金錢，但本研究發現未必是犯罪黑數高所導致，因為提供人頭者的逮捕上並無困難，但是有些人頭資料尚未被用於犯罪，所以查獲時間不一；或是受害者不願報案，使得販賣人頭資料行為無法成罪。

至於司法實務的刑責，其實在一罪一罰的情況下已經頗重。許多受訪者也明確的表示，就算被判三個月只換數千元，相當不值得。再來是金融機構的徵信作業不確實，在目前金管會一再要求下，辦理帳戶前的認識客戶(Know Your Customer)政策已經落實，而且當客戶在短期內要辦兩個以上的帳戶，銀行行員也會多方確認，接受申請的態度已相當嚴謹。

### 二、先前研究對冒用人頭資料犯罪的防制建議

在本研究對實務有深入了解後，先前所提的防制建議如：加強教育宣導、提高民眾報案率、嚴格查辦犯罪集團虛設公司行號等，和研究者的發現大致相符。

但是有些政策在當前情勢發展下並不適合，以下說明之。先前所推動的「花一元，凍結帳戶」的作法，之前有民眾配合使用過，結果卻遭到詐欺集團的報復，如撥打大量威脅、恐嚇電話，代點大量外送食物，更有甚者將民眾帳號用作人頭帳戶，讓被騙民眾匯入少量金額後被檢舉，於是熱心民眾的帳號就被設為警示帳戶，多費波折方能解除，故警方後來也不敢再鼓勵民眾用此方法凍結詐騙帳戶。

還有加重刑期來防制民眾販賣自己資料，就研究者發現，儘管只有三個月的刑期，但對只有獲利數千元的民眾而言，已相當具有警惕作用，再犯意願不高。若要加重刑期，作者認為應針對累犯和收購帳戶者。

之前學者所提的許多建議雖然都相當精闢而實際，但是犯罪手法經過時間演變，防制方式也要隨之改變，才能發揮效果。

## 第三節 研究建議

### 一、偵查冒用人頭資料犯罪之建議

偵查作為的討論重心主要是針對負責收購人頭資料轉賣的犯罪者。在實務上冒用人頭資料犯罪之偵查，大都被視為偵辦詐欺犯罪的一環，冒用人頭資料犯罪和詐欺犯罪可說是環環相扣。

#### (一) 建立查詢金融交易資料之平台

同前文所述，想要偵破此類犯罪，掌握時效就相當重要，但是依照目前體制來說，因為要調閱銀行交易明細，總需要利用公文往返，相當耗費時間。若是能整合所有金融機構的帳戶交易資料，建立整合的查詢平台，並對檢警開放權限。對有可疑帳號的交易資訊、時間、地點，就能迅速的得到資訊。同時面對會將帳戶轉過幾層再提領的情況，也不用透過公文的來往，才能一層層的分析出帳戶所有人、提款時間和地點，如此效率必能大幅提高，改善破案成效。

#### (二) 降低通聯調閱費用

通聯費用對偵辦案件的偵查員，往往都是一大負擔。對於電信業者而言，警方逮捕濫用人頭電話的詐欺集團，也可以減少電信業者欠費不繳的呆帳，對電信公司而言其實也是間接得利。以國家調查犯罪的立場，就算調閱通聯需要耗費機器、人事成本，相關單位本就有配合的義務。若能設法降低通聯費用，對警方偵查犯罪的幫助頗大。

#### (三) 加強兩岸司法互助

要減少冒用人頭資料的犯罪，遏止「市場需求」相當重要，想要降低此種人頭需求，就必須破獲詐欺集團，減少詐騙次數。其實以台灣目前在偵破詐欺集團上，並非沒有能力查到首謀，有時好不容易透過層層分析，向上追循，查出主嫌身分，總是人不在本島，沒有辦法逮捕歸案。若是兩岸能建立司法互助，幫忙遣返這些主嫌，相信能對詐欺集團造成重大打擊。

#### (四) 提高偵辦詐欺的行政獎勵

詐欺案件的偵破難度很高，對許多地方單位來說，與其要花半年的時間去監聽、破獲一個集團，其中獲得的嘉獎支數可能遠不如在相同的時間，去逮捕毒犯、查找贓車。對案件破獲難度高、需時長的詐欺犯罪，目前訂定的獎勵額度明顯過低，嚴重影響警方辦案意願和投入程度。故應比照偵辦詐欺的難度提高額度，對辛苦偵辦的警方才算合理。

#### (五) 強化二類電信、網路電話的管理

犯罪者為了逃避警方監聽，運用許多通訊方式，例如透過二類電信可以節省費用，同時增加警方偵辦難度。警方若調閱通聯，出現二類電信的代表號，還必須行文至二類電信業者調出時間內所有使用者，增加警方監聽及偵辦的難度。

目前網路電話逐漸盛行，然而其所使用的通訊方式也最令警方頭疼，因為網路電話為了選擇最便宜的方式，會轉經多種線路，包括網路、有線電話及行動電話，這讓警方光是要追出一通電話的發話地，就必須透過層層步驟，更遑論要監聽通話內容。

在警方尚未發展出完善的管理機制，就先行開放二類電信、網路電話的使用，讓電信安全產生漏洞，使犯罪者有機可乘。如今開放已成事實，為今之計只好努力發展可以監控二類電信、網路電話的管控機制和設備，並強制要求這些單位在警方偵查調閱資料時的回應效率和配合度，以提高辦案績效。

#### (六) 追緝犯罪者虛設的公司

犯罪集團用人頭當負責人，虛設公司行號，利用公司名義來違法賺取金錢，對社會治安、經濟狀況影響極大：

1. 成立人頭公司後，表面上合法經營，就可利用公司名義，幫其他業者開立空白發票，幫助其他公司非法逃漏稅，紊亂國內稅制。
2. 以公司名義可以申辦大量的電話門號，一般民眾在同家電信業者一次只能申辦兩~三個門號，但以公司負責人的名義就能大量申請，這些門號最後大都淪為犯罪工具。
3. 犯罪者成立人頭公司，會偽造薪資轉帳證明，利用底下的人頭，向銀行大量貸款。
4. 人頭公司貸款後還會將這些人頭資料再度轉賣給詐欺集團，成為人頭供應商。

可見違法的人頭公司對社會、經濟都會帶來相當大的衝擊，不只檢警雙方應投注更多心力加以查緝，金融相關單位也應全力配合，剷除此類犯罪組織。

#### (七) 查緝地下機房

不管是哪類案件，地下機房一直是警方偵辦上的阻礙。不但大幅降低詐騙集團撥打電話的通話費，也讓警方無法從基地台位置判斷犯罪者所在。若能掃蕩大型地下機房，對詐欺集團、各類犯罪的偵查都會有極

有助益<sup>10</sup>。

## 二、防治冒用人頭資料犯罪之建議

對於防治層面而言，就是著重在販賣人頭資料者，透過合理的控管及限制，遏止嫌疑人出賣自己資料求利之行為。

### (一) 教育宣導

對於提供人頭資料供人使用，多會淪為犯罪工具，也極易被警方逮捕入獄，很多民眾確實對此懵懂無知，因為一時缺錢，又輕信犯罪者的花言巧語，一時不慎淪為犯罪集團的犧牲品及幫兇。所以讓百姓正確認識到儘管只有提供資料，依然會成為犯罪的幫兇、加害者，而且事後所獲判的刑責就算可易科罰金，也需付出當時所得的數十倍。販賣人頭資料行為的負面影響，不但要透過文宣、報紙等平面宣導，也應多利用電視廣告等更輕鬆的方法，讓更多民眾能了解此一資訊。

### (二) 加強查緝幫助洗錢的地下匯兌

以往的研究及偵查只注重犯罪者本身，很少顧及地下匯兌。但地下匯兌所使用的帳戶多是人頭帳戶，而且透過大筆的贓款流入，地下匯兌業者從幫助洗錢中獲取豐厚利益，本應加以懲處。而且許多詐欺集團主嫌都不住台灣，都透過頻繁的地下匯兌才拿到詐騙金額，相當依賴這個體系。若是檢警調能對此種違法行為戮力偵辦，進而偵破地下匯兌的業者，無疑也會讓詐欺集團的金流浮出檯面，更容易掌握。

### (三) 電信業者成立聯徵系統

銀行成立的金融聯合徵信中心，是為了保持資訊流通，確保與銀行往來的都是安全的顧客。聯徵中心就像資料庫，是資料保管交換的中心，資料都是有關於金融機構與自然人或法人往來的債信情形，由銀行提供再進行彙整，提供銀行做查詢。故銀行對可疑的客戶，如短期內頻繁開戶、或是曾經被列為警示帳戶，就可以預先警示，在開戶時更詳實完成徵信工作。

然而因為聯徵中心只針對金融機構的債信往來，若在電信公司欠費未繳，則不會有相關警示機制。若是有人在中華電信公司申辦門號，大量撥打卻不繳費，那此人就算去亞太、遠傳等公司所申辦的門號，應該也會面臨一樣的情形。再說一般人會用的門號多則兩~三支，若有人短時間內申辦了大量門號、預付卡，此種異常的使用情形，若是電信業也有聯徵中心，就可以預先警示，不但可以減少大量欠款不繳的電信呆帳，更可避免人頭電話被用作犯罪工具。

### (四) 金融聯合徵信中心的配合

最新洗錢防治法有規定，每當銀行發現可疑金流或帳戶時，應通報洗錢防治中心，若能規定銀行要通報的單位也包含警方，警方便能先一

<sup>10</sup> 在台北破獲一處大型地下機房後，單日的詐騙件數就少了 105 件，PChome 新聞，2009/03/20，<http://news.pchome.com.tw/society/bcc/20090320/index-12375387571682321002.html>

步掌握嫌疑人的犯罪及洗錢行為。

#### (五) 立法建議

在冒用人頭資料犯罪上，法律的相關規定在實務適用上其實有頗多爭議，本研究也對此做了不少討論。以下僅列出對於立法的建議：

##### 1. 立法限制個人開戶及申辦門號之權限

對於一般人來說，除非有特殊情況，否則會用到的帳戶及門號皆是有限的。曾有嫌疑人一共賣了十一個帳戶，對於非公司負責人或從事金融相關工作者，會申辦十一個帳戶就相當可疑，對此法律應該有所限制，特別是曾經帳戶及門號被列警示的人，更要小心其有再犯可能。還有不只數量上應該限制，有前科之人申辦使用帳戶的權限，比如說網路銀行之功能也可以考慮設限。

##### 2. 洗錢防制法

洗錢防制的罰責較刑法重，警惕效果也更好，但須一次詐欺犯罪所得五百萬以上，方能適用。規定若能改成該集團犯罪所得總和達五百萬以上，會較符合實際情形。

##### 3. 單獨立法處罰對冒用人頭資料犯罪之行為

目前實務上以幫助犯的名義懲處提供人頭資料者，但產生兩個問題，一是造成目前販賣資料者的刑期長短不一，二是不一定會成罪，使販售資料者心存僥倖。故可仿照日本立法，對提供人頭資料供人犯罪之行為單獨成罪，不用依附隨後的犯罪行為來判刑。

日本的〈本人確認及防止帳戶不當利用法〉，雖有處罰提供人頭帳戶供他人使用的情形，但是對於人頭電話、人頭公司就無法適用。學者慶啟人於國會月刊曾發表「防制人頭帳戶成為洗錢管道芻議」一文中，提及為了能讓立法涵蓋面向更完整，不應只侷限在人頭帳戶，而建議在刑法第二一五條之後增訂如下條文<sup>11</sup>：

第二一五條之一：「無商業或金融交易之正當理由而提供自己名義予他人使用者，處五年以下有期徒刑、拘役或科或併科五萬元以下罰金」。

「無商業或金融交易之正當理由而取得或利用他人名義者，亦同」。

作者認為是可以參考的想法，因為對於人頭電話、人頭公司等其餘名義也適用此法處罰，和日本的〈本人確認及防止帳戶不當利用法〉相較下更加完善，較適合國情。

雖然民眾目前對詐騙集團都有一定的警覺心，但是詐欺集團不斷更新詐騙手法，導致還是有民眾持續上當，詐欺案件數仍居高不下，詐騙手段推陳出新，政府防制對策也該識時通變，抑制冒用人頭資料之情事，不予犯罪集團有可趁之機。

<sup>11</sup> 慶啟人(2007)，防制人頭帳戶成為洗錢管道芻議，國會月刊，第35期，頁94-95。

## 參考文獻

### 一、書籍

1. 內政部警政署(2007)，警政工作年報，內政部警政署出版。
2. 許春金(2006)，犯罪學，中央警察大學出版。
3. 蔡蒼柏主編(2006)，經濟犯罪偵查實務，元照出版有限公司。

### 二、期刊

1. 田習如(1999)，危機企業相關人自保守則，財訊，第201期，頁258-261。
2. 吳克昌(2002)，詐騙集團利用人頭戶以違約詐財案之檢討，證交資料，第478期，頁25-35。
3. 林宜隆、吳清海、吳柏霖(2007)，電話詐欺犯罪分析與偵查模式之研究，執法新知論衡，第四卷第一期，頁35-36。
4. 郭宗雄(2001)，談人頭董事之防制，實用稅務，第316期，頁69-74。
5. 高武義(2004)，防範人頭及冒名開戶因應措施之探討，今日合庫，第350期，頁62-81。
6. 楊士隆、程敬閔、王中吟、郭人豪(2005)，臺灣地區擄人勒贖犯罪模式之研究，執法新知論衡，第一期，頁101-132。
7. 慶啟人(2007)，防制人頭帳戶成為洗錢管道芻議，國會月刊，第35期，頁74-95。
8. 羅贊興、吳翰明、吳博聰、林宏錦(2007)，證券市場人頭戶之探討--從市場監視觀點評析(上)，證交資料，第539期，頁7-23。
9. 羅贊興、吳翰明、吳博聰、林宏錦(2007)，證券市場人頭戶之探討--從市場監視觀點評析(下)，證交資料，第540期，頁8-27。

### 三、學位論文

1. 丁水復(2004)，新興詐欺犯罪問題防制法制之研究，中山大學大陸研究所碩士論文。
2. 方淳安(2006)，我國期貨交易犯罪型態及偵查之研究，中央警察大學刑事警察研究所碩士論文。
3. 古慧珍(2006)，我國網路詐欺防制之研究—以使用人頭帳戶為中心，交通大學科技法律研究所碩士論文。
4. 林俊清(2003)，證券市場犯罪之研究，中央警察大學刑事警察研究所碩士論文。
6. 周幼偉(2004)，兩岸偵防經濟犯罪之研究，中國文化大學中國文化研究所碩士論文。
7. 施明志(2005)，詐欺犯罪之經濟分析，中央警察大學行政警察研究所碩士論文。
8. 陳順和(2004)，電信犯罪與防制對策之研究，中正大學犯罪防制研究所碩士論文。

9. 陳永鎮 (2006), 台灣地區新興詐欺犯罪趨勢與歷程之研究, 中央警察大學犯罪防治研究所研究所碩士論文。
10. 許清事 (2006), 通訊金融詐欺成因與防制—以臺北縣處理涉及人頭之詐欺案件為例, 台北大學犯罪學研究所碩士論文。
11. 楊士隆等 (2007), 詐騙犯罪防制策略之成效評估研究, 國立中正大犯罪研究中心, 內政部警政署刑事警察局委託研究報告。
12. 劉邦繡 (2008), 瞭解人頭盜用的法律責任, 九十七年度全國遊民個案研討會。
13. 賴添貴 (2005), 台灣地區經濟詐欺狀況處理與防制之實證研究, 大葉大學事業經營研究所碩士論文。
14. 盧俊光 (2006), 新興詐欺犯罪模式及其偵查作為之研究, 中央警察大學刑事警察研究所碩士論文。

#### 四、網頁

1. 內政部警政署全球資訊網, 警政統計年報, 網址:  
<http://www.npa.gov.tw/NPAGip/wSite/lp?ctNode=11395&CtUnit=1740&BaseDSD=7&mp=1>
3. 台北市政府警察局刑事警察大隊網站, 警政資訊, 2009/04/14, 網址:  
[http://cid.tcpd.gov.tw/cgi-bin/Message/MM\\_msg\\_control?mode=viewnews&ts=49e422f3:6c34&theme=3790000000/379130000C/379130200C/Msg](http://cid.tcpd.gov.tw/cgi-bin/Message/MM_msg_control?mode=viewnews&ts=49e422f3:6c34&theme=3790000000/379130000C/379130200C/Msg)
4. 施敏雄, 人頭戶的風險和法律責任, 台灣大紀元-財經專欄, 2001/05/28, 網址: <http://epochtw.com/008/1208.htm>
5. 網路新聞稿, 金管會強調各銀行應落實認識客戶政策、洗錢防制機制與保密義務, 2008/08/18, 網址: <http://www.banking.gov.tw/>
6. 虛設公司向銀行詐貸刷爆信用卡得手數千萬, 卡優新聞網, 2007/11/20, [http://www.cardu.com.tw/news/detail.htm?nt\\_pk=7&ns\\_pk=2762](http://www.cardu.com.tw/news/detail.htm?nt_pk=7&ns_pk=2762)
7. 詐欺犯罪預防, 犯罪預防寶典, 內政部警政署刑事警察局, 2008/02, 網址: [http://www.cib.gov.tw/crime/Crime\\_Book\\_Content.aspx?chapter\\_id=0000006&rule\\_id=0000002](http://www.cib.gov.tw/crime/Crime_Book_Content.aspx?chapter_id=0000006&rule_id=0000002)
8. 黃敦硯、賴仁中, 堵治安漏洞, 新制有幫助, 大紀元新聞網, 2005/02/24, 網址: <http://www.epochtimes.com/>
9. 賴仁中, 銀行櫃檯 反詐騙最前線, 自由時報電子新聞網, 2005/04/22, 網址: <http://www.libertytimes.com.tw>
10. 法源法律網, 洗錢防制法第三條立法理由, 網址: <http://db.lawbank.com.tw/FLAW/FLAWDOC01.asp?lsid=FL006664&lno=3>

#### 五、其他

1. 金融機構開戶作業審核程序暨異常帳戶風險控管之作業範本, 行政院金融監督管理委員會金管銀(一)字第09585013680號函, 2006/06/30。
2. 最高法院刑事判決判決書, 96年台上字第4037號, 2007/07/26。
3. 銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法, 2006/07/06修正。