

# 國立交通大學

科技法律研究所

## 碩士論文

我國網路詐欺防制之研究  
—以使用人頭帳戶為中心



Prevention of Internet Fraud  
—Focusing on the dummy account

研究生：古慧珍

指導教授：吳巡龍 博士

胡均立 教授

劉尚志 教授

中華民國九十五年六月

我國網路詐欺防制之研究－以使用人頭帳戶為中心  
Prevention of Internet Fraud—Focusing on the dummy account

研究生：古慧珍

Student：Ku,Hui-Chen

指導教授：吳巡龍博士

Advisors：Dr. Wu,Hsun-Lung

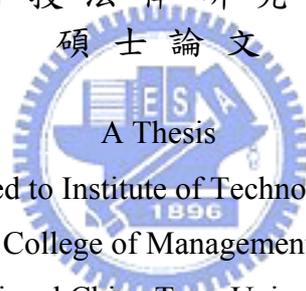
胡均立教授

Dr. Hu,Jin-Li

劉尚志教授

Dr. Liu,Shang-Jyh

國立交通大學  
科技法律研究所  
碩士論文



Submitted to Institute of Technology Law

College of Management

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

In

Technology Law

May 2006

Hsinchu, Taiwan, Republic of China

中華民國九十五年六月

# 我國網路詐欺防制之研究—以使用人頭帳戶為中心

研究生：古慧珍

指導教授：吳巡龍、胡均立、劉尚志

國立交通大學科技法律研究所碩士班

## 摘 要

隨著網際網路的普及，網路技術之成熟與上網人口、時數之激增，網路使用的活動內容也日趨多樣化，伴隨而來的負面效應，即是增加了新型態的犯罪機會，其中網路詐欺犯罪之層出不窮，直接對於電子商務的發展造成嚴重威脅，加之，網路犯罪之隱匿性、即時性，導致查緝之困難性，故對於網路詐欺犯罪之防制，已成為刻不容緩之議題。經本文實證統計發現，我國之網路詐欺案件多達 66.23% 伴隨使用人頭帳戶，換言之，即在網路之虛擬世界中，利用人頭帳戶從事詐騙行為之比例甚高，故本文認為從查緝人頭帳戶之角度來防制網路詐欺之發生，應能有效降低犯罪之發生數。

依照經濟學家 Becker 提出之「理性犯罪模型」，我國目前從人頭帳戶角度制定之防制詐欺犯罪策略，包括：「警示帳戶通報機制」、「非約定帳戶之轉帳限制」及「洗錢防制法第 9 條之修法」，分別為降低犯罪利得及提高刑罰之降低犯罪量手段。本文先從法律面探討前開防制策略之適法性，其中「警示帳戶通報機制」之運作並無法源依據，雖然先後於 2005 年 5 月 8 日修正公布「銀行法第 45 條之 2 第 2、3 項」、2006 年 4 月 27 日發布「銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法」，法律明文賦予金融機構對於可疑帳戶得暫停帳戶之交易功能，賦予「警示帳戶通報機制」運作之正當性，然而，在 2006 年 4 月 27 日之前無法源依據運作下之警示帳戶，仍有違法之虞。何況，「銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法」之行政命令仍有多處超越母法授權範圍、目的之不當，應有再修正之必要。

再者，本文為檢驗政策及法律之制定，是否在實際運作上達到降低「網路詐欺」犯罪量效果，試從實證統計數據來檢視，然而，經過分析以後發現，從人頭帳戶角度制定之防制詐欺政策或手段，對於特定之詐欺類型即「網路詐欺」，並無明顯成果。繼之，本文則嘗試利用「法律之經濟分析」觀點來探討犯罪防制策略並無成效之原因。最後，本文依照「理性犯罪模式」及最低預防成本之觀點，建議應先要求金融機構審核、過濾可疑帳戶之申請及克盡配合員警查緝可疑帳戶之義務，另應提供法律誘因促使經營網路拍賣之業者更有意願採取預防網路詐欺發生之預防措施，此外，督促司法機關同步加重提供人頭帳戶以及使用人頭帳戶從事詐欺之量刑，以變動最小及最低之預防成本來達到嚇阻網路詐欺犯罪之效果。

# Prevention of Internet Fraud—Focusing on the dummy account

Student : Ku,Hui-Chen

Advisors : Dr. Wu,Hsun-Lung

Dr. Hu,Jin-Li

Dr. Liu,Shang-Jyh

Institute of Technology Law

National Chiao Tung University

## ABSTRACT

Along with the popularity, technology enhancement, rapid growth of users and expansion of spending time in the Internet, the activities in this virtual world have multiplied. Its negative side-effect nourished new types of crime. Among them, Internet fraud has posed a serious threat to the development of e-commerce. Moreover, the anonymity and the instantaneous features of the Internet hinder the crackdown against this crime. According to this research, up to 66.2 percent of all Internet fraud cases, there was dummy account involvement. Therefore, hypothetically, detecting dummy accounts should effectively prevent Internet fraud.

In the light of Becker's "rational crime model", prevention policies would function in two methods; one is to reduce the illegal gains, the other one is to increase the penalty. Several prevention policies announced on May 8, 2005 and April 27, 2006 justified the mechanism for banks to temporarily freeze dummy accounts. Nevertheless, modifications to a certain degree should be made to those laws and regulations regarding abuse of the power of autorotation and the manipulation for inappropriate purposes.

Furthermore, this research tried to review the effectiveness of such prevention policies and regulations. Apparently, according to the statistics, there hasn't been any obvious result in deterring Internet fraud by implementing policies to track down dummy accounts. From the viewpoint of economic analysis of law, this study probed the reasons why the prevention policies failed. In addition, following the "rational crime model" and the rule of minimum prevention cost, we suggest that, in order to deter Internet fraud in the most cost-effective way, the audit and screening procedures of personal accounts should be tightened up and the penalty of dummy accounts vending should be increased.

## 誌 謝

我於民國八十七年自東吳大學畢業後，隨即接受司法官訓練，並自九十年一月開始投入犯罪偵查之實務工作。但是在工作中，一直感到自己在學識上仍有相當欠缺之處，尤其是大學中較少接觸到的智慧財產權及科技法律方面，更是必須從頭學起。因此，在九十一年時候，才毅然決定投考交通大學科技法律研究所，一方面希望學習工作中不足的知識，一方面也算是填補大學畢業立刻工作而未能繼續進修的遺憾。

每逢要到交大上課的時候，我的心情總是格外的興奮，因為一來可以轉換心情，不用再面對繁難的工作而可以接受新知，二來可以接觸到一些法律專業以外的課程以增廣見聞。在交大科法所長達三年多的求學過程中，雖然常常覺得工作、課業二頭忙，有點分身乏術，九十二年懷孕期間，更要每週「帶球」從桃園至台北，或從桃園到新竹上課，期間的辛苦不足為外人道。但是同窗的好友的相互勉勵及親人的照顧支持，仍使我得以順利在三年內修完所有的學分。

就讀在職專班的學生，在汲汲於工作之餘，想要挪出時間完成論文，實在不是件容易的事，除了要有極大的抗壓性及耐力，更需要有師友之鼎力相助。而我能夠在繁忙工作中完成論文，要感謝的人實在太多。首先，要感謝當初為我寫推薦信之二位恩師：謝大法官在全及陳檢察長守煌，使我能夠順利考上交大科法研究所。而在論文撰寫過程中，要感謝吳巡龍老師給我的指導，老師的豐富學養及謙遜的處事態度，讓我由衷地敬佩。另感謝胡均立老師，在百忙之中耐心指導我的論文，並在統計學、法律經濟分析上給我莫大的助益，同時，老師治學的嚴謹態度及超強的邏輯分析、論理能力，都著實讓我印象深刻。更要感謝所長劉尚志老師提供人力協助完成龐大數據之統計工作，並在論文上給我適時的提點，使我的論文論述能夠更加完整。還有，要感謝郁楓、英志學長、欣儀、瑤嫻、桂綾、建中幫我處理龐雜、繁複之判決搜尋與統計，及志宏學長、端郡學姐在我需要時，給我最大的助力。此外，更要感謝老公先志及超級可愛的女兒允晨，給我最大實質及精神支柱。

最後，謹以本論文獻給在我生命中所有曾經幫助過我的人。

古慧珍 謹誌於桃園

中華民國九十五年六月

# 目 錄

摘 要.....	i
ABSTRACT.....	ii
誌 謝.....	iii
目 錄.....	iv
表 目 錄.....	vi
圖 目 錄.....	vii
一、 緒論.....	1
1.1 研究動機與背景.....	1
1.2 研究目的.....	3
1.3 研究方法.....	3
1.3.1 文獻探討法.....	3
1.3.2 統計分析法.....	8
1.3.3 事件研究法 (Event Study) .....	8
1.3.4 法律之經濟分析.....	8
1.4 研究限制.....	8
二、 理論、背景介紹及文獻探討.....	10
2.1 網路詐欺.....	10
2.1.1 電腦犯罪與網路犯罪.....	10
2.1.2 網路詐欺之定義.....	11
2.1.3 國內、外網路詐欺現況與類型.....	12
2.2 人頭帳戶.....	16
2.2.1 人頭帳戶之定義與類型.....	16
2.2.2 提供人頭帳戶之法律責任.....	19
2.2.3 各國家對防制人頭帳戶法律面之規範.....	21
2.3 網路詐欺與人頭帳戶.....	24
2.3.1 網路詐欺與人頭帳戶之關連性.....	24
2.3.2 我國網路詐欺類型、取款方式之實證研究.....	25
2.3.3 我國使用人頭帳戶之詐欺防制現況.....	27
三、 從法律面探討犯罪防制策略之適法性.....	29
3.1 警示帳戶通報機制.....	29
3.1.1 警示帳戶之定義與由來.....	29
3.1.2 設置警示帳戶之作業規定及處理程序.....	30
3.1.3 警示帳戶之法律性質.....	33
3.1.4 2006年4月27日「異常帳戶管理辦法」發布前「警示帳戶」之適法性....	33
3.1.5 「異常帳戶管理辦法」發布後「警示帳戶」之法律性質.....	38
3.1.6 警示帳戶內款項之處置.....	40

3.1.7	警示帳戶之解除.....	41
3.1.8	被誤列為警示帳戶之救濟管道.....	42
3.1.9	「異常帳戶管理辦法」之適法性問題.....	43
3.2	限制轉帳方式之適法性.....	43
3.2.1	限制轉帳之由來與歷程.....	43
3.2.2	限制轉帳之適法性.....	45
3.3	洗錢防制法之修法.....	45
3.3.1	洗錢防制法之修法.....	45
3.3.2	販賣人頭帳戶犯罪之適用法律疑問.....	46
四、	從實證面檢驗犯罪防制策略對網路詐欺之成效.....	65
4.1	本章之研究方法.....	65
4.2	實證研究結果.....	69
4.2.1	警示帳戶通報機制執行之成果.....	69
4.2.2	限制轉帳之實行結果及有效性.....	73
4.2.3	提高刑罰之有效性.....	78
五、	依理性犯罪模式架構提出建言.....	87
5.1	降低被告犯罪利得方面.....	87
5.2	提高受制裁機率方面.....	92
5.3	提高刑罰方面.....	93
5.2.1	提供人頭帳戶之刑責方面.....	93
5.2.2	使用人頭帳戶之刑罰部分.....	93
5.4	從成本分析看防制手法之可行性.....	94
六、	結論.....	97
	參考文獻.....	98
	附錄一.....	105
	銀行對疑似不法或顯屬異常交易之存款帳戶.....	105
	銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法.....	107
	銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法.....	114
	附錄二.....	118
	金融電信人頭帳戶及電話犯罪案件處理執行規定.....	118
	警察機關受理詐欺案件通報電話斷話(復話)流程圖.....	125
	警察機關受理詐欺案件通報(解除)警示帳戶流程圖.....	126
	附錄三.....	127
	受理詐騙帳戶通報警示、詐騙電路段話簡便格式.....	127
	簡    歷.....	128

## 表 目 錄

表 1 關於網路詐欺之論文、期刊文獻表.....	4
表 1 關於網路詐欺之論文、期刊文獻表（續）.....	5
表 1 關於網路詐欺之論文、期刊文獻表（續）.....	6
表 2 談及人頭帳戶之詐欺研究論文表.....	6
表 2 談及人頭帳戶之詐欺研究論文表（續）.....	7
表 3 人頭帳戶提供者之法律責任表.....	19
表 3 人頭帳戶提供者之法律責任表（續）.....	20
表 4 網路詐欺類型之名稱、定義說明表.....	26
表 5 網路詐欺類型之件數、被害金額表.....	26
表 6 網路詐欺與人頭帳戶之關連比例表.....	27
表 7 洗錢防制法第 2、9 條修正前後對照表.....	46
表 8 法院論罪整理表.....	47
表 8 法院論罪整理表（續）.....	48
表 9 販賣人頭帳戶犯罪之適用條文表.....	51
表 10 自動櫃員機轉帳交易次數、金額.....	73
表 11 自動櫃員機轉帳交易次數、金額之月平均表.....	73
表 12 網路詐欺平均轉帳金額、件數及人頭帳戶件數表.....	77
表 13 人頭帳戶案件偵查終結情形表.....	79
表 14 人頭帳戶案件判決確定情形表.....	79
表 15 人頭帳戶案件執行情形表.....	80
表 16 修法前後販賣人頭帳戶宣判刑度統計比較表.....	81
表 17 販賣人頭帳戶宣判刑度比較變動百分比.....	81
表 18 販賣人頭帳戶之平均販賣本數及犯罪利得比較表.....	82

## 圖目錄

圖 1 台灣地區上網人口比較圖.....	1
圖 2 2001 年至 2005 年臺閩地區電腦網路犯罪發生及破獲件數.....	2
圖 3 2001 年至 2005 年臺閩地區電腦網路犯罪破獲率.....	2
圖 4 警察機關受理詐欺案件通報(解除)警示帳戶流程圖.....	32
圖 5 「警示帳戶通報機制」事件之觀察期間.....	65
圖 6 「非約定帳戶之限制轉帳」事件之觀察期間.....	66
圖 7 「洗錢防制法第 9 條修法」事件之觀察期間.....	66
圖 8 販賣帳戶用以詐欺之犯罪量圖.....	70
圖 9 網路詐欺之犯罪發生數圖.....	71
圖 10 全部詐欺發生數圖.....	72
圖 11 2005 年自動櫃員機轉帳件數逐月曲線圖.....	74
圖 12 2005 年自動櫃員機轉帳金額逐月曲線圖.....	74
圖 13 2005 年全部詐欺逐月曲線圖.....	75
圖 14 2005 年手機簡訊詐欺逐月曲線圖.....	75
圖 15 2005 年全部詐欺逐月曲線圖.....	76
圖 16 2005 年網路詐欺逐月曲線圖.....	76
圖 17 非約定轉帳限制對網路詐欺之影響圖.....	78
圖 18 網路詐欺逐月發生數圖.....	83
圖 19 理想的懲罰狀況圖.....	85
圖 20 預期制裁成本與犯罪決策圖.....	85

# 一、緒論

## 1.1 研究動機與背景

網際網路 (Internet) 是繼機械革命後，影響人類生活之重大發明，無論現在與未來，都將是資訊社會重要之應用與溝通媒介，藉由網際網路之廣泛應用，打破了世界各地有形之疆域，提供企業新穎而有利的商品或服務交易，也給予使用者無限的憧憬與期待。近年來，電子商務隨著網際網路積極發展，日益炙手可熱，尤其是亞洲地區各新興國家的發展態勢，更是驚人<sup>1</sup>。根據台灣網路資訊中心於2006年1月23日公布2006年1月「台灣寬頻網路使用調查」報告，截至2006年1月16日為止，台灣地區上網人口成長約1,476萬人，整體人口(0-100歲)上網率達65.07%，12歲以上人口的上網率則為65.97%<sup>2</sup>。而台灣網路使用戶於1996年僅40萬用戶，迨至2006年1月已飆漲至1476萬使用戶，顯示台灣網路與寬頻發展進入成熟期，又從該報告可觀察出，網路的迅速發展，使得不同年齡層接觸網路之機會與日遽增。

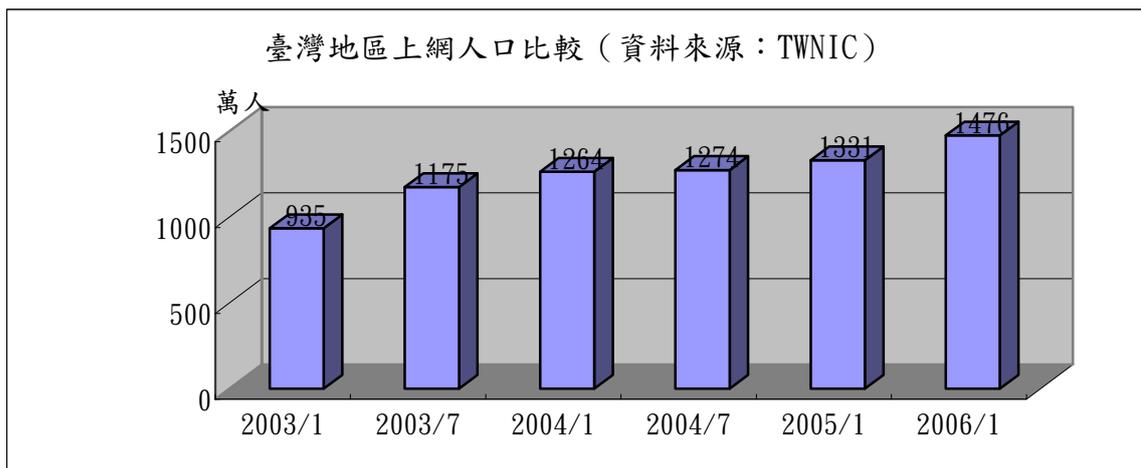


圖 1 台灣地區上網人口比較圖  
(資料數據來源：財團法人台灣資訊中心網站)

而隨著網際網路之互動越趨緊密後，也衍生一些難以避免的問題，尤其是日益嚴重之網路犯罪問題。在我國，依據內政部警政署之電腦網路犯罪發生件數之統計：2001年之發生件數僅390件、2002年2,566件、2003年6,824件、2004年15,311件，至2005年12月止已高達22,111件，顯見網路犯罪發生率已成倍數急遽增加<sup>3</sup>，惟網路犯罪之破獲率卻逐年降低<sup>4</sup>。再參以研究顯示網路犯罪之犯罪損害以財產損害最多，網際

<sup>1</sup>郭士傑，「詐欺及其類似犯罪區辨之研究」，東吳大學法律學系，專業碩士班碩士論文，第65頁，2003年。

<sup>2</sup>見財團法人台灣資訊中心網站，TWNIC 2006年1月「台灣寬頻使用調查」摘要分析 <http://www.twNIC.net.tw/index4.php>，(2006/Feb/26)。

<sup>3</sup>2001年至2005年臺灣電腦網路犯罪發生數及破獲數-依案類別，資料來源：內政部警政署統計室。

<sup>4</sup>2001年之發生件數、破獲數為390、265件；2002年發生件數、破獲數為2,566、1,340件；2003年發

網路儼然成為詐欺犯罪之溫床，而網路詐欺多以網路購物、網路交友、網路遊戲、電子郵件等方式為之<sup>5</sup>。且從台灣網路資訊中心調查結果報告顯示個人使用網路最常使用之電子郵件 E-mail (53.96%)、玩網路遊戲 (21.27%)、網路交友 MSN, ICQ (32.06%)、網路購物 (12.64%) 等功能之比例甚高<sup>6</sup>，從而，使用網際網路之人多暴露在成為網路詐欺潛在被害人之危機中。

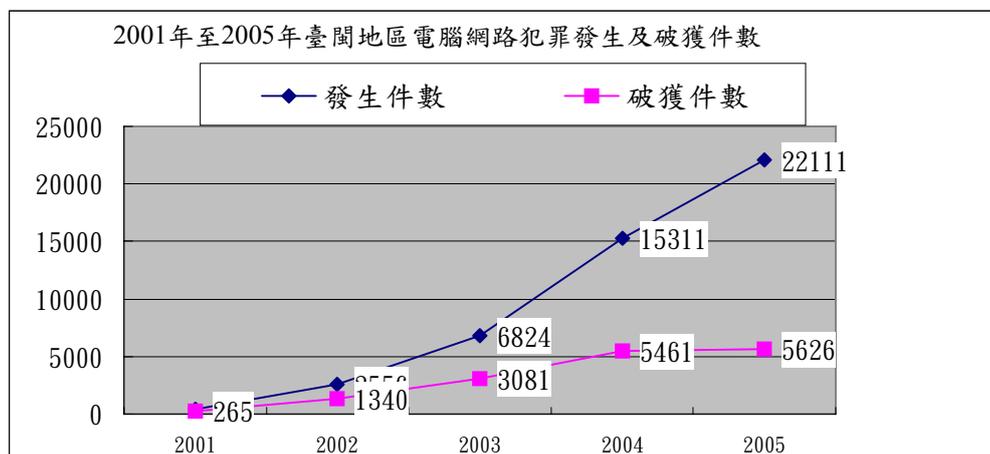


圖 2 2001 年至 2005 年臺閩地區電腦網路犯罪發生及破獲件數  
(資料數據來源：內政部警政署統計室)

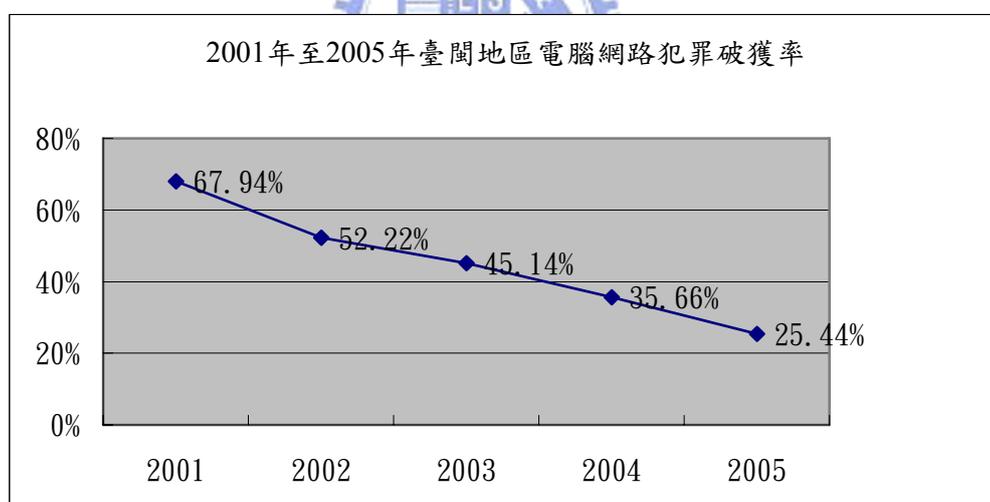


圖 3 2001 年至 2005 年臺閩地區電腦網路犯罪破獲率  
(資料數據來源：內政部警政署統計室)

由上可知，網際網路之興盛，確實造成網路詐欺之層出不窮。以美國為例，美國

生件數、破獲數為 6,824、3,081 件；2004 年發生件數、破獲數為 15,311、5,461 件；至 2005 年 12 月止發生件數、破獲數為 22,111、5,626 件。則 2001 年至 2005 年網路案件之破獲率分別依序為 67.49%、52.22%、45.14%、35.66%、25.44%。原始資料來源：2001 年至 2005 年臺閩電腦網路犯罪發生數及破獲數-依案類別，內政部警政署統計室，

<sup>5</sup> 洪志忠，「我國網路犯罪案例及發展趨勢之探討」，2003 年網際空間：科技、犯罪與法律社會學術研究暨實務研討會，第 443 頁，2003 年。

<sup>6</sup> 同前揭註 2。

網路犯罪報案中心（The US Internet Crime Complaint Center, IC3, 乃美國詐欺犯罪報案中心 IFCC 之前身）於 2005 年 1 至 12 月網路詐欺申訴之件數已超過 231,493 件<sup>7</sup>。2006 年 1 月 25 日美國聯邦交易委員會（Federal Trade Commission, FTC）之統計報告指出 2005 年一整年網路購物詐欺案件已達 196,503 件，損失金額超過美金 335,000,000 元<sup>8</sup>。以上在在顯示，網路詐欺案件因網際網路之無遠弗屆而更層出不窮。根據 GatnerG2 之 2002 年初發表之調查報告，2001 年線上銷售額因網路詐欺損失金額高達七億美金，佔年度總銷售額的 1.14%，這個報告也指出，詐欺在網路上發生的次數是在實體世界發生次數的 17 倍<sup>9</sup>。由此可見，網路詐欺對電子商務之發展直接構成威脅，又因為網路環境具有即時性、可匿名性，犯罪成本被有效降低，而犯罪者越來越難被追蹤、逮捕與定罪<sup>10</sup>，是以如何將低網路詐欺之發生率，實乃刻不容緩之課題。

## 1.2 研究目的

作者目前任職檢察機關，直接從事犯罪偵查工作，根據近來觀察詐欺案件之發生比率居高不下與國內人頭帳戶之氾濫與取得容易有相當之關連性。然而，我國既無官方或學術機構對網路詐欺之類型、數據、被害人付款方式做任何之觀察、統計，致使無從瞭解我國實務上網路詐欺之真實現況。故本文利用實證研究發現，我國網路詐欺犯罪中以各種名目誘使被害人以自動櫃員機（以下均簡稱：ATM）轉帳方式將金錢交付者佔 90.15%，而此種案件中有 73.47% 之詐欺者係利用「人頭帳戶」來收取詐得之款項，此部分實證研究留待第二章詳述。因此，本文基於上開實證統計之結果，導出研究主要命題為：「查緝人頭帳戶之犯罪或從人頭帳戶角度來制定防制犯罪策略，應能有效地降低網路詐欺犯罪之案件數。」，從而，本文研究之目的有以下幾點：

1. 從法律層面討論，我國從防制人頭帳戶角度遏止詐欺犯罪防制策略之適法性問題。
2. 利用科學之實證方式及法律之經濟分析，來檢驗前開犯罪防制手法是否能有效降低「網路詐欺」之犯罪量。
3. 再依照經濟學家 Becker 提出之「理性犯罪模型」提出防制網路詐欺之建言。最後，並引入犯罪預防成本、誘因機制等觀念，提出目前我國比較可行之防制策略。

## 1.3 研究方法

### 1.3.1 文獻探討法

文獻法是指根據調查目的所進行蒐集和分析書面或聲音影像資料的方法。文獻是人們從事各種社會活動的紀錄，包括：文字、圖像、符號、聲頻等紀錄型態。而文獻

<sup>7</sup>“IC3 2005 Internet Fraud –Crime report”，[http://www.ic3.gov/media/annualreport/2005\\_ic3report.pdf](http://www.ic3.gov/media/annualreport/2005_ic3report.pdf)，（2006/May/1）。

<sup>8</sup> Consumer Fraud and Identity Theft Complaint Data January-December 2005，page3，<http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf>（2006/Feb/26）。

<sup>9</sup>楊惠鈞，「網路犯罪日益嚴重消費者如何自保？」，電子商務時報，2002 年 9 月 20 日。

<sup>10</sup>吳照琰，「網路入侵型犯罪法治議題分析」，財團法人資訊工業策進會科技法律中心戴豪君等合著，數位科技法律大未來，第 137 頁，2004 年 12 月。

探討是將與研究問題相關且已被研究過的文件資料，加以分析、探討、綜合或摘述。此類文獻包括：期刊、評論、圖書、雜誌、研究報告、會議紀錄、日誌等檔案資料<sup>11</sup>。

網路詐欺屬於新型態之趨勢性犯罪，而就作者直接從事犯罪偵查工作之觀察，國內人頭帳戶之氾濫與取得容易與詐欺案件之層出不窮，有相當之關連性，且近年來人頭帳戶之不法使用有越來越嚴重之趨勢。然而，國內外學術界對於以使用人頭帳戶為網路詐欺之犯罪問題的關切極為有限，在網路詐欺犯罪之相關議題研究中，研究者多將焦點集中於公布詐欺犯罪相關統計數據與犯罪手法等文獻，表 1。惟對於從防制人頭帳戶角度來遏阻網路詐欺犯罪之研究，可謂是付之闕如，茲於此挑選數篇論文中談及人頭帳戶與詐欺間關係之相關研究文獻，概略敘述如下表 2：

表 1 關於網路詐欺之論文、期刊文獻表

	文獻名稱	主要內容
論文	蕭愛貞，「網際網路犯罪之責任內涵—兼論網路服務業者之責任」，輔仁大學法律研究所，2002年。	主要是以「網路作為犯罪場所」之網路犯罪行為的法律責任提出討論。文中針對網路詐欺行為及不實廣告問題，提出我國現行法及美國之法律規範。並討論網路服務業者對網路服務用戶從事詐欺行為時，網路服務業者所應負之責任。
論文	李明儒，「網路詐欺之法律探討與管理—以線上拍賣為例」，國立交通大學管理研究所，2005年1月	該論文將網路詐欺定義為：行為人經由網路，欺騙自然人或操縱電腦，取得財產之行為。並針對「拍賣詐欺」案件整理歸納目前消費者、拍賣網站及政府所採取防堵詐騙之措施，進一步提出建言。
論文	劉忠陽，「拍賣網站消費與詐欺行為之研究」，銘傳大學管理研究所，2004年	除探討拍賣網站詐欺行為與常見手法外，分析拍賣網站消費者之行為決策模式，並藉此提出拍賣網站經營者與消費者預防網路詐欺之對策。
論文	郭士傑，「詐欺及類似犯罪區辨之研究」，東吳大學法律學系法律專業碩士，2003年	將網路詐欺歸類在「新型態詐欺行為」，並探討網路詐欺與刑法339、339條之3及線上遊戲「寶物」之問題。

<sup>11</sup>國立交通大學科技法律研究所，調查研究方法手冊，第21頁，2004年1月。

表 1 關於網路詐欺之論文、期刊文獻表 (續)

	文獻名稱	主要內容
論文	賴添貴，「台灣地區經濟詐欺狀況處理與防制之實證研究」，大業大學事業經營研究所，2005年2月	<p>1. 本文以實證方式探討新興經濟詐欺之形成原因、手法，進而提出建言。該論文並未定義何謂經濟詐欺案件，僅舉例：刮刮樂、手機簡訊、退款、退稅、假綁票、假黑道、金融卡盜領及信用卡盜刷等詐欺案件為經濟詐欺案件。又在章節中提出常見經濟詐欺手法及類型，包括網路購物詐欺、網路銀行轉帳詐欺、網路盜取信用卡詐欺、網路交友詐欺、網路金光檔詐欺、網路虛設行號詐欺、網路購租證件詐欺、冒牌網站詐騙卡號詐欺等。</p> <p>2. 實證研究之方式是以：(1) 觀察詐欺案件官方之數據變化並介紹刑事局實際偵破之詐欺案件，以瞭解詐欺犯罪之現況及手法。(2) 製作問卷訪問台北、台中及台南監獄受刑人瞭解詐欺犯罪行為人之社會背景、犯案動機與手段。</p>
研討會論文	章京文，「與網路詐欺奮戰—以美國及我國之現況為例」，2002 網路犯罪與法制研討會論文集。	文中將網路詐欺定義為：係指以任何形式使用一個或多個網路原件的詐騙方式，例如以聊天室、電子郵件、訊息布告欄或者是網址方式去對預期的被害人引起誘惑，並進而實施交易，或者傳送詐騙收益予金融機構或其他相關機構。另介紹美國與我國之網路詐欺現況，並提出防制之建言。
期刊文章	林佳蓉，「網路詐欺案件類型、法律適用及犯罪防治之道」，90年8月法務透析。	介紹美國與我國之網路詐欺現況，並提出網路詐欺防制之道。
文章	林宜隆、楊鴻正，「網路交易犯罪之偵查要領—以網路詐欺犯罪為例」，	介紹美國 FTC 報告公布 2003 年網路詐欺犯罪手法，繼之簡介國內、外犯罪網路交易案例。最後，依據網路交易可能之犯罪原因，探討偵查網路交易案件之方法與要領。
論文	趙秀雯，「網路犯罪問題與規範機制之研究」，國防大學管理學院法律學研究所，2001年6。	本文在探討目前網路上發生之網路犯罪類型，及網路使用所引發之法律爭議、網路服務提供業者之法律責任。且認為網路行為所侵害之客體仍屬自然人，而僅係利用網路服務為其犯罪方法之一，與傳統刑法上之詐欺行為並無差異，只是另一種利用新興科技犯罪之犯罪型態。

表 1 關於網路詐欺之論文、期刊文獻表 (續)

	文獻名稱	主要內容
論文	丁水復，「新興詐欺犯罪問題防治法制之研究」，國立中山大學大陸研究所碩士在職專班，2005年6。	<ol style="list-style-type: none"> <li>1. 介紹新興詐欺犯罪之手法與模式，並檢視台灣防制此種犯罪之防制策略及手法，進而提出建言。</li> <li>2. 文中提到之新興詐欺犯罪是指大量運用收購或偽造證件，辦理金融、電信人頭帳戶，以人頭帳戶、電話為犯罪工具，設計與時事相結合之話題情境，與民眾社會的信賴感或同情心及恐懼心等心理弱點，進而誘使或恐嚇被害人至金融機構臨櫃匯款或以自動提款機轉帳，將指定款項匯入詐欺集團所指定之人頭帳戶，且透過單向聯絡、多重電話轉接之犯罪手法，逃避警察追緝者。</li> <li>3. 新興詐欺犯罪方式實務上大致可分為「手機簡訊詐財」、「刮刮樂彩金詐騙」、「電子商務詐騙」、「恐嚇類詐騙」、「電子求職廣告詐騙」、「信用貸款詐騙」、「以人頭戶從事洗錢」等七大項詐欺手法。</li> </ol>

表 2 談及人頭帳戶之詐欺研究論文表

	文獻名稱	內容
論文	江志慶，「ATM 轉帳詐欺犯罪之實證研究」，中央警察大學犯罪防治系研究所，2005年。	<ol style="list-style-type: none"> <li>1. 本文研究範疇為新型態詐欺犯罪類型，有關使用 ATM 轉帳而被詐騙之案件均屬之，將研究焦點置於「ATM 轉帳」一環節上。</li> <li>2. 針對「有動機及能力的犯罪者」、「適合的犯罪標的物」、「抑制犯罪者」三方面，探討 ATM 轉帳詐欺之犯罪，並以訪談方式（訪談對象：偵破 ATM 轉帳詐欺案件之偵查員、金融電信風險控管員、被害人），進行資料蒐集，並依訪談紀錄進行整理、分析、比對，將研究方向區分「有動機及能力的犯罪者」、「適合的犯罪標的物」、「抑制犯罪者」等三部分。最後援引「情境預防犯罪理論」之對策表提出具體建言。</li> <li>3. 在人頭帳戶、人頭電話相關議題探討章節內，說明實務上收購「人頭帳戶」的方式，及現行防制「人頭帳戶」之作為。</li> </ol>

表 2 談及人頭帳戶之詐欺研究論文表 (續)

	文獻名稱	內容
委託研究報告	內政部警政署委託中央警察大學之研究報告， <u>ATM 轉帳詐欺犯罪之實證研究</u> ，2004 年 12 月。	<ol style="list-style-type: none"> <li>1. 依刑事警察局統計 2002 至 2004 之詐欺受理案件，發現台灣詐欺類型發生數較高者計有手機簡訊詐欺、刮刮樂詐欺、電話詐欺、網路詐欺等，幾乎都與「ATM 轉帳詐欺犯罪」相關。</li> <li>2. 以訪談方式(訪談對象：偵破 ATM 轉帳詐欺案件之偵查員、金融電信風險控管員、被害人)，進行資料蒐集，並依訪談紀錄進行整理、分析、比對，將研究方向區分「ATM 轉帳詐欺集團犯罪歷程分析」、「被害人被害歷程分析」、「各單位打擊 ATM 轉帳詐欺犯罪作為分析」等三部分。最後從情境預防角度提出預防詐欺之建言。</li> <li>3. 將 ATM 轉帳詐欺犯罪集團組織結構區分為「集團首腦」、「後勤支援」、「實施詐騙」、「機動領款」四大部分，其中「後勤支援」、「機動領款」是指收購人頭帳戶、人頭電話用以實施詐欺，而由車手持人頭帳戶存簿臨櫃提領被害人匯入款項或是持人頭帳戶之提款卡至各金融機構 ATM 櫃員提款機提領被害人匯入之金錢。</li> <li>4. 依據實證研究發現，人頭帳戶可謂是「ATM 轉帳詐欺犯罪」之最大幫兇，警方及金融機構多有如此認知，欲遏止新型態詐欺，必須從遏止人頭帳戶的氾濫著手。</li> </ol>
論文	賴添貴，「台灣地區經濟詐欺狀況處理與防制之實證研究」，大業大學事業經營研究所，2005 年 2 月	<ol style="list-style-type: none"> <li>1. 本文以實證方式探討新興經濟詐欺之形成原因、手法，進而提出建言。並未定義何謂經濟詐欺案件，僅舉例：刮刮樂、手機簡訊、退款、退稅、假綁票、假黑道、金融卡盜領及信用卡盜刷等詐欺案件。又在章節中提出常見經濟詐欺手法及類型，包括網路購物詐欺、網路銀行轉帳詐欺、網路盜取信用卡詐欺、網路交友詐欺、網路金光檔詐欺、網路虛設行號詐欺、網路購租證件詐欺、冒牌網站詐騙卡號詐欺等。</li> <li>2. 本文之實證研究：(1) 觀察詐欺案件官方之數據變化並介紹刑事局實際偵破之詐欺案件，以瞭解詐欺犯罪之現況及手法。(2) 製作問卷訪問台北、台中及台南監獄受刑人瞭解詐欺犯罪行為人之社會背景、犯案動機與手段。</li> <li>3. 實證研究結果發現，新興經濟詐欺案件共通性即是大量利用偽造證件、人頭帳戶及人頭電話等犯罪工具，以各種名目要求被害人將指定款項匯入詐欺集團所指定之人頭帳戶中，以詐騙不知情民眾之錢財。再綜合以上實證研究，說明經濟詐欺形成原因、所造成影響及防制之道。</li> </ol>

### 1.3.2 統計分析法

統計分析是指建立在數學科學基礎上的分析方法，以掌握事物總體的數量特性為目標，因為主要以處理數據的方式分析資料，又稱為量化分析。而統計分析是一種工具，並非目的，所以研究者必須先確定自己要由研究的目的與任務來確定統計分析的對象、提綱以及各階段統計方法的選擇，使統計分析能環繞著研究主題進行。在確定統計目的後，對蒐集調查資料進行加工整理，使之系統化與條理化，且針對不同類型之數據必須選用不同之統計方法，最後則依據加工整理之調查資料進行計算統計值。又如果是進行抽樣調查，在計算樣本值後，必須對母體特性進行系統推論，從計算出的樣本統計值推斷母體三束，並進行假設檢定<sup>12</sup>。

目前我國探討法律制度、問題之文章，多僅以文獻探討、比較演繹法為研究之方法，鮮少利用實證分析之方式，來探討實際之法律執行面上是否達到法律所欲企圖達到減少犯罪量之目的，故本文嘗試利用統計、分析法院判決、犯罪案件量之變化等實證方式，來分析特定詐欺防制策略，是否足以達到降低網路詐欺犯罪量之成效。

### 1.3.3 事件研究法 (Event Study)

本文在實證統計方面，另採取一般會計與財務學研究所經常使用之「事件研究法」。「事件研究法」主要目的是觀察某一事件的發生或資訊的發布，是否會改變投資人的決策，進而影響股票價格或交易量的變化。而本文借用此「事件研究法」觀察特定犯罪防制政策之實施，是否會改變理性犯罪者之決策，進而影響所欲遏止之特定犯罪之犯罪量的變化。本文係以實證、統計方式觀察目前實務採取從人頭帳戶角度來防制詐欺「警示帳戶通報機制」、「非約定帳戶之轉帳限制」及「洗錢防制法第9條修法」等事件發生期前後各一年或半年之月資料，來檢視此三種犯罪防制策略是否能有效降低網路詐欺犯罪之發生率。

### 1.3.4 法律之經濟分析

本文借用「法律之經濟分析」中理性犯罪模型及犯罪成本等概念，進行分析、解釋實證統計之結果。經濟學提供科學式的理論來預測法律制裁對潛在行罪者之影響，此理論不僅完全超乎直覺，更超越傳統法律人「公平正義」之抽象思維。除對犯罪行為提供科學的理論外，經濟學亦提供法律和政策評估是否有效、有用之準則。而法律應是達成社會重要目標之工具，藉由經濟學利用效率、分配理論來預測政策效果，希望能以較低之成本達成政策之目標，並將有限資源做更有效率之配置<sup>13</sup>。

## 1.4 研究限制

本文著重在從人頭帳戶之角度來探討防制網路詐欺之成效，進而提出觀察結果、結論與建言，然而防制網路詐欺之手法並非僅能從人頭帳戶之角度出發，而本文限縮圍繞在從人頭帳戶之犯罪為中心討論，目的係希望能聚焦不至於論文焦點散漫致無法深度討論，從而，此外之探討及建議並非在本文多加討論之範疇。

<sup>12</sup>同前揭註 11，第 25 頁。

<sup>13</sup>Cooter 及 Ulen 著，法律經濟學，溫麗琪編譯，華泰文化事業公司，第 2、3 頁，2003 年 6 月初版。

又本文有以搜尋、分析判決之實證方法來觀察目前實務所採特定之犯罪防制策略是否對防制網路詐欺有成效，惟受限於研究人力、時間等因素，本文所有法院判決、檢察官書類之統計，均僅搜尋宣判日、終結日至 2005 年 12 月 31 日之判決、書類為本文之實證研究標的。



## 二、理論、背景介紹及文獻探討

### 2.1 網路詐欺

#### 2.1.1 電腦犯罪與網路犯罪

「網路犯罪」雖已成為公眾採用之名詞，然目前學者、專家並未有嚴格之定義與統一見解，一般學者多將之與「電腦犯罪」混為一談，從而，試圖對網路犯罪一詞下定義前，首應瞭解什麼是電腦犯罪，只是目前世界各國對電腦犯罪似乎都還沒有一致、明確的定義，不過電腦犯罪的行為人所違犯的必須是與電腦特性有關的犯罪，則是沒有爭議的<sup>14</sup>。而所謂電腦特性，是指電腦具有之快速隱密而有效地處理、傳遞大量資料之功能<sup>15</sup>。故所謂電腦犯罪是指利用電腦之特性，以電腦作為犯罪場所或以電腦作為犯罪客體（攻擊目標）的犯罪行為。若非利用電腦之特性，而僅以電腦作為犯罪之犯罪客體，則不是電腦犯罪，例如：某甲持木棒到某乙的辦公室將某乙的電腦全部砸爛，使某乙的電腦系統無法使用，此犯罪雖然與電腦有關，但是其與電腦的特性無關，此並非電腦犯罪，應屬於一般的毀損罪。

一般而言，利用電腦特性的犯罪，依電腦在犯罪中所扮演的角色，可以分成以下三類：一、以電腦作為犯罪工具；二、以電腦作為犯罪場所；三、以電腦作為犯罪客體。如果要嚴格來看，對於電腦犯罪採最狹義的定義，應只有第三類：利用電腦之特性，以電腦為作犯罪客體的情形，才能稱為電腦犯罪。電腦犯罪宜採較為廣義的定義，將第二類也納入，以偵辦犯罪與證據蒐集的角度來看，犯罪證據最後仍會以電子形式保留在電腦媒體或電子設備中，所以電腦犯罪的定義應包含以電腦為犯罪場所的情形<sup>16</sup>。

網路犯罪概念強調必須藉由網路的使用才能完成犯罪，而網路是網際網路(Internet)<sup>17</sup>之簡稱，又網際網路是電腦與通訊設備所組成，且是廣域網路之一種，由全球各地之區域網路依據 TCP/IP 協定連結而成，透過網際網路的連接，讓各個國家或不同網路使用者可以彼此交換資訊、共同資源。故所謂網路犯罪，應屬於電腦犯罪的下位概念，簡言之，即為電腦犯罪之電腦網路類型。

有學者認為應將網路犯罪定義為利用網際網路之特性為犯罪手段或犯罪工具之網路濫用行為。而所謂網際網路特性，應包含：大量傳播、即時性、可匿名性等特性<sup>18</sup>。又利用網路之犯罪，依照網路在犯罪中所扮演之角色可定義為，一、以網路作為犯罪

<sup>14</sup>黃榮堅，「電腦犯罪的刑法問題」，刑罰的極限，元照出版社，第 202 頁，1999 年。

<sup>15</sup>高大宇、王旭正，「網路病毒傳播與偵防機制策略研究」，資訊學會季刊，第 2 卷第 3 期，第 57 到 62 頁，1999 年。

<sup>16</sup>電腦鑑識科學的現在與未來（一），台灣電腦網路危機處理暨協調中心網頁，<http://www.cert.org.tw/document/column/show.php?key=68>（2006/Feb/27）。

<sup>17</sup>Internet 之原意是，將世界上所有之電腦，透過網路的連結和標準化的通訊協定，彼此相互通訊。

<sup>18</sup>馮震宇著，「我國網路犯罪類型及案例探討」，網路法基本問題研究（一），第 337 頁，學林出版社，1997 年 7 月 1 日。

工具：利用網際網路之特性，透過網路以其為工具進行各種犯罪活動。如：經營應召站者，利用網路傳遞嫖客資料，並通知應召站小姐前往約定地點從事色情行業。二、以網路作為犯罪場所：利用網際網路之特性，使用網路以其為犯罪之活動空間，換言之，即指犯罪之行為係在網路上所為者而言。如：在電子布告欄上張貼猥褻色情圖片或販賣色情資訊。三、以網路作為犯罪客體：攻擊網路以其為目標進行網路犯罪<sup>19</sup>，如：電腦駭客利用網路上共享軟體下載區，或以電子郵件傳輸等方式，侵入他人電腦系統施放病毒，癱瘓他人電腦系統。

雖有學者認為網路詐欺均屬以網路為犯罪工具之犯罪型態<sup>20</sup>，然不能一以概之。實際上，網路詐欺類型究係以網路作為犯罪工具或是利用網路作為犯罪場所，有時難以區辨，比如：利用網路拍賣購物之詐欺，既是係利用網路拍賣為詐騙之工具，亦是利用網路之空間作為犯罪場所，是以網路作為犯罪工具及以網路為犯罪空間類型之網路犯罪，既難區辨，且在區辨似無實義的情況下，若採將此二種型態之網路犯罪，歸納稱之為「利用網路服務之網路犯罪」，以便與以網路為犯罪客體之網路犯罪區別，不僅簡單，且亦不致有無法分類之困擾<sup>21</sup>。

### 2.1.2 網路詐欺之定義

網路詐欺一詞，是目前報章雜誌常見之特定名詞，然而，對於網路詐欺之定義與意涵，並未有一致的看法。學者林宜隆認為，網路詐欺是網路犯罪中利用網路作為犯罪工具或犯罪空間的一種犯罪類型<sup>22</sup>；另謝開平認為，應當將網路詐欺理解為：行為人經由網際網路，欺騙自然人或操控電腦，而取得財產之行為<sup>23</sup>。然而，在瞭解網路詐欺之意涵前，應先瞭解詐欺之基本概念。所謂詐欺，從民法之意義觀察係指，欲使相對人陷於錯誤，故意以不實之事，令其因錯誤而為意思表示<sup>24</sup>。而刑法就詐欺罪即有明確之定義：意圖為自己或第三人不法所有，以詐術使人將本人或第三人之物交付，或以詐術之方式使本人或第三人取得財產上之不法利益者<sup>25</sup>。且詐騙之對象不以自然人為限，若詐騙之對象為收費或自動付款設備等機器，或是詐騙之對象為電腦或其他相關設備，亦成立刑法上之詐欺罪<sup>26</sup>。網路詐欺，亦應不脫前開討論詐欺概念之意涵，只是行為人不再使用傳統之傳播媒介，而是改以網路作為媒介之方式，本文試圖將網路詐欺定義為：意圖為自己或第三人不法所有，利用網路服務或以之為媒介，以詐術

<sup>19</sup>同前揭註5，第436頁。

<sup>20</sup>同前揭註，第19頁。

<sup>21</sup>葉奇鑫，刑法有關電腦（網路）犯罪研修資料彙編，法務部印製，2002年12月。

<sup>22</sup>林宜隆，「網路犯罪之案件分析」，中央警察大學學報，第37期，第224頁，2000年。

<sup>23</sup>謝開平，「電腦詐欺在比較刑法上之研究」，國立台北大學法律系，博士論文，第19頁，2003年7月。

<sup>24</sup>參見最高法院18年上字第371、56年台上3380號判例。

<sup>25</sup>刑法第339條第1項及第2項。

<sup>26</sup>參見刑法第339條之1至之3之規定。刑法第339條之1：意圖為自己或第三人不法之所有，以不正方法由收費設備取得他人之物者，處1年以下有期徒刑、拘役或3千元以下罰金。刑法第339條之2：意圖為自己或第三人不法之所有，以不正方法由自動付款設備取得他人之物者，處3年以下有期徒刑、拘役或1萬元以下罰金。刑法第339條之3：意圖為自己或第三人不法之所有，以不正方法將虛偽資料或不正指令輸入電腦或其相關設備，製作財產權之得喪、變更紀錄，而取得他人財產者，處7年以下有期徒刑。以前項方法得財產上不法之利益或使第三人得之者，亦同。前二項之未遂犯罰之。

自他人取得財物或財產上之不法利益。而此之他人則不限於自然人。

又觀察美國司法部 (Department of Justice) 對於網路詐欺 (Internet Fraud) 所下之定義為：係指利用網路或網路空間對潛在之被害人實施誘騙行為，進而使被害人與之進行交易，或依照詐欺指示將款項匯入金融機構。而利用網路之方式，例如：聊天室、電子郵件、訊息佈告欄、網頁網站等<sup>27</sup>。而此定義亦不脫本文嘗試定義之範疇，只是將利用網路或以之為媒介之方式，以例示之方式告訴讀者。

### 2.1.3 國內、外網路詐欺現況與類型

#### 一、美國網路詐欺現況：

美國網路犯罪報案中心 (IC3) 於 2005 年 1 至 12 月總收到超過 231,493 件關於網路犯罪之申訴，比去年 2004 年之 207,449 件增加 11.73%。而網路犯罪中有超過 214,826 件是網路詐欺申訴之件數，較 2004 年之 103,959 之申訴案件增加 106.64%。又網路詐欺申訴案件中，網路拍賣詐欺 (auction fraud) 仍是案件之大宗，佔全部網路犯罪申訴案件之比例高達 62.7%<sup>28</sup>。

美國經濟犯罪研究中心 (National Internet Fraud Watch Information Center) 2005 年之觀察報告指出：該年度網路詐欺之總損失金額為美金 13,863,003 元，較 2004 年之 5,787,170 元為多；又 2004 平均每個受害者損失金額為美金 10,794 元，然 2005 年已高達 12,315 元；網路拍賣詐欺佔所有網路詐欺達 42%，為網路詐騙類型之大宗；在詐騙者利用網站進行詐騙者佔 75%，其餘則是利用電子信件進行詐騙佔 25%<sup>29</sup>。

美國聯邦交易委員會 (FTC) 已統計 2005 年超過 431,118 件詐欺申訴案件，其中網路詐欺案件數為 196,503 件，佔全部詐欺案件之 46%，損失金額超過達美金 335,000,000 元，平均每人損失金額為美金 345 元<sup>30</sup>。網路詐欺中支付款項方式有：Credit Cards (30%)、bank account debit (23%)、check (16%)、wire transfer (15%)、money order (11%)、cash/cash advance (4%)，可看出美國網路消費購物者，以信用卡支付購物價金者佔多數，而付現金或預先付現則只佔 4% 的比例。

#### 二、我國網路詐欺現況

據報載，台灣的電話恐嚇、詐欺案件發生率，世界第一<sup>31</sup>。根據內政部警政統計年報資料顯示<sup>32</sup>，包括詐騙集團在內的詐欺背信案，最近 5 年犯罪比率從 2001 年的

<sup>27</sup>The term "Internet fraud" refers generally to any type of fraud scheme that uses one or more components of the Internet - such as chat rooms, e-mail, message boards, or Web sites - to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to other connected with the scheme,  
<http://www.internetfraud.usdoj.gov/#What%20Is%20Internet%20Fraud>, (2006/Feb/26)。

<sup>28</sup>"IC3 2005 Internet Fraud - Crime report", [http://www.ic3.gov/media/annualreport/2005\\_ic3report.pdf](http://www.ic3.gov/media/annualreport/2005_ic3report.pdf), (2006/May/1)。

<sup>29</sup>"Internet Scams Fraud Trends January-December 2005", [http://www.fraud.org/2005\\_Internet\\_Fraud\\_Report.pdf](http://www.fraud.org/2005_Internet_Fraud_Report.pdf), (2006/Feb/26)。

<sup>30</sup>Consumer Fraud and Identity Theft Complaint Data January-December 2005, page3-4,  
<http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf> (2006/Feb/26)。

<sup>31</sup>郭尚義，防制電話詐欺與簡訊詐欺之治標與治本對策，ET today.com 東森新聞報，2005 年 4 月 20 日，  
<http://www.ettoday.com/2005/04/20/320-1779631.htm>, (2006/Mar/3)。

<sup>32</sup>參見內政部警政署網站，統計資料之警政統計年報，網址：

16,082 件（佔全部刑案的 3.27%），年年節節升高，到 2005 年變成 43,342 件（佔全部刑案 7.79%），以急遽之速度成長中。又從前開年報統計中亦可觀察出，近年詐欺背信案手法翻新，佔刑案數比率也逐年增加，在 2003 年即已躍居第二多犯罪手法，僅次於竊盜案，由此可見，防制詐欺案件乃當務之急。其中網路詐欺之發生率，2001 年僅佔的全部詐欺背信案件的 0.44%，然於 2005 年已攀升至全部詐欺背信案件的 8.99%，成長了八倍之多<sup>33</sup>，而在可預見之未來，隨著資訊教育之普及與網路網路、電子商務之快速發展，網路詐欺發生之比例佔全部詐欺或網路犯罪之比例只有越來越高之趨勢。

### 三、我國常見網路詐欺類型

（一）網路購物詐欺：隨著網際網路的興起，電子商務活動日漸活絡，其中 B2C（Business to Consumer 簡稱 B2C，指企業透過網際網路對消費者所提供的商業行為或服務）、C2C（Consumer to Consumer 簡稱 C2C，個人透過網際網路對個人進行交易行為）的市場生意興隆，新商品不斷上架，也因此讓不肖業者有機可乘。這些不肖業者大多是利用大型購物網、拍賣網站作掩護，以低價名牌精品，或是 3C（Consumer Electronics / Computer / Communication）產品為幌子，讓購買者見獵心喜，出價競標，再進行詐財或騙物的行為。歸納線上拍賣購物常見的詐騙術有以下幾種態樣<sup>34</sup>：

1. 買空賣空型：（1）先用假資料申請拍賣帳號，再至其他大牌的網站中下載圖檔，貼在網頁上叫賣，並找他人充當競標者，以博取購買者的信任，線上付款之後，卻永遠等不到貨<sup>35</sup>。（2）利用高單價商品在網路廣告上以便宜離譜的價格拍賣，並大方告訴網友「收到貨再付款」。等網友收到貨後認為應該不會有問題，就把錢匯給賣家，事實上賣家是用偽造的假信用卡訂貨，商品直接從郵購公司寄到網友手中。
2. 以低價或瑕疵品濫竽充數型：（1）在網路上刊登非常低廉之商品如：電腦燒錄器、行動電話等二手貨或大補帖等物品，誘使民眾匯款，再以劣品或不堪使用的貨物充數，交易完成後即避不見面。（2）網路假賣車<sup>36</sup>：以「超低價販賣高級進口借屍還魂車，因為有問題無法當面交車，必須先預付部分款項」之詐術，或其他技巧，逐步誘騙被害人轉帳到人頭帳戶。
3. 名牌低價型：在大型拍賣網站刊登拍賣 LV、GUCCI 等高級品牌名號之真品，而售價不到市價二分之一，並利用網站的信用背書與評等機制，博取網友信任，購買者誤以為真而交付款項。實際上之情形為賣家送到網站評等的商品大多是真貨，只是交貨時給的是仿冒品。又近來最新詐騙手法為，詐騙者在網路上購

---

[http://www.npa.gov.tw/stats.php?page=content06\\_1&id=70&tr\\_id=&pages=1](http://www.npa.gov.tw/stats.php?page=content06_1&id=70&tr_id=&pages=1)，（2006/Mar/4）。

<sup>33</sup>內政部警政署統計室提供資料，1、臺閩地區詐欺背信統計，2001 年至 2005 年之發生數分別為：16082、26397、37191、40001、43342。2、臺閩地區電腦網路犯罪發生數及破獲數-依按類別，2001 年至 2005 年電腦網路中詐欺背信之發生數分別為：71、869、3061、2500、3899。資料未公開。

<sup>34</sup>E 騙術宣導，司法院政風處第一科，

[http://w2.judicial.gov.tw/ged/workSystem/3\\_workshow.asp?work\\_id=46](http://w2.judicial.gov.tw/ged/workSystem/3_workshow.asp?work_id=46)（2006/Mar/1）。

<sup>35</sup>台北市警察局犯罪預防宣導團，常見詐騙犯住類型及防制之道，

[http://www.tcpd.gov.tw/all-tcpd.php?topage=1&id=243&t\\_type=d&tcpdlink=防制詐騙專區#網路交易詐騙](http://www.tcpd.gov.tw/all-tcpd.php?topage=1&id=243&t_type=d&tcpdlink=防制詐騙專區#網路交易詐騙)（2006/Mar/1）。

<sup>36</sup>驚悚回顧國內 2004 資安事件，<http://www.acc.ncku.edu.tw/>（2005/May/5）

買偽造之名牌保證書或他人購買真品之發票後，利用取得之偽造保證書或發票以取信於網路購買者後，待取得款項後再交付仿冒之商品。

- 駭客攔截競標者資料，再假冒賣方通知該競標者，並要求付款到特定帳戶，使競標者誤以為是賣方而付款<sup>37</sup>。此種類型詐欺常在 YAHOO 奇摩拍賣平台發生，如：詐騙者等某拍賣商品結標後，在該商品網頁上看到得標者為 james123 後(因 YAHOO 奇摩有提供免費之電子信箱，且多數競標者之帳號為求方便均會選擇與電子信箱相同之帳號)，即猜到得標者之聯絡電子信箱為 james123@yahoo.com.tw，遂冒充賣方以電子郵件方式告知得標者匯款至特定帳戶，得標者不疑有他而匯入款項，等取不到貨後，始知被騙。又最近發生一實際案例，即詐騙者得知賣家帳號為「jack\*\*\*chao2002」，即以極為相似之「jack\*\*\*chao\_\_2002」帳號冒充為賣家並發出「截標信」，致使得標者誤信而將款項匯入詐騙者指定之帳戶<sup>38</sup>。

#### (二) 提供商品、服務之詐欺類型：

- 網路銀行轉帳詐欺：在報紙刊登廣告或散發傳單，宣稱可幫助民眾貸款、加盟、購買法拍物等，要求被害人先行至其指定銀行開戶，存入相當之權利金或保證金，並設定電話語音約定轉帳帳戶(網路銀行服務及語音查詢帳戶餘額)，然後進一步要求被害人提供語音查詢餘額密碼及身分證證件、地址等相關資料以便確認，利用電話語音轉帳功能(網路電子交易)將被害人之存款轉帳領走。
- 網路虛設行號或民宿網頁詐欺：(1) 在網路上虛設高科技公司，以低價販售高科技新產品，並在網路上展示 MP3 隨身聽等產品，該公司及網站俟收到網友所寄購買產品之款項後，公司便人去樓空，網站亦隨之關閉。(2) 虛設民宿網頁，利用春節期間必須全額預付，多人受騙<sup>39</sup>。
- 在網路上散播提供色情服務：在網路上散發內容為「來電可找辣妹」或其他援交廣告之訊息，誘使不特定民眾查詢該訊息時，以查驗身分為由，謊騙對方需先至自動櫃員機(ATM)前按指示操作，匯款至該詐騙集團所收購之人頭帳戶<sup>40</sup>。

#### (三) 信用卡詐欺類型：

- 利用以下方式取得偽造或他人所有之信用卡卡號，進而上網冒名消費購物：(1) 網路駭客入侵攔截被害人在電腦網路上購物消費之信用卡卡號。(2) 利用信用卡公司在網路上登載檢測偽卡程式，輸入一組正確信用卡卡號，程式卡產生數千至數萬各信用卡卡號。
- 信用卡犯罪集團利用偽造的信用卡、或是他人遺失的信用卡來向郵購公司訂購網路消費者所要購買之貨品，並指明將該項商品寄送到訂購消費者的住所。網路消費者在收到沒有問題的商品後，就會將價款匯入犯罪集團所指定的帳戶，

<sup>37</sup>同前揭註第 36。

<sup>38</sup>陳亮諭，「假冒賣家帳號詐財 網拍陷阱」，聯合報，C4 版，2006 年 3 月 22 日。

<sup>39</sup>同前揭註第 36。

<sup>40</sup>桃園地方法院檢察署 93 偵 14660 號、94 偵 8296、9024、9882、11252 號書類，台南地方法院檢察署 94 偵字第 5709 號書類。

但等到郵購公司發現真正持卡人聲明未曾訂購相關商品而拒絕付款時，郵購公司便會轉向追查商品送達處所。這時事實上已經付出貨款的消費者，就得再付出一筆貨款，或者眼睜睜的看著貨品被郵購公司收回<sup>41</sup>。

3. 利用「e COIN」之退款服務詐騙金錢：盜取他人信用卡之資料，進而冒用他人名義進入網路商業服務網，並盜刷信用卡購買遊戲卡帳號點數後，復利用該網站之退款服務，將儲值之款項轉入指定之帳戶<sup>42</sup>。

#### (四) 網路釣魚型詐欺：

1. 拷貝網路銀行網站的網頁，假冒該銀行之名提供「活期儲蓄存款」、「定存本利和」、「定期儲蓄存款利率」、「零存整付本利和」等多功能，讓使用者誤上冒牌的網路銀行，洩漏個人身分證件或銀行帳號及密碼等重要資料，再進行盜領。
2. 假冒銀行名義向客戶發出 email 誘導客戶到假網頁留下帳戶密碼，再進行盜領。

#### (五) 網路遊戲詐欺型<sup>43</sup>：

1. 詐騙取得線上遊戲之帳號密碼後，輸入帳號密碼並取得寶物：而取得帳號密碼之方式常見者有以下幾種：(1) 在線上假冒他人名義詢問帳號密碼。(2) 寄發電子郵件，而該郵件內容謊稱是遊戲公司進行活動或恭喜玩家中獎，並要求玩家回報帳戶密碼即可取得稀有寶物等。(3) 佯稱自己是「可愛妹妹，想寄照片給你」的方式，騙得玩家之電子信箱號碼後，寄上夾帶木馬程式檔案的信件給玩家，玩家下載並開啟檔案同時，程式就會伺機擷取回傳玩家的帳號密碼。
2. 虛擬寶物交易詐欺：(1) 用線上遊戲中之廣播頻道、拍賣網站或虛擬寶物交易市場專門網站等管道，向玩家佯裝欲買賣裝備道具，然於取得現金或虛擬裝備寶物後，即不見蹤影。(2) 其他網路詐騙寶物之手法：如在網路上佯裝玩家朋友，向玩家借用寶物後，即逃逸無蹤。或是誘騙玩家將寶物丟掉，趁機拾取寶物。又或者是誘騙玩家可代為複製寶物使玩家陷於錯誤而交付寶物。

#### (六) 提供工作機會詐騙型<sup>44</sup>：

1. 利用電子郵件方式詐騙：網路上之有心人士利用網路隱匿的特性，以「一函多發」方式，寄出大量的電子郵件給不特定對象或全部的網路使用者。而這些「不請自來」的電子郵件信函中，通常都聲稱提供各式各樣的賺錢機會，或宣稱你已被「特別挑選」，可以獲得價值不菲的獎品或旅遊，而結果這些都只是一些吸引消費者上當的騙局而已。
2. 利用網站之電子廣告信詐騙：詐騙集團利用近年失業率之攀升，而民眾求職不易之機會，以政府 200 億元公共服務擴大就業方案為誘餌，透過網站的電子廣

<sup>41</sup>同前揭註 34。

<sup>42</sup>PC home on line 新聞，2005 年 7 月 22 日，  
<http://news.pchome.com.tw/society/chinatimes/20040731/index-20040731023624240700.html>  
(2005/Oct/11)

<sup>43</sup>王文君、賴文智，線上遊戲防騙-線上遊戲常見詐騙手法與因應之道（一），  
<http://www.is-law.com/OurDocuments/GM0011WA.pdf>，(2006/Mar/1)；王文君、賴文智，「線上遊戲防騙-線上遊戲常見詐騙手法與因應之道（二）」，  
<http://www.is-law.com/OurDocuments/GM0012WA.pdf>，  
(2006/Mar/1)。

<sup>44</sup>小心網路騙局，公平會新聞稿，<http://www.ftc.gov.tw/news0918.htm>，(2006/Mar/1)。

告信，內容指出職訓局釋出 11.5 萬個工作機會，並臚列全省各級縣市政府、北高市議員、全省各公立學校、績優國營事業、各縣市銀行及農漁會等名額數十至數百名約聘雇人員職缺，表示只要繳交 2000 元加入會員，保證可獲錄取得到就業機會。經查發現詐騙集團刊登電子廣告信的網站網址之伺服器設於南太平洋某小島，難以追查<sup>45</sup>。

(七) 利用網路電話詐騙<sup>46</sup>：歹徒利用網路電話不顯示真實發話號碼之特性進行電話詐騙，而歹徒利用此一特點進行電話詐騙，使得受騙者及警方皆難以追查，致使歹徒逍遙法外。

(八) 其他類型：

1. 利用民眾在網路上張貼協尋遺失物，佯稱握有被害人之遺失物，並向被害人進行詐騙或恐嚇之行為<sup>47</sup>。
2. 網路交友詐欺：利用網路聊天室認識多名異性網友，假冒身份如偽稱某知大學研究生、課餘兼職拍攝廣告等，並將電視廣告模特兒照片寄給對方，最後假藉理由向網友借錢，款項到手後不知去向。
3. 網路金光黨詐欺（或稱網路老鼠會<sup>48</sup>）：歹徒在網路上以「大家來賺錢，這是真的，不是騙人的」標題，在新聞討論群組張貼郵遞名單事業信件，信中列有 500 人姓名地址，指示網友寄給名單上 5 人各 100 元，再將列於第一位者之姓名自名單除去，交第二名以下者皆往前遞補一位，最後將自己姓名置於第五位，以此類推，信中並告訴網友當自己的姓名遞補至第一位時將可獲得約 7000 萬元。

## 2.2 人頭帳戶

### 2.2.1 人頭帳戶之定義與類型

#### 一、人頭帳戶之定義

何謂「人頭帳戶」？廣義定義：利用他人名義於金融機構開立帳戶並取得存款契約之相關服務，或是利用他人已開立之帳戶而受讓金融機構存款契約之相關服務，即俗稱之人頭戶。狹義定義<sup>49</sup>：利用他人名義申請或已開立之帳戶，用以規避政府相關法令限制規定，或掩飾其犯罪意圖及阻斷犯罪線索之犯罪行為，無論此人頭是否知情，均蓋稱之為「人頭帳戶」。而本文所欲探討防範之人頭戶，僅限於用於不法行為之人頭戶，若未涉不法用途之人頭戶，並非刑事偵查與防制之重點，故本文以下所稱之人頭戶，係指前開狹義定義之人頭戶，先予說明。

而人頭戶之存在與利用，往往成為犯罪者從事非法行為之工具，易言之，即犯罪者假借第三人名義之帳戶，掩飾其身分與企圖，從事各種犯罪活動，藉以逃避警察之追緝。邇來，又因電腦網路之使用普及，犯罪者藉由網路銀行及電子轉帳之大量運用，

<sup>45</sup>同前揭註第 34。

<sup>46</sup>網路安全新聞總覽，<http://www.acc.ncku.edu.tw/>（2005/May/7）

<sup>47</sup>Hinet 新聞網，<http://times.hinet.net/SpecialTopic/940525-cheat/1425463.htm>，（2005/July/22）。

<sup>48</sup>張維平，我國網路犯罪現狀分析，<http://www.ccpb.gov.tw/internet-fraud-01.htm>，（2005/ July /22）。

<sup>49</sup>陳茂益，「金融交易『人頭戶』洗錢犯罪問題探討與建議」，中華民國九十一年洗錢防制工作年報，第 74 頁，法務部調查局，2003 年 4 月出版。

只要瞬間即可將龐大之犯罪所得移轉至他處甚至國外，使得資金流向追查益加困難，導致社會蒙受巨大損失，危害國家經濟安定。何況，台灣地區各種人頭資料取得容易與民眾個人資料外洩之情形，可謂居世界之冠<sup>50</sup>，又人頭戶雖非我國特有現象，惟氾濫情況確屬我國特別嚴重<sup>51</sup>。從而，解決人頭帳戶非法使用之問題，已達刻不容緩之境，否則將對我國治安形成一大漏洞。

## 二、類型

人頭戶防範之課題，首先應探討人頭戶存在之原因，始得正本清源，對症下藥擬定防範措施。然因利用人頭戶從事不法行為之態樣眾多，本文僅就實務上常見之型態簡述之，而依產生人頭戶之原因，可區分為：規避法令管制、不法交易、租稅安排、銀行貸款、洗錢等類型<sup>52</sup>。

- (一) 規避法令管制型：為規避行政機關之管理措施，而尋求規避之方法，人頭戶因此產生。如為規避公司法第 197 條之董事申報股份義務限制，即股份有限公司董事為規避於任期中不得轉讓超過二分之一的股份及為免股份增減須向主管機關申報、公告之規定，便會利用人頭戶代為持股。又如為規避證券交易法第 157 條歸入權行使之規定：即發行公司董事、監察人、經理人或持股超過百分之五十之大股東，利用他人戶頭從事股票短線交易，以規避該條公司得請求將買賣股票所獲得之利益歸於公司之規定。雖然證券交易法第 22 條之 2 第 3 項規定，發行公司董事、監察人、經理人或持股超過百分之五十之大股東等人所持有之股票，應包括其配偶、未成年子女及利用他人名義者，但實務上要證明係以他人名義持股或買賣股票甚為困難。再如，我國企業或投資者慣用人頭戶經由集中市場收購股權，即收購者可以透過人頭戶分散收購股權之比例，以規避證券交易法第 43 條之 1 第 1 項之申報義務<sup>53</sup>。
- (二) 不法交易型：此類行人頭戶的產生，係因為謀求不法之利益所生之安排，典型為利用人頭帳戶從事證券交易之內線交易、短線交易、操縱行為及丙種墊款。如：94 年爆發之勁永案，即是透過人頭帳戶放空勁永公司股票以謀不法利益<sup>54</sup>。
- (三) 租稅安排型：利用人頭戶來減免或逃漏各種稅捐。如：國內部分公司在辦理股票上市、上櫃時，為符合上市審查準則股權分散規定，大股東或董監事會將持股過戶至他人名下，利用人頭戶分散股權，藉以規避持股變動申報制度及分散

<sup>50</sup>內政部警政署刑事警察局委託研究報告（申請機構：中央警察大學，研究主持人：范國勇，共同主持人：張平君），ATM 轉帳詐欺犯罪之實證研究，第 42 頁，2004 年 12 月。

<sup>51</sup>人頭戶之風險以及法律責任簡介，中華民國證券商業同業公會，<http://www.csa.org.tw/csa10/%E4%BA%BA%E9%A0%AD%E6%88%B6%E4%B9%8B%E9%A2%A8%E9%9A%AA%E4%BB%A5%E5%8F%8A%E6%B3%95%E5%BE%8B%E8%B2%AC%E4%BB%BB%E7%B0%A1%E4%BB%8B.doc>，(2006/Mar/4)。

<sup>52</sup>台灣證券交易所股份有限公司委託研究報告，（研究人蓋華英、楊佳政、吳淑惠），如何消弭證券市場人頭戶氾濫問題，第 2-1 頁，1994 年 9 月 30 日。

<sup>53</sup>王藏偉，「公開收購有價證券之制度及運作淺析」，證券暨期貨月刊，第 23 卷，第 7 期，2005 年 7 月 16 日出版，<http://www.sfb.gov.tw/reference/magazine/9407/ss1a.doc> (2006/ Mar /4)。

<sup>54</sup>廖德琦，「法務部：勁永案 11/7 前水落石出」，Taiwan New 新台灣雜誌，第 500 期，2005 年 10 月 20 日，<http://www.newtaiwan.com.tw/bulletinview.jsp?period=500&bulletinid=23029>，(2006/ Mar /4)。

個人股利所得，但此舉已經涉及逃漏稅<sup>55</sup>。

(四) 銀行貸款型：為確保金融體系之健全運作，「分散授信風險原則」成為經營授信業務之金融機關之金科玉律，故銀行法就銀行授信業務特設內部人員授信限制及對個人或同一企業授信總額之限制，有該法第 32、33 條、第 33 條之 3 等規定可參。然而，實務上常見農會總幹事或職員利用人頭戶貸款，規避銀行法就內部人員授信之限制，或利用人頭戶之「分散借款、集中使用」之方式，超額貸款規避個人授信總額之限制<sup>56</sup>。又或是集團利用無報稅所得或報稅所得偏低之「人頭戶」違法申貸，並以「分散借款、集中使用」方式大量套取銀行之資金，規避銀行法對個人或同一企業授信總額之限制<sup>57</sup>。

(五) 洗錢型：實務上常見多為常業詐欺類型，即以不同之詐騙、恐嚇手法誘使或迫使被害人匯款至人頭帳戶<sup>58</sup>，或利用人頭帳戶從事交易行為，進而將人頭帳戶內之款項提領一空，致使被害人求償無門。又如販毒集團將販毒不法所得，利用人頭戶進行交易達到洗錢目的。

### 三、人頭戶取得之管道

實務上人頭帳戶取得之管道，不外乎以下二種：第一種，「非自願性之人頭戶」，以偽造證件至金融機構申辦帳戶：就金融機構而言，設立人頭帳戶最典型之手法，就是不法之徒利用偽造、變造他人遺失或竊取所得之身分證向金融機構申請存款開戶、辦理貸款、申請信用卡，並以相同偽造文件向不同之金融機構申請，以獲取人頭帳戶<sup>59</sup>。第二種，「自願性之人頭戶」，利用各種管道向他人取得申辦之帳戶：而取得之途徑多樣，有以下幾種：1. 友人介紹：帳戶所有人透過友人介紹而將帳戶出賣或出租予他人。2. 報章雜誌報導：詐欺集團之成員會在報紙、雜誌等刊登「高價收購手機門號及存摺」、「存簿換現金」或「買賣郵局 5000、銀行 3000、市話電話卡及現今送你，不用還」、「現在馬上付，郵局一律 6000 元起，長期可拿，合法免還」等廣告<sup>60</sup>，吸引急需用錢之貪小便宜者主動與刊登廣告者聯繫後，指示、帶領欲販賣帳戶者前往銀行辦

<sup>55</sup> 鄭琪芳，利用人頭戶逃漏稅財政部追查，自由新聞網，

<http://www.libertytimes.com.tw/2004/new/sep/23/today-e4.htm> (2006/ Mar /4)。

<sup>56</sup> 見彰化地檢 90 年度偵字第 3992 號起訴書。

<sup>57</sup> 財政部對處理中興銀行案之說明，中央存款保險股份有限公司網址：

<http://www.cdic.gov.tw/ct.asp?xItem=65&ctNode=192> (2006/May/1)。

<sup>58</sup> 實務上利用人頭戶進行詐騙之態樣甚多，近來發現在網路上販賣盜版光碟的人，亦會利用人頭戶來規避查緝。目前大補帖網站業者為逃避檢警查緝，皆使用人頭申請郵局帳戶並申請金融卡，或上網或在跳蚤雜誌上以一至三千不等的價錢購買人頭存款帳戶、郵政信箱、鑰匙、金融卡，再冒用他人身分辦理代收貨款服務，再以代收貨款服務寄送盜版光碟，而所得不法款項則以金融卡提領。由於金融人頭戶可如此輕易購得，使得這些人頭戶成為大補帖業者從事不法之護身符。見張維平，我國網路犯罪現況分析，<http://www.ccpb.gov.tw/internet-fraud-01.htm>，(2006/ Mar /4)。

<sup>59</sup> 鐘慧珍，「防制犯罪集團利用銀行存款帳戶進行詐騙之執行成果報告」，法務部調查局「經濟犯罪防制執行會議」第 101 次會議專題報告，第 3 頁，2004 年 12 月 29 日。

<sup>60</sup> 雲林地方法院檢察署 94 年度偵字第 2920 號起訴書。此案係雲林地檢署指揮刑事局、北港警分局，破獲以陳世鴻為首的收購人頭帳戶詐騙集團，逮捕 5 名嫌犯，起出 40 餘戶人頭帳戶。嫌犯在報上刊登「存簿換現金」廣告，4 個月來已陸續收購 400 餘戶人頭戶，詐騙金額可能超過 10 億元。且該犯罪集團以 3000 至 6000 元代價收購人頭戶，並以老鼠會傳銷方式吸收成員擴大犯罪組織，平均每日可收購 3 至 4 戶，目前已收 400 餘戶，清查後每戶有上百人受害，如果每人被詐騙 10 萬元，金額可能高達數 10 億元。

理開戶之相關程序，並當場交付剛開戶之金融卡、存摺等資料，或由欲販賣者直接交付業已開戶、使用之存摺、金融卡等物予詐欺集團之成員<sup>61</sup>。3.利用求職面洽之機會：詐欺集團在報紙上刊登求職、求才廣告，吸引急需工作者前往面洽後，再利誘該求職者販賣或出租帳戶以牟利。4.利用網路收購<sup>62</sup>：利用網站之聊天室，在網路上廣交缺錢的年輕男、女，以提供所謂快速賺錢方法，利誘販售個人帳戶。如：在「UT HOME 網際空間」網站之「網路四季風聊天室」暱稱「高租郵銀簿～換現」之留言，進而誘使瀏覽聊天室者出售帳戶<sup>63</sup>。又自願出租、出借帳戶之帳戶持有人，其所得之代價，1000元到10000元均不等。而這些大量收來的人頭帳戶，則提供予從事「簡訊詐欺」、「信用貸款詐欺」、「網路購物詐欺」、「假交友聯誼中心」等不同類型的詐欺集團使用。

### 2.2.2 提供人頭帳戶之法律責任

依照人頭帳戶之不同類型所觸犯之法律，可能有：民法、刑法、公司法、證券交易法、洗錢防制法、稅捐稽徵法等。本文將分就不同類型及所觸犯法律整理如下表3：

表 3 人頭帳戶提供者之法律責任表

利用人頭帳戶之類型		提供帳戶者之法律責任
規避法令管制型	公司法第 197 條	無
	規避證券交易法第 157 條歸入權行使之規定	無
	證券交易法第 43 條之 1 第 1 項之申報義務	無
不法交易型	證券交易法之內線交易(證券交易法第 157 條之 1 第 1 項)	民事責任：依證交法第 157 之 1 第 2 項規定，與行為人共負損害賠償責任。 刑事責任：與行為人共同違反證交法第 157 之 1 第 1 項規定，應負同法第 171 第 1 款之刑責。
	證券交易法之短線交易(證券交易法第 157 條第 1 項)	民事責任：人頭戶仍是民事交易買賣之名義人，故仍須負擔契約之相關責任。 若買賣股票涉有詐欺情事，則有刑事責任：與行為人共同違反證交法第 20 條第 1 項規定，應負同法第 175 條之刑責。

<sup>61</sup>桃園地方法院 94 壩簡 976 號及 94 壩簡 122 號之判決。

<sup>62</sup>謝中凡，網路蒐購人頭戶轉賣 年轉千萬，中華日報，2004 年 12 月 22 日，

<http://www.cdnnews.com.tw/20041223/news/shwx/733720002004122219204025.htm>，(2006/ Mar /4)。

<sup>63</sup>台北地方法院 94 年度簡字第 1863 號判決。

表 3 人頭帳戶提供者之法律責任表 (續)

利用人頭帳戶之類型		提供帳戶者之法律責任
不法交易型	證券交易法之操縱行為(證交法第 155 條第 1 項)	<p>民事責任：依證交法第 155 條第 3 項規定，與行為人共負損害賠償責任。</p> <p>刑事責任：與行為人共同違反證交法第 155 條第 1 項規定，應負同法第 171 第 1 款之刑責。</p>
	證券交易法之三種墊款	<p>民事責任：人頭戶仍是民事交易買賣之名義人，故仍須負擔契約之相關責任。</p> <p>刑事責任：與證券商共同違反證交法第 60 條第 1 項規定，應負同法第 175 條之刑責。</p>
租稅安排型	利用人頭戶減免逃漏各種稅捐	違反稅捐稽證法第 43 條幫助他人逃漏稅。
	公司大股東、董監事利用人頭戶分散股利所得	
銀行貸款型	農會總幹事或職員利用人頭戶貸款，規避銀行法就內部人員授信之限制，或利用人頭戶之「分散借款、集中使用」之方式，超額貸款規避個人授信總額之限制。	<p>民事責任：人頭戶仍為借款名義人，仍須負擔償還貸款之責任。</p> <p>刑事責任：與行為人共同違反銀行法第 32、33、33 之 3 規定，應負同法第 127 條之 4 第 1 項之刑責。</p>
	集團利用無報稅所得或報稅所得偏低之「人頭戶」違法申貸，並以「分散借款、集中使用」之方式大量套取銀行之資金，規避銀行法對個人或同一企業授信總額之限制	<p>民事責任：人頭戶仍為借款名義人，仍須負擔償還貸款之責任。</p> <p>刑事責任：與行為人共同違反銀行法第 33 之 3 規定，應負同法第 127 條之 4 第 1 項之刑責。</p>
洗錢型	常業詐欺類型	<p>民事責任：對於存戶內之不法取得金錢，被詐欺之人仍得依不當得利規定請求返還。</p> <p>刑事責任：刑法幫助詐欺罪及違反洗錢防制法第 9 條之規定。</p>
	將販毒等不法所得，利用人頭帳戶進行交易以達到洗錢目的	刑事責任：違反洗錢防制法第 9 條第 2 項之規定。

### 2.2.3 各國家對防制人頭帳戶法律面之規範

使用人頭帳戶之詐欺，在其他國家發生的並不多見。各司法先進國家中僅有日本的情形與我國相似<sup>64</sup>，故世界各國對防制人頭帳戶之規定，均散見於各個法律中，本文以為可區分為金融機構管制及法律刑罰二方面，以下分別介紹之。

#### 一、金融機構管制方面：

金融機構對防制人頭帳戶所得採取之措施，大都與洗錢防制規定相關，其中又可細分為帳戶身份辨明方面、留存交易紀錄及可疑交易匯報方面，以下分別介紹美國及日本之相關規定：

(一) 美國：由於美國對於洗錢防制的規定散見於各個法律與行政規定，簡述如下：

1. 確認客戶身份：美國國會於 1970 年制定「銀行紀錄及國外交易法」，通稱「銀行秘密法」(Bank Secrecy Act of 1970,BSA) 其立法目的在於報告或紀錄客戶交易資料，以便取得有助於稅務的調查及洗錢犯罪偵查、起訴的證據，故規定於刑事、稅捐或法定調查程序上有必要時，應就金錢往來交易行為予以報告，或作成紀錄；特別是授權財政部長得規定金融機構就特定交易行為予以報告。依照該法及「貨幣與外國交易之金融記錄保存與報告規則」(Financial Record keeping and Reporting of Currency and Foreign Transactions) 之規定，超過 10000 美元現金之交易應予報告，金融機關並應確認登記交易者之姓名、地址等基本資料，如果是由代理人代辦者，亦應登記代理人之基本資料<sup>65</sup>。
2. 保留交易的紀錄：依照前開「貨幣與外國交易之金融記錄保存與報告規則」之規定，對於每筆 10000 美元以上之交易，應留存授信紀錄、交易資料等，而保留之期限為 5 年<sup>66</sup>。
3. 可疑交易匯報：美國之銀行秘密法採用定額申報，規定貨幣交易報告、跨國運送貨幣工具報告、外國金融帳戶報告、外國金融代理機構交易之報告等均在超過一定金額（目前為 10000 美元）時，均需申報<sup>67</sup>。另外美國於 1992 年制訂之 Annunzio-Wylie 反洗錢法，則明文採取可疑申報制，該法第 1517 條授權美國財政部得制訂行政規則，要求金融機構將可疑的交易向「經濟犯罪調查中心」申報<sup>68</sup>。

(二) 日本

日本政府鑑於使用人頭帳戶的詐欺在日本日益嚴重，故於 2002 年 4 月 26 制定「關於金融機構關客戶之身份確認法」<sup>69</sup>，並於翌年 2003 年 1

<sup>64</sup>平成 18 年之被害總金額約為 20 億日圓。其種類、方式可參見日本警視廳之網 [http://www.npa.go.jp/safetylife/seianki31/1\\_hurikome.htm](http://www.npa.go.jp/safetylife/seianki31/1_hurikome.htm)，(2006/May/1)。

<sup>65</sup>王麗芳，「洗錢暨防制洗錢相關法律責任之省思—兼論美國九一一事件後防治洗錢之新發展」，中國文化大學法律系，碩士論文，第 94 頁，2002 年 6 月。

<sup>66</sup>同前註 65。

<sup>67</sup>同前註 65，第 95 頁。

<sup>68</sup>同前註 65。

<sup>69</sup>日本平成 14 年法律第 32 號：金融機關等による顧客等の本文確認等に関する法律，參見

月 6 日正式施行，該法希望可以達到健全金融機構健全客戶管理體制之目的，以及確保司法機關關於犯罪組織犯罪收益及資金來源之情報蒐集，並更進一步希望可以防止經由金融機構提供恐怖活動資金法第 1 條所列犯行的資金<sup>70</sup>。該法主要內容可分為以下幾個部分：

1. 明定「金融機構等」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、金融期貨交易業者等。(第 2 條)<sup>71</sup>。
2. 確認本人義務及該記錄之製作、保存：金融機構受理客戶開立存款帳戶或高額現金交易時(200 萬日圓以上)，必須以當事人提出駕照、護照、健康保險證、居留證等政府機關發行之證明書類的方式，確認客戶(自然人時)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(第 3 條第 1 項)。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)均進行本人確認(第 3 條第 2 項)。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(第 3 條第 4 項)。又在製作確認本人紀錄後，即使在結清該帳戶後，該相關紀錄仍須保存 7 年(第 4 條)<sup>72</sup>。
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 7 年(第 5 條)。
4. 刑罰規定：
  - (1) 行政當局對違反本法第 3 條第 1 項至第 3 項(確認本人義務等)、第 4 條(製作、保存確認本人義務等)、第 5 條(製作、保存交易紀錄的義務)規定時，得命令其採改善之必要措施(第 9 條)，對違反規定者，處 2 年以下有期徒刑，或科或併科 300 萬日幣以下罰金(第 14 條)。
  - (2) 對未提出與其業務相關報告、資料或提出虛偽的報告、資料或對依據第 8 條第 1 項規定之詢問未予答覆、虛偽答覆或拒絕、阻礙、規避該項規定者，處 1 年以下有期徒刑，或科或併科 300 萬日幣以下罰金(第 15 條)。
  - (3) 以隱藏本人特定事項的目的，違反第 3 條第 4 項(客戶或其代表人不得偽造本人特定事項)規定者，處 50 萬日幣以下罰金(第 16 條)。
  - (4) 兩罰規定：法人之代表人、法人或自然人之代理人、受雇人或其他從業人員，因執行業務違反下列各款所示規定時，除處罰行為人外，對該法人科以各該款所定之罰金。

又日本之組織犯罪處罰法：原本日本洗錢防制制度，係以防止未來藥物犯罪之發生為重點，而日本國會於 1999 年立法通過之組織犯罪處罰及

---

<http://www.fsa.go.jp> (2006/May/9)。

<sup>70</sup>參見日本金融廳網站 [www.fsa.go.jp/policy/honninkakunin/00.pdf](http://www.fsa.go.jp/policy/honninkakunin/00.pdf)。

<sup>71</sup>同前註 69。

<sup>72</sup>李傑清，「我國洗錢防制法『確認身份』規定之研究—與日本『本人確認法』比較之觀點」，九十二年洗錢防制工作年報，第 54 頁以下，法務部調查局，2004 年 4 月。

犯罪收益規範法<sup>73</sup>，為日本對於組織犯罪首次以概括性規定所制定的刑事法。在組織犯罪處罰法中，對於組織犯罪規定並不僅限於毒品犯罪，即使是其他各種犯罪，為防止組織犯罪利用其犯罪所得擴大、維持其組織並影響合法的經濟活動，大幅擴張洗錢前提犯罪之範圍，不限於藥物犯罪，而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第 54 至 58 八條，規定疑似洗錢交易之申報制度（麻藥特別法之可疑交易申報制度廢止）。疑似洗錢交易申報制度之目的，除便利隱匿犯罪收益等罪及其前提犯罪偵查之主目的外，亦有防止犯罪者利用金融機構存款及確保對於金融機構信賴之次要目的。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。其中第 54 條第 1 項規定，金融機構認為疑似違反本法第 10 條及麻藥特別法第六條之行為（隱匿不法收益等及藥物犯罪收益等罪）負有向行政命令所定之行政機關申報義務；而第 2 項規定金融機構不得洩漏給當事人或其關係人<sup>74</sup>。

## 二、刑罰遏止方面：

### （一）美國：

若行為人開帳戶之初即是要將帳戶交付他人以做為掩飾非法取得之金錢，則本文以為可能構成銀行詐欺（Bank fraud 18 USCS § 1344）及洗錢防制（laundry of monetary instrument 18 USCS § 1956）之相關刑罰規定。另若開戶後始出售帳戶予他人做為掩飾非法所得，則會構成 Bank fraud 18 USCS 之詐欺銀行罪，又之後詐騙集團利用「車手」將銀行存款提領出來，則應會構成 § 1344 (2) 之行為，銀行詐欺法之法定刑為處有期徒刑 30 年以上或科或併科 100 萬元美金以上。

### （二）日本：

自 2003 年以來利用人頭帳戶詐騙情形已成為一個嚴重的社會問題，而詐騙類型不外乎有「匯款詐欺」、「融資保證金詐欺」及「虛位請求詐欺」等方式<sup>75</sup>，而這些詐欺手法的共通點均是：告知被害人虛偽之事實或巧用各種名目，使被害者受騙陷於錯誤，而將金錢匯入詐騙之行為人所得支配管理之金融機構存款帳戶中，且此類詐欺通常多係利用他人販賣、轉讓或冒名申請之存款帳戶。而利用人頭帳戶詐欺取得財物之犯罪行為，除構成日

<sup>73</sup>日本在 1999 年立法：「組織的な犯罪の處罰及び犯罪收益の規制等に関する法律」，2004 年 12 月 8 日修正，法律第 156 號。

<sup>74</sup>吳天雲，「日本反洗錢制度與我國利法之比較」，九十年洗錢防制工作年報，第 66 頁以下，法務部調查局，2002 年 4 月。

<sup>75</sup>日本之「振り込め詐欺」，係指利用電話假裝親屬、員警、律師、職場上長官等名義要求給付交通事故調解金等名義，要求存入人頭帳戶進行詐騙，又稱之為「オレオレ詐欺」，本文稱之為「匯款詐欺」。另日本之詐欺類型：「融資保證金詐欺」係指詐騙行為人知悉被害人之親屬或家人有急需金錢周轉之困難，即佯裝可貸與金錢，並要求被害人需先給付一筆借款保證金始可借款，而誘騙被害人將借款保證金匯入人頭帳戶；「架空請求詐欺」，是指利用郵件、網路向不特定人送達虛偽名義給付款項之文書，以此方式進行詐騙。參見伊藤涉，「振り込め詐欺」，法學教室月刊，296 期，第 13 頁，2005 年 5 月 1 日。

本刑法第 246 條第 1 項之財物詐欺罪外，若有隱蔽詐取金錢之情形，則另涉組織犯罪處罰及犯罪收益規範法第 10 條之隱匿犯罪收益罪。

而因為詐騙金錢及隱匿犯罪收益之日益嚴重，故於 2002 年制定「關於金融機構關客戶之身份確認法」，雖然依據金融機構與存戶間之契約約定，不得擅自買賣他人之帳戶，但是，在網路上仍常見存款帳戶販賣、轉讓之非法交易，因為如此，日本為防止人頭帳戶販賣、轉帳不法情形之氾濫，故於 2004 年將「關於金融機構關客戶之身份確認」變更法條名稱為「關於金融機構關客戶之身份確認及防止帳戶存摺不當利用法」<sup>76</sup>，並新增第 16 條之 2 之規定。於 2004 年將「關於金融機構關客戶之身份確認」變更法條名稱為「關於金融機構關客戶之身份確認及防止帳戶存摺不當利用法」，並新增第 16 條之 2 之規定。該第 16 條之 2 第 1 項規定：為自己或第三人以冒充他人關於金融機構存款契約服務而取得、受讓金融機構存款契約服務時，處 50 萬日圓以下罰金。無通常商業或金融交易之正當理由而有償取得、受讓者亦同。第 2 項規定，明知第 1 項之目的或無通常商業或金融交易之正當理由而有償提供、交付或轉讓者亦同。第 3 項規定：常業犯前 2 項之罪者，處 2 年以下有期徒刑或科或併科 300 日圓以下罰金。第 4 項規定：以勸誘、廣告或其他類似方法誘使他人犯第 1、2 項之罪者，依第 1 項之規定處罰。

## 2.3 網路詐欺與人頭帳戶

### 2.3.1 網路詐欺與人頭帳戶之關連性

據報載，近年詐騙案已成為危害最烈的犯罪形態<sup>77</sup>，且詐騙集團為逃避偵查，大量運用人頭帳戶為犯罪工具，將騙得款項層層轉匯，經警方查緝發現，追查匯入都是被利用的人頭，人頭戶一般以租買方式取得<sup>78</sup>。在全國刑事會議之結論中亦認為，少數民眾貪圖小利、販賣人頭帳戶，是警方難破詐騙案之主因<sup>79</sup>，警方認為若能有效減少人頭帳戶存在，將可有效降低詐騙案件發生<sup>80</sup>。

又學者章光明認為，就國內狀況而言，網路犯罪中之網路詐欺案件比例逐年升高，其成因複雜，「金融人頭戶之輕易購得」為其主要成因之一，文中提到：「目前大補帖網站業者為逃避檢警查緝，皆使用人頭申請郵局帳戶並申請金融卡，目前網路上或在

<sup>76</sup>將原為「金融機關等による顧客等の本文確認等に関する法律」，改為「金融機構等による顧客等の本文確認等及び預金口座等の不正な利用の防止に関する法律」，參見「ロー・フォーラム—立法の話—『振り込め詐欺』の防止に向けて—携帯電話本人確認・不正利用防止法の成立」，法學セミナー，第 606 期，第 127 頁，2005 年 6 月。

<sup>77</sup>人頭帳戶犯罪，警署強力打擊，台中地檢署電子公佈欄，2003 年 7 月 4 日，[http://www.tcc.moj.gov.tw/html/6/bulletin\\_detail.asp?news\\_id=131&kind\\_id=0](http://www.tcc.moj.gov.tw/html/6/bulletin_detail.asp?news_id=131&kind_id=0)，(2005/May/6)。

<sup>78</sup>申辦貸款未查證，小心成為人頭戶，刑事警察局網站資料，[http://www.cib.gov.tw/crime/crime02\\_2.aspx?no=136](http://www.cib.gov.tw/crime/crime02_2.aspx?no=136)，(2005/Dec/4)。

<sup>79</sup>2004 年 4 月份新聞彙集，參 <http://gptaiwan.org.tw/~ayo/2Info/2004Apr.html>，(2005/Dec/4)。

<sup>80</sup>聯合報，社會版 A8，2005 年 11 月 1 日。

跳蚤雜誌上常見以 1,000 元價錢可購得人頭存款帳戶、郵政信箱、鑰匙、金融卡的廣告，以他人身分辦理代收貨款服務，再使用代收貨款服務寄送盜版光碟，而所得不法款項則以金融卡提領。由於金融人頭戶可如此輕易購得，或借用無辜遊民人頭開戶使得這些人頭戶成為大補帖業者從事不法之護身符。」<sup>81</sup>。又有實證研究報告顯示，新興詐欺案件之共通性，即是大量利用偽造證件、人頭帳戶等犯罪工具，以各種名目要求被害人將指定款項匯入詐欺集團所指定之人頭帳戶中，以詐騙不知情民眾之錢財<sup>82</sup>。且因為金融服務業因自由市場競爭，以追求利用、便利服務為導向，相關帳戶申請手續、審核較為寬鬆，導致為詐騙集團所利用，形成人頭帳戶之氾濫。加之，因我國金融轉帳及提款機領款迅速，詐欺集團要求被害人依指示將匯款匯入人頭帳戶後，詐欺集團成員即會將之再轉入其他人頭帳戶內，並委託他人至不特定地點之提款機將款項提領一空，致使警方在查緝上詐欺案件上困難重重。

作者從事犯罪偵查實務工作發現，檢調機關在接獲被害人被詐騙之申告後，所進行詐欺案件偵查之普遍結果，往往只能查知申請設立人頭帳戶之名義人為何人，很難再據以追查真正實施詐欺犯罪之行為人，使該等詐欺集團之主要成員仍舊逍遙法外，也就是因為如此，詐欺集團仍繼續大量利用「人頭帳戶」進行犯罪，且詐欺案件之發生亦層出不窮，故提供帳戶予他人使用之犯罪型態，可謂是詐欺案件之「衍生犯罪」，或可稱為「前置犯罪」行為。

### 2.3.2 我國網路詐欺類型、取款方式之實證研究

我國既未如美國有成立網路詐欺申訴中心，亦無如美國交易委員會、或經濟犯罪研究中心有對年度網路詐欺之類型、數據、被害人付款方式做任何之觀察、統計，致使無從瞭解我國實務上網路詐欺之真實現況。而詐欺罪為財產犯罪之一種，其構成要件除「施用詐術」外，最重要的就是「取得不法的財產或利益」，從前開文獻、實證研究及職司偵查犯罪之專業人員均咸認，詐欺集團利用人頭帳戶從事各種詐欺取款之手段，乃是導致查緝困難而致使詐騙案件氾濫成災的主因。然而，在我國學術、實務上均未有何實證數據可以說明：到底那幾種詐欺的態樣佔網路詐欺的大宗？詐欺案件中有多高的比例是使用人頭帳戶來取款？及人頭帳戶之氾濫，是否確實是詐欺案件無法繼續查緝之主因？因此，本文擬從網路詐欺原始資料（primary data）著手，先觀察統計網路詐欺之態樣、類型。再從詐欺行為人「取款」即被害人「付款」的面向來檢視，人頭帳戶與網路詐欺間的關連性之高低。

而在網路詐欺的原始資料方面，本文抽樣各檢調機關或人民告訴而移送至各地方法院檢察署之案件，進而統計網路詐欺之態樣與類型。資料分析之對象為全國各地檢察署的書類<sup>83</sup>，案件抽取之方式，係利用法務部部內網站之檢察書類查詢系統，以「網路

<sup>81</sup>章光明，第 11 章台灣人權，莫讓網路成為天堂路，2005 年台灣年鑑，

[http://www.gov.tw/EBOOKS/TWANNUAL/show\\_book.php?path=3\\_011\\_001](http://www.gov.tw/EBOOKS/TWANNUAL/show_book.php?path=3_011_001)，(2006/Mar/15)。

<sup>82</sup>賴添貴，「台灣地區經濟詐欺狀況處理與防制之實證研究」，大業大學事業經營系，碩士論文，第 54、127 頁，2005 年 2 月。

<sup>83</sup>在現行的刑事訴訟法制度中，檢察官為偵查之主體，故所有的案件，不論是警方的移送案件、告訴、告發案件，均會由地檢署的檢察官判斷其是否應起訴或是為其他處理，故地檢署的書類較警方的移送案件更為全面。其次，由於檢察官具有法律之專業及長時間的偵查訓練，故其書類之撰寫多經過一定

「&詐欺」、「網站&詐欺」、「網際網路&詐欺」三組關鍵字搜尋，搜尋期間設定為偵結日期 2005 年 1 月 1 日至同年 12 月 31 日之書類，包含起訴、緩起訴、不起訴處分等所有案件，再進一步過濾不符合網路詐欺類型之案件。

全部統計、分析的案件數目共為 924 件，而實證調查結果發現：網路詐欺案件中以網路拍賣詐欺、網路遊戲詐欺、網路色情詐欺及網路盜刷信用卡等四大類為大宗，故本文製作圖表說明網路詐欺之類型與比例，分別參見表 4、5。

表 4 網路詐欺類型之名稱、定義說明表

網路詐欺類型之名稱	網路詐欺類型之定義說明
網路拍賣詐欺	在拍賣網路中販賣物品 <sup>84</sup> 而導致之詐欺。
網路遊戲詐欺	與網路遊戲相關之詐欺案件。包含買賣寶物、遊戲帳號。
網路色情詐欺	在網路上偽稱可進行色情交易以進行詐欺
網路盜刷信用卡詐欺	在網路上盜刷他人之信用卡
其他網路詐欺	如：使用網路電話進行詐欺、木馬程式（以木馬程式或間諜軟體竊取帳戶或銀行密碼詐取款項）、假冒他人名義帳戶上網、網路上交友而進行詐欺等詐欺行為。

表 5 網路詐欺類型之件數、被害金額表

網路詐欺類型	件數	比例	總金額（元）	平均金額（元）
網路拍賣詐欺	465	50.32%	16,575,255	35,645.7
網路遊戲詐欺	303	32.79%	7,382,260	24,363.9
網路色情詐欺	78	8.44%	9,277,134	118,937.6
網路盜刷信用卡詐欺	35	3.79%	269,078	75,973.7
其他網路詐欺	43	4.65%	7,946,914	184,812
全部合計	924	100%	43,840,641	47,446.58

其中，由上表可知，網路拍賣所佔之比例約五成，與美國網路詐欺發展之趨勢相類。又都會區之網路拍賣詐欺佔網路詐欺之比例均較平均值為高，如士林為 59.26%、台北為 52.38%、台中為 63.3%、高雄為 62.7%<sup>85</sup>，這可能是在商業經濟越是發達之都

之思考，才會判斷其是否符合刑法某一個犯罪之構成要件，故若檢察官將之判斷該行為確實符合某一個構成要件，則其錯誤之可能性甚小。最後，檢察官之書類也會遵循構成要件而清楚說明，故在資料分析的時候，一方面不會因為書類內容不明而導致錯誤，更進而可以加快搜尋的速度。基於以上的幾個理由，本文嘗試從各檢調機關或人民告訴而移送至各地方法院檢察署之案件，統計網路詐欺之態樣與類型。

<sup>84</sup> 包含有體物或無體財產（如服務、IP），但不包含網路遊戲之相關寶物、天幣等。

<sup>85</sup> 統計一級地方法院檢察署之 2005 年度網路詐欺案件中網路拍賣比例：士林（59.26%）、台北（52.38%）、板橋（40.3%）、桃園（46.3%）、台中（63.3%）、彰化（34.7%）、台南（30.6%）、高雄（62.7%）。而全國地方法院檢察署 2005 年度案件網路拍賣佔全部網路詐欺案件為 50.32%。

市，網路拍賣等交易越是興盛，而網路詐欺之發生率亦隨之攀升。

另從詐欺行為人「取款」即被害人「付款」的角度觀察，人頭帳戶與網路詐欺間的關連性，而統計之結果如下表 6：

表 6 網路詐欺與人頭帳戶之關連比例表

網路詐欺案件	件數	件數百分比	金額（元）	金額百分比
全部	924	100%	43,840,641	100%
以轉帳方式付款	833	90.15%	19,780,532	45.6%
以人頭帳戶取款	612	66.23%	34,153,014	78.7%

本文從統計發現國人在網路上消費購物付款之習慣仍與美國不同。上開統計網路詐欺案件 924 件中，有 833 件是利用轉帳匯款詐欺之案件，佔全部網路詐欺之 90.15%<sup>86</sup>。另外，值得注意的現象為，網路詐欺案件中施詐行為人使用人頭帳戶之比例偏高，共計 612 件，佔全體網路詐欺 924 件中之 66.23%，佔轉帳匯款詐欺件數 833 件之 73.47%，此為美國網路詐欺中所罕見。

從以上實證統計分析可證明，人頭帳戶與網路詐欺間有相當高程度的密切關連性，而人頭帳戶之猖獗可謂我國之特殊現象，且確實造成查緝上之嚴重困難。故若能從查緝販賣人頭帳戶之犯罪或從此人頭帳戶角度思考，來降低、遏止詐欺集團取得人頭帳戶之來源，並藉此提高詐欺集團之犯罪成本，應能降低詐欺案件之犯罪量。因此，本文實證之研究命題為：「查緝人頭帳戶之犯罪或從人頭帳戶角度來制定防制犯罪策略，均應能有效地降低網路詐欺犯罪之案件數。」

### 2.3.3 我國使用人頭帳戶之詐欺防制現況

內政部警政署刑事警察局為因應新興詐欺及經濟犯罪日益猖獗，於 1998 年 7 月 1 日以任務編組方式成立經濟犯罪專責隊，即目前刑事局之偵查第 7 隊，並於 2001 年正式將該單位納入編制，負責偵辦新興之詐欺案件。而現行警調機關因深知新型態詐欺大量運用人頭帳戶、人頭電話犯案，導致偵辦案件之難度，故為有效遏止詐欺犯罪，刑事警察局提專案報告，由行政院院長裁示委由許政務委員召集成立「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，並邀集內政部、財政部、交通部、法務部、教育局、新聞局、陸委會、檢警調等機關首長召開「反詐騙跨部會協調會議」達成防制詐欺之共識，而其中從防制人頭帳戶方面之防制詐欺之重大措施，包括：設立警示帳戶通報機制、調降金融機構金融卡非約定轉帳金額上限<sup>87</sup>。又洗錢防制法於 2003 年 2 月 6 日修正公布，並於同年 8 月 6 日施行，將掩飾「他人」重大犯罪所得財物或財產上利益之洗錢態樣，特別移列到同條第 2 款，並提高刑罰為「處七年以下有期徒刑，得併科新臺幣五百萬元以下罰金」。而提供帳戶予他人，即為掩飾他人重大犯

<sup>86</sup>我國網路詐欺中交付現金之方式只有轉帳匯款及面交二種，而在本文統計 2005 年度結案全地檢署之案件共 924 件中，有 833 件轉帳匯款，僅有 1 件是面交，其餘受害者交付的是財產上之不法利益：如網路遊戲中之虛擬寶物。

<sup>87</sup>同前揭註 82，第 51 頁。另參江志慶，「ATM 轉帳詐欺犯罪之實證研究」，中央警察大學犯罪防治系，碩士論文，第 30 頁，2005 年。

罪所得財物之行為，本質上已含有幫助他人洗錢之性質（提供人頭帳戶之行為，是否該當洗錢罪，實務上有不同看法，此部分留待第三章詳述）。此次修法將此種提供人頭帳戶之幫助犯性質之犯罪，提升為正犯之性質來處罰，並且提高法定刑，顯係藉由提高刑罰之手段，來遏止人頭帳戶之氾濫。

簡言之，即「警示帳戶通報機制」、「非約定轉帳限制」及「提高洗錢防制法第 9 條刑度」等手段，應為查緝人頭帳戶之犯罪或從人頭帳戶角度來制定之犯罪策略。從而，本文以下研究之重點為，此三種防制詐欺之策略是否對「網路詐欺」類型之犯罪有降低犯罪量之成效。而取採分析之方式，先從法律面探討適法性及相關法律問題，繼之則從實證方面檢驗犯罪防制策略之成效，並進行數據分析及法律經濟面之說明。



### 三、 從法律面探討犯罪防制策略之適法性

我國從防制人頭帳戶角度防制詐欺之方式可分為金融機構方面之「警示帳戶通報機制」、「非約定轉帳限制」；及「提高洗錢防制法第9條刑度」之法律刑罰二方面。而在探討防制策略成效前先予探討法律層面之相關問題，以下分節說明之。

#### 3.1 警示帳戶通報機制

##### 3.1.1 警示帳戶之定義與由來

詐騙金額動輒新台幣上千萬的詐騙案，近年已成為危害最烈的犯罪型態，由於詐騙集團多以「人頭帳戶」為犯罪工具，為有效遏止人頭帳戶被犯罪集團所利用，行政院於2003年之強化社會治安第16次專案會議決議，請金融主管機關協商警察、調查等相關單位建立「警示通報機制」，並研議就被疑似犯罪之帳戶，終止客戶使用金融卡條款之契約內容<sup>88</sup>。財政部金融局（現改隸為行政院金融監督管理委員會銀行局，以下簡稱行政院金管會銀行局）旋依據前開行政院強化社會治安會議之決意，與內政部警政署等單位共同研商建立「警示通報機制」，即警調機關通知金融機構將可疑之帳戶列為「警示帳戶」後，金融機構則終止該帳戶之提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳功能，使歹徒在金融機構接獲通知後，無法利用自動提款機提領「警示帳戶」內之款項，以求能即時防止可疑帳戶資金之加速流動，進而減低受害人之金錢損失。故在警調單位於2003年7月正式建制、啟用建置「人頭帳戶資料庫」之始，所謂之警示帳戶係指：「警調機關接獲民眾詐財報案，為查緝利用人頭帳戶進行詐騙等犯罪之案件，依警示通報機制，請金融機構列為警示帳戶後，金融機構則終止該帳號使用提款卡、語音轉帳、網路轉帳及其他電子支付轉帳功能<sup>89</sup>。」

然而，2006年4月27日行政院金管會銀行局，依據銀行法第45條之2第3項之授權訂定之「銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法（以下簡稱異常帳戶管理辦法，管理辦法全文見附錄一）」第3條第1項明訂「警示帳戶」是指「法院、檢察署或司法警察機關為偵辦刑事案件需要，通報銀行將存款列為警示者。」，且依該管理辦法第5條第2點明訂警示帳戶之法律效果：「存款帳戶經通報為警示帳戶者，應即通知金融聯合徵信中心，並暫停該帳戶全部交易功能，匯入款項逕以退匯方式退回匯款行」。

此外，「異常帳戶管理辦法」亦明訂，一人持有多個金融機構存款帳戶，其中一帳戶經通報為警示帳戶，其餘帳戶即是管理辦法所稱之「衍生管制帳戶」。依該辦法第3條之定義，「衍生管制帳戶」，是指警示帳戶之開戶人所開戶之其他存款帳戶。而金融機構擷取或收到金融聯合徵信之「警示帳戶」通報資料後，應即時查證比對金融機構所有分支單位是否有同一開戶名義人之「衍生管制帳戶」，若發現有存款帳戶屬「衍生管制帳戶」者，依辦法第5條之內容，應即「暫停該帳戶使用提款卡、語音轉帳、網

<sup>88</sup>建立警示通報機制及訂定終止客戶使用金融卡之契約條款，行政院監督管理委員會網站發佈之新聞稿，參網站 <http://www.fscey.gov.tw/ct.asp?xItem=28503&ctNode=17&mp=2>，(2006/Mar/5)

<sup>89</sup>廉政電子報，<http://www.tcmvd.gov.tw/d9k/main/>，(2006/Feb/27)。

路轉帳及其他電子支付功能」，且必須將「匯入款項逕以退匯方式退回匯款行」<sup>90</sup>。

簡言之，即在 2006 年 4 月 27 日前之警示帳戶，金融機構僅片面終止臨櫃提領以外之功能，而在「異常帳戶管理辦法」發布後，將警示帳戶之限制措施擴大為「暫停該帳戶全部交易功能」，此即「凍結」帳戶之法律效果<sup>91</sup>。尤有甚者，該管理辦法另創設所謂「衍生管制帳戶」，被列為「衍生管制帳戶」之法律效果，則與「異常帳戶管理辦法」發布前之警示帳戶相同。再者，不論是「警示帳戶」或是「衍生管制帳戶」內之款項，均不待當事人之請求或法院之判決，即由金融機構「以退匯方式退回匯款行」之方式返還給匯款之當事人。

### 3.1.2 設置警示帳戶之作業規定及處理程序

內政部刑事警察局偵 7 隊暨各市、縣（市）警察局刑警（大）隊於 2003 年 7 月 4 日起成立「人頭帳戶、電話犯罪案件專責處理、偵辦窗口」，各警察分局亦自 2004 年 1 月 5 日起成立專責窗口，並分別於 2003 年 7 月 16 日及 2004 年 1 月 1 日正式啟用「人頭資料庫」，提供各警察機關、民眾查詢及整合各種詐騙人頭資訊，以有效斷絕詐騙集團所使用之犯罪及吸金工具。依據 2005 年 3 月 1 日修正之「金融電信人頭帳戶及電話犯罪案件處理執行要點」（參附錄二）<sup>92</sup>可知，將可疑帳戶列為警示帳戶之作業流程說明如下，另流程圖表（見圖 4）：

一、各轄區內之分駐（派出）所之處理情形：分駐所受理報案後，先作初步查證，經查證屬實後：

1. 填報「詐欺帳戶通報警示、詐騙電話斷話簡便格式表」（參附錄三）、「報案三聯單」傳真至人頭帳戶開戶金融機構通報警示。
2. 再將前項簡便格式表及相關報案（筆錄、三聯單、通報單等）、檢舉告發資料陳送分局辦理。
3. 又依網路詐欺案件之特殊性規定，於執行時應注意：有關網路購物、拍賣疑有交易糾紛之案件，應先行查證釐清，確屬以人頭帳戶作為詐財工具，以隱瞞真實身份，防止司法機關追查之情形，方可列為警示帳戶。如係交易糾紛案件，不得列為警示帳戶，可請被害人循民事求償程序辦理，以維雙方權益。（第 5 點第 2 項）

二、分局刑事組應辦理事項：

1. 審核分駐所陳報之資料。
2. 3 日內製作正式公文函發金融機構將帳戶列為警示帳戶（終止人頭帳號使用提款卡、語音轉帳、網路轉帳、其他電子支付轉帳），並向金融機構調閱開戶人基本資料，另通知警察局專責組追蹤、列管。
3. 將人頭帳戶開戶資料、被害人基本資料、轉帳明細等輸入人頭資料庫及相關刑案系統。

<sup>90</sup> 衍生管制帳戶是參酌行政院金融監督管理委員會 2005 年 8 月 16 日金管銀（一）字第 0948011044 號函之附件「一人有多個金融機構存款帳戶，其中一帳戶經通報為警示帳戶，其餘帳戶之通報及控管作業程序」所訂。

<sup>91</sup> 依洗錢防制法第 8 條之 1，檢察官、法官得依法凍結帳戶，使帳戶內之金錢完全無法提領。

<sup>92</sup> 該執行規定是依照 2003 年 7 月 7 日行政院強化治安第 19 字專案會議院長裁定事項辦理。

4. 依據內政部警政署 93 年 9 月 15 日警署刑偵字第 0930136441-A 號函規定，要求各警察機關於受理報案後，應儘速查明該帳戶是否屬遭偽造、變造或冒名開立，並函復金融機構，據以辦理警示帳戶內款項發還事宜。
5. 再依內政部警政署 94 年 1 月 27 日警署刑偵字第 0940006418 號之函文：要求各單位受理查證可疑帳戶確屬遭詐騙集團持偽造或變造證件冒名申請者，應即函請設置警示帳戶之金融機構准許被冒名者重新開戶，惟該遭冒名之帳戶仍應持續列管警示。

2006 年 4 月 27 日「異常帳戶管理辦法」發布前，均是由司法警察機關將初步查證為可疑帳戶之情形通報金融機構將帳戶列為「警示帳戶」，即由警調機關擔負判定帳戶是否「疑似不法或顯屬異常交易之帳戶」。然而，前開辦法訂定公布後，金融機構得依據管理辦法第 4 條第 3 類「疑似不法或顯屬異常交易帳戶」之認定標準，自行將可疑帳戶依銀行法第 45 條之 2 第 2 項規定，暫停存入或提領、匯出款項。



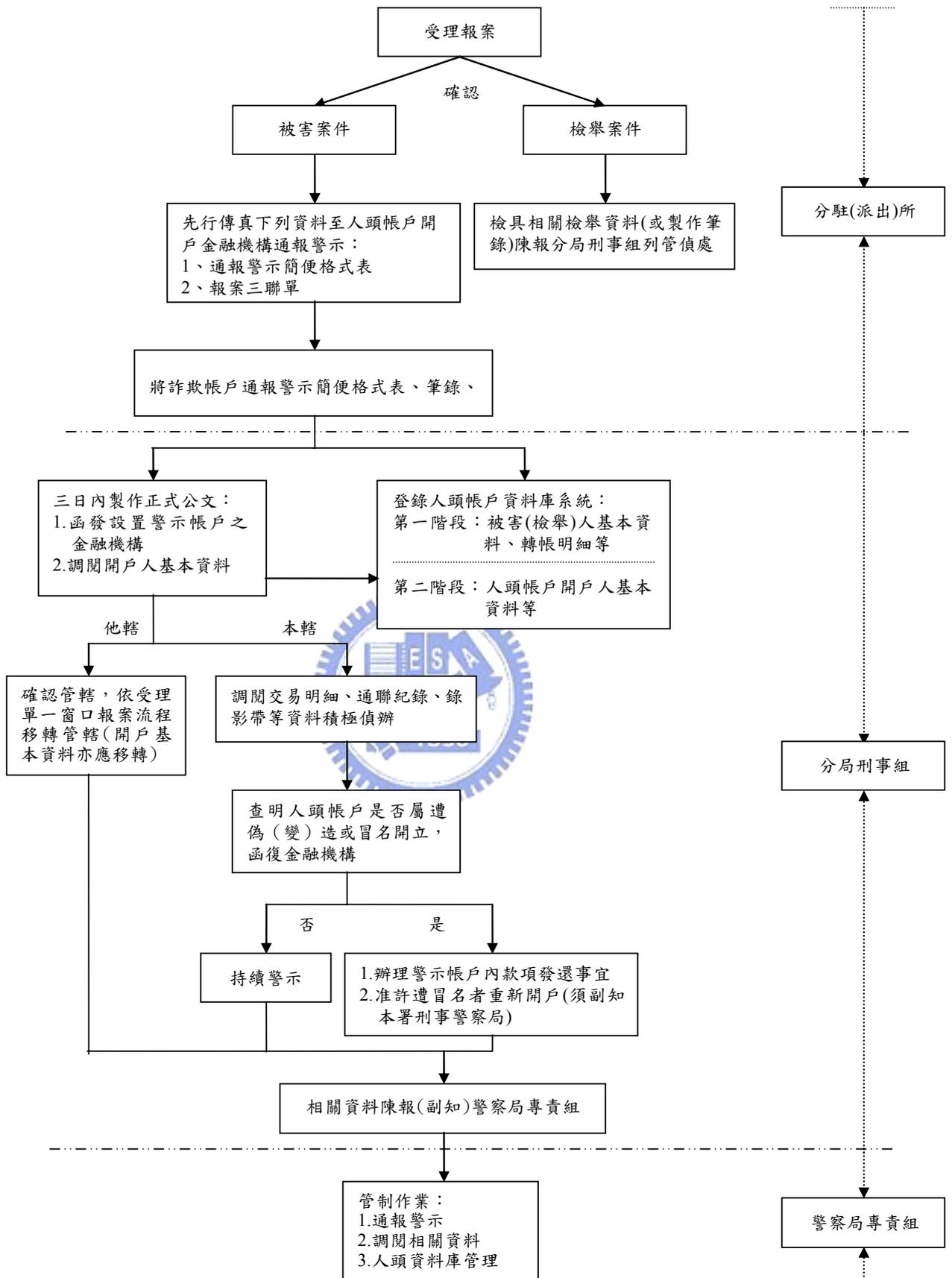


圖 4 警察機關受理詐欺案件通報(解除)警示帳戶流程圖  
(資料來源：內政部警政署刑事局)

### 3.1.3 警示帳戶之法律性質

在討論警示帳戶之性質前，需先探究金融機構與存戶間之法律關係為何。人民向金融機構申請設立活期存款帳戶，需填具「存款存摺約定書」之契約，該契約內容約定，以金融機構所簽發之存摺作為記載存款帳戶收付之憑證，而得隨時辦理提存款項之活期性存款。惟各金融機構為加強服務存戶，提供存戶得電話自動語音、網路銀行、EDI 電子轉帳、行動銀行，及利用「(晶片)金融卡」至各金融機構設置之自動臨櫃機(ATM)取款等服務，而此等之服務，於存戶申請開戶時，得視個人需要填具相關約定書向金融機構申請之。按銀行法第 7 條規定：「本法稱活期存款，為存款人憑存摺或依約定方式隨時提取之存款」，活期存款與活期儲蓄存款之提款方式，以存摺為之，統稱為存摺存款<sup>93</sup>，而存款戶與金融機構間訂立之「存款存摺約定書」之契約，應屬民法第 603 條之金錢消費寄託契約。又若存戶於申請開戶時，另外向銀行申請利用提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳功能等服務，應屬委任契約。是以，存戶與金融機構訂立開戶之契約後，金融機構即應依契約約定內容提供服務，即受任之金融機構原則上不得變更存戶之指示，民法第 536 條定有明文<sup>94</sup>，合先敘明。

警調機關為查緝詐欺等犯罪案件，依警示通報機制，請金融機構將可疑帳戶列為警示帳戶後，金融機關則片面終止該帳戶使用提款卡、語音轉帳、網路轉帳及其他電子支付轉帳功能，惟仍能臨櫃提領<sup>95</sup>，但是，在 2006 年 4 月 27 日「異常帳戶管理辦法」發布後之警示帳戶，金融機構依該辦法則是凍結該帳戶，即暫停帳戶全部交易功能。易言之，即不論是在「異常帳戶管理辦法」訂定前後，均是由警察機關審核認定是否為應警示之帳戶，所不同的是，金融機構依警調之通知，將帳戶列為警示帳戶後，在「異常帳戶管理辦法」發布前，金融機構片面終止委任契約之內容，並拒絕提供存戶得利用提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳功能等服務，惟原存戶與金融機構間之金錢消費寄託契約並未因之受影響，故存戶仍得為臨櫃提領之行為；然而在 2006 年 4 月 27 日後，被列為警示之帳戶，金融機構全面終止與存戶間之所有契約，包括「金錢消費寄託契約」及「委任契約」。然而，在「異常帳戶管理辦法」發布前金融機構之片面終止提供存戶使用提款卡、語音轉帳、網路轉帳及其他電子支付轉帳功能之委任契約，是否於法有據？及在「異常帳戶管理辦法」發布後「警示帳戶」及「衍生管制帳戶」之法律性質，本文將繼續討論之。

### 3.1.4 2006 年 4 月 27 日「異常帳戶管理辦法」發布前「警示帳戶」之適法性

#### 一、「警示帳戶」之法源依據為何？

按民法第 549 條第 1 項固明定：「當事人之任何一方得隨時終止委任契約，惟終止委任契約，應向他方當事人以意思表示為之。非對話而為意思表示者，其意思表示，以通知達到相對人時，發生效力，民法第 549 條第 1 項、第 236 條、第

<sup>93</sup>第三章存款存摺實務，<http://www.boaf.gov.tw/site/boaf/public/Attachment/52210233371.doc>，(2006/Mar/5)。

<sup>94</sup>民法第 536 條規定：「受任人非有急迫情事，並可推定委任人若之有此情事亦允許變更其指示者，不得變更委任人之指示。」

<sup>95</sup>「國內經濟金融日誌」，中央銀行季刊，第 27 期卷第 2 期，2005 年 4 月份。

258 條第 1 項、第 95 條第 1 項前段定有明文。故委任契約當事人之一方，向他方表示終止委任契約者，在終止契約之意思表示達到對方（非對話）使對方了解前，委任關係仍然存在<sup>96</sup>。故金融機構雖得隨時終止委任契約，然在終止契約之意思表示未到達契約之他方即存戶時，委任契約仍繼續有效存在。而金融機構依據警調單位之通知，將疑似帳戶列為警示帳戶後，在未通知帳戶使用人將終止委任契約之情況下，即先終止提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳功能等服務，則仍違法。

又財政部於 2002 年 11 月 11 日以台財融(一)第 0910047349 號函示各金機構：請銀行於活期性存款開戶約定書中增訂（包括金融卡、語音轉帳、網路轉帳申請約定書中增訂）「如經貴行研判帳戶有疑似不當使用之情事時，貴行得逕自終止客戶使用提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳，提款卡並得收回作廢。」，則倘於存戶申請開戶時，在「存款存摺約定書」之契約已為上開終止權之約定時<sup>97</sup>，則金融機構依警調機關認定，並將可疑帳戶列為警示帳戶後，依該契約約定內容，似得在未通知存戶的情形下，片面終止提供存戶使用提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳之委任契約。準此，則此終止權行使之約定，應為金融機構片面終止存戶委任契約內容之護身符。

然而，仍有疑問之處在於，若存戶於申請開戶時，契約中並未載明「如經貴行研判帳戶有疑似不當使用之情事時，貴行得逕自終止客戶使用提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳，提款卡並得收回作廢。」終止權行使之約定條款，或是於 2002 年 11 月 11 日以前業已申請開戶之存戶，則金融機構在未通知存戶前提下，逕自片面終止提供存戶使用提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳等功能，仍無法源依據，實有違法之情事。

按洗錢防治法第 8 條之 1 第 1 項之規定：「檢察官於偵查中，有事實足認被告利用帳戶、匯款、通貨或其他支付工具從事洗錢者，得聲請該管法院指定六個月以內之期間，對該筆洗錢交易之財產為禁止提款、轉帳、付款、交付、轉讓或其他相關處分之命令。其情況急迫，有相當理由足認非立即為上開命令，不能保全得沒收之財產或證據者，檢察官得逕命執行之。但應於執行後三日內，報請法院補發命令。法院如不於三日內補發時，應即停止執行。」、「前項禁止提款、轉帳、付款、交付、轉讓或其他相關處分之命令，法官於審判中得依職權為之。」、「前

<sup>96</sup> 司法院高等法院 84 年度台抗字第 257 號判決：按當事人之任何一方得隨時終止委任契約。終止委任契約，應向他方當事人以意思表示為之。非對話而為意思表示者，其意思表示，以通知達到相對人時，發生效力，民法第五百四十九條第一項、第二百六十三條、第二百五十八條第一項、第九十五條第一項前段定有明文。又委任關係消滅之事由，係由當事人之一方發生者，於他方知其事由，或可得而知其事由前，委任關係視為存續，民法第五百五十二條亦定有明文。故委任契約當事人之一方，向他方表示終止委任契約者，在終止契約之意思表示達到對方（非對話）使對方了解前，委任關係仍然存在。  
<sup>97</sup> 目前金融機構之契約條款多有加註：『立約人填寫資料不實或（及）使用偽變造之文件資料，經本公司研判相關帳戶有疑似不當使用之情事，或本公司經財團法人金融徵信中心通報於其他金融機構之存款帳戶已遭設定為警示帳戶時，本公司得逕予將本帳戶設定為警示帳戶，除停止網路轉帳其其他電子支付服務外，金融卡及語音轉帳亦停止使用，並得將金融卡及其他電子交易憑證收回作廢或結清帳戶。但經本公司查證後判斷為正常客戶時，將路腹帳戶之各項正常交易功能』，參中華郵政網路郵局服務約定書，[http://download.post.gov.tw/post/intranet/DL\\_SERVER/P98044092.doc](http://download.post.gov.tw/post/intranet/DL_SERVER/P98044092.doc)，（2006/Mar/5）。

二項命令，應以書面為之、。惟若是依照洗錢防制法規定凍結之帳戶，則該帳戶內之金錢完全無法提領，顯與上開警示帳戶之限制僅能臨櫃交易不同。又依照警示通報機制，被各金融機構列為「警示帳戶」之帳戶，並非經由檢察官或法官所為命令後之處分結果，即該警示帳戶並非等同於司法機關依照洗錢防制法相關規定所為之帳戶凍結。是故洗錢防制法第 8 條之 1 之規定，亦非上開警示帳戶之法源依據。

再按銀行法第 48 條第 1 項、郵政儲金匯兌法第 11 條<sup>98</sup>規定：「銀行非依法院之裁判或其他法律之規定，不得接受第三人有關停止給付存款或匯款、扣留擔保物或保管物或其他類似之請求」、「中華郵政公司非依法院之裁判或檢察機關之書面通知或其他法律之規定，不得接受第三人有關停止帳戶交易活動或給付匯款之請求」，故在未經法院裁判或無法律依據之情況下，對第三人請求凍結帳戶或停止帳戶部分交易功能，金融機構是應予婉拒的。換言之，行政機關在無法律依據或授權下，不得要求金融機構片面終止其與帳戶使用人間之契約約定，此即依法行政原則下「法律保留」<sup>99</sup>原則之重申。然而，2006 年 4 月 27 日「異常帳戶管理辦法」發布前之警示通報機制，警調機關要求金融機構將可疑帳戶終止客戶使用提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳功能，如前所述，既無法律規定，亦無法律之授權，然各金融機構卻接受警調機關之請求，實有違反銀行法、郵政儲金匯兌法之相關現行規定。

財政部、行政院金管會銀行局及各金融機構均明知前開警示帳戶並無明確法源依據，且實務執行上之結果確有違法之虞，故財政部及行政院金管會銀行局力倡修改銀行法並增定警示帳戶之法源依據。而立法院始於 2005 年 5 月 18 日修正公布銀行法，其中第 45 條之 2 第 2 項、第 3 項雖有規定：「銀行存款帳戶應負擔善良管理人責任。對於疑似不法或顯屬異常交易之存款帳戶，得予暫停存入或提領、匯出款項」、「前項疑似不法或顯屬異常交易帳戶之認定標準，及暫停帳戶之作業程序及辦法，由主管機關定之。」，此應為銀行限制警示之帳戶部分或全部交易功能之法源依據。但是，該規定方於 2005 年 5 月 18 日修正公布，然警示帳戶之設置與作業早於 2003 年間起實施，則修法前之法源依據仍付之闕如。何況，行政院金管會銀行局依前開銀行法第 45 條之 2 第 3 項授權訂定之「異常帳戶管理辦法」，遲至 2006 年 4 月 27 日始公布<sup>100</sup>，且該管理辦法亦無回溯既往適用之規定。

<sup>98</sup> 郵政儲金匯兌法於 2002 年 6 月 11 日立法通過，見 <http://lis.ly.gov.tw/npl/fast/02077/910611.htm>，(2006/Mar/10)。

<sup>99</sup> 行政機關必須依法行政，依法行政原則乃支一切行政行為必須遵守之首要原則，而依法行政之兩項要素：法律優位與法律保留，旨在維持法律之規範效力，避免行政行為侵越立法機關之權限。「法律優位」原則，乃為行政行為或其他一切行政活動，均不得與法律相抵觸，惟並不要求一切行政活動均有法律之明文依據，只需消極不違背法律之規定即可，故稱之為消極的依法行政。然而憲法已將某些事項保留予立法機關，需由立法機關以法律加以定，此即「法律保留」原則，即行政機關在干涉人民生命、自由、財產等時，不能以消極不抵觸法律為已足，尚須有法律明文依據或法律授權之命令，始得為行政處分或其他措施，否則合法性即生問題。又我國憲法第 23 條、中央法規標準法第 5 條第 2 款均為法律保留原則之實踐。參吳庚，行政法之理論與實務，增訂 4 版，第 77、83、88、92 頁，自版，1998 年。

<sup>100</sup> 2006 年 4 月 27 日行政院監督管理委員會以金管銀（一）字第 09510001640 號令公布。

換言之，在此之前，金融機構依「警示帳戶通報機制」所列之「警示帳戶」，還是有違背法律之不當。加之，台北地方法院一判決見解，也明白指出金融機構依照財政部金管會銀行局之函令片面終止存戶臨櫃提領以外之交易功能，確屬違法<sup>101</sup>。

## 二、行政院金管會銀行局函文指示金融機構實施警示帳戶機制之法律性質

金融機構之存戶於申請開戶時，在「存款存摺約定書」之契約書內，並未載明「如經貴行研判帳戶有疑似不當使用之情事時，貴行得逕自終止客戶使用提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳，提款卡並得收回作廢。」之終止權行使條款，則金融機構依行政院金管會銀行局之函令指示列為警示帳戶，並終止與存戶間部分契約之效力，則該金融監督管理委員會銀行局之函文指示行為之法律性質為何，殊值探討。

按行政程序法第 92 條第 1 項規定之行政處分，係指行政機關就公法上具體事件所為之決定或其他公權力措施，而對外直接發生法律效果之單方行政行為。金管會銀行局固先於 2005 年 4 月 19 日向各金融機構宣布，自願性人頭戶一旦被列為警示帳戶，該帳戶所有人名下所有帳戶均限制只能臨櫃交易。再於 2005 年 9 月 12 日以金管銀（一）字第 0941000693 號函各金融機關：「、、、（二）為加速偵辦案件，重申金融機構應落實『警示帳戶』通報機制，加強『警示帳戶』作業聯絡窗口緊急處理功能，除正常營業時間外，於假日及夜間仍可緊急處理，俾利檢警調單位之查緝。」。惟實際上對帳戶使用人而言，是各金融機構依警調機關認定為應警示之帳戶後，由各金融機構終止臨櫃交易以外之帳戶使用行為，並非金管會銀行局之前揭函令，直接對各金融機構及帳戶使用人發生終止「存款存摺約定書」中之委任契約，從而，金管會銀行局在其職權範圍內，為實現其與內政部警政署協商共同建立之「警示帳戶之通報機制」，而為前揭函示，促請各金融機構將可疑帳戶列為「警示帳戶」後，即應立刻終止該帳戶使用提款卡、語音轉帳、網路轉帳及其他電子支付之轉帳等功能。換言之，即金管會銀行局之行政機關，所為函令指示之單方行政行為，並未直接對外發生法律效果，即此種行政行為，並非屬於行政程序法第 92 條第 1 項之行政處分，應無疑問。

又金管會銀行局對各金融機構之指示，並非行政處分，已如前述，則是否屬於行政法上之行政指導，仍值得繼續探究。而所謂「行政指導」，是指行政機關在其職權或所掌事務範圍內，為實現一定之行政目的，以輔導、協助、勸告、建議或其他不具法律上強制力之方法，促請特定人為一定作為或不作為之行為。而行政指導之概念是源自於日本行政法<sup>102</sup>，相當於德國行政法學所稱之「非正式行政行為」，我國於 1999 年制定行政程序法時已立法明定，將行政指導之一般規定予以法制化，有行政程序法第 165 條可參。行政指導之特性在於行政機關關係不用法

<sup>101</sup> 蘇位榮，凍結警示帳戶法官認違法，聯合報，A9 社會話題版，2006 年 3 月 8 日。

<sup>102</sup> 行政指導「因屬於非權利的，非拘束的行政手段，即使在法律未完備的情路下，亦可以『行政規範外』之措施，對於新的行政上之需要，迅速並柔軟地加以因應。而且由於係依照對方的意願而進行合作，相較於權力性質的行政手段，反而圓滿達成一定的社會作用的情況頗多」。參見，佐藤英善，「經濟行政法」，1990 年 6 月，第 943 頁，轉引自，李傑清，「我國洗錢防制法『確認身份』規定之研究—與日本『本人確認法』比較之觀點」，九十二年洗錢防制工作年報，第 56 頁以下，法務部調查局，2004 年 4 月。

律之強制力，而以輔導、協助、勸告、建議或其他不具法律上強制力之方法，促請相對人注意一定作為或不作為。現行法制上有很多立法例是以行政指導之方式進行<sup>103</sup>，由於行政指導係以不具法律上強制力之方法，用輔導、協助、勸告、建議等方式，促請相對人履行一定作為或不作為之行為，以達成行政目的。因此，行政指導具有以下之特質：

- (一) 行政指導本身是事實行為：行政指導不是法律行為，因此，行政指導不會對於相對人產生一定法律上之效果，所以，行政程序法第 165 條規定：「本法所稱行政指導、促請特定人為一定作為或不作為之行為。」，另同法第 166 條第 2 項規定：「相對人明確拒絕指導時，行政機關應即停止，並不得據此對相對人為不利之處置。」。依上開規定，行政指導重點在於「促請」履行一定作為或不作為，但該相對人縱使不履行亦並不致於會立即產生一定之法律效果；此與行政處分於送達後會對當事人發生直接之法律上效果，大不相同。
- (二) 行政指導是一種單方行政行為：行政指導係由行政機關以輔導、協助、勸告、建議等方式，促請相對人履行一定作為或不作為之行為，所以不必有相對人相互對立之意思表示，只須以機關之單方行為即可成立。
- (三) 行政指導之特定性：依行政程序法第 165 條規定：「本法所稱行政指導……促請特定人為一定作為或不作為之行為。」依上開規定，行政指導必須明確對於特定人促請其履行一定作為或不作為之行為，但所謂「特定人」，在解釋上應包括於一定範圍內可得特定之行為人在內。
- (四) 行政指導之任意性：行政指導除具有事實性、單方性、特定性之性質外，另外一個最重要之特性就是任意性，也就是行政指導本質上並不具有一定之法律效果，而是以輔導、協助、勸告、建議或其他不具法律上強制力之方法，促請特定人履行一定作為或不作為之行為，所以行政指導是一種非權力之行政行為，德國行政法學則稱為「非正式行政行為」。因此，相對人如不履行行政指導上一定之作為或不作為內容，並不會被課以行政罰或受行政執行或其他不利之處分。

而金管會銀行局對各金融機構為前揭函文內容之指示，實際上比較像是利用不具法律強制力之指導方式，促請各金融機構為一定之作為或不作為。又參以金

<sup>103</sup> 司法院組織法第 15 條之 1 第 4 款規定：「少年及家事廳掌理左列事項：四、關於兒童及少年保護事件執行業務之規劃、指導、監督事項。」，少年事件處理法第 52 條第 1 項規定：「對於少年之交付安置輔導及施以感化教育時，由少年法院依其行為性質、身心狀況、學業程度及其他必要事項，分類交付適當之福利、教養機構或感化教育機構執行之，受少年法院之指導」，土地所有權人辦理農村社區土地重劃辦法第 5 條第 4 款規定：「籌備會之任務如下：四、向有關機關申請提供地籍資料及技術指導。」，內政部消防署辦事細則第 12 條第 4 款規定：「民力運用組職掌如下：四、鳳凰志工、社區婦女防火宣導隊及社區睦鄰救援隊之規劃、編組、訓練、管理、指導、福利及協調等事項。」另外消防法第五條規定：「直轄市、縣（市）政府，應舉辦防火教育及宣導，並由機關、學校、團體及大眾傳播機構協助推行。」，依上開規定司法機關對於少年之輔導，地政機關對於土地所有權人辦理農村社區土地重劃之技術指導，消防機關對於鳳凰志工、社區婦女防火宣導隊及社區睦鄰救援隊之防災、救護、火災預防之指導，以至於直轄市、縣（市）政府，每年定期舉辦之防火教育及宣導都是行政程序法第 165 條之行政指導。參見劉克正，行政指導（一）、（二）、（三），內政部消防署消防影音新聞台，<http://enews.nfa.gov.tw/one-news.asp?NewsNo=5352>，(2006/Mar/5)。

融監督管理委員會亦認定：「94年4月15日金管銀（二）字第0942000227號函銀行公會轉知所屬會員機構於自94年6月1日起實施『金融卡非約定轉帳單日限額調降為3萬元』措施，係一種『行政指導』」<sup>104</sup>。從而，金管會銀行局亦以函文指導之方式，促請金融機構確實落實「警示通報機制」，依照警調認定為可疑帳戶者，應列為警示帳戶並限制僅能臨櫃交易，此種單方行政行為，應亦認定是行政指導之一種，方屬合理。

從上可知，行政院金管會銀行局係利用函令透過銀行公會要求各銀行等金融機構約束各金融機構實行「警示帳戶」之機制，而目前銀行公會只要主管機關有何指示，就遵照辦理，從而，金融監督管理委員會銀行局之函令，實乃主管機關規避依法行政的白手套，換言之，即金管會銀行局明知「警示帳戶」並無法可據，若逕由其限制警示帳戶之使用人權利，實有違法行政處分之虞，而以此迂迴方式函令各金融機構，由各金融機構擔負違法之風險，實有立法怠惰及行政獨裁之不恰當。

### 3.1.5 「異常帳戶管理辦法」發布後「警示帳戶」之法律性質

依照銀行法第45條之2第2項、「異常帳戶管理辦法」，是由「法院、檢察署或司法警察機關」通報銀行將帳戶列為警示，而此「疑似不法或顯屬異常交易存款帳戶」之認定機關，係屬「法院、檢察署或司法警察機關」而非金融機構。目前在現行警示通報機制運作下，警示帳戶之通報多為司法警察機關，即各縣市政府警察局之分駐（派出）所接受人民詐騙等報案，先初步查證認定為「人頭帳戶」後，即先行以傳真簡便格式表之方式通知「人頭帳戶」所屬之金融機構，請金融機構將該帳戶列為警示帳戶，正式公文則由各縣市政府警察局之分局刑事組於三日內後補。金融機構一旦將通報之可疑帳戶列為「警示帳戶」後，直接對該存款帳戶人發生之法律效果有二：第一，該警示帳戶本身之帳戶全部交易功能被終止。第二，該警示帳戶之名義申請人其餘金融機構之所有存款帳戶（即衍生管制帳戶）會被限制僅能臨櫃提領。而此法律效果乃使存戶與銀行間之「金錢消費寄託契約」、「委任契約」全部或部分終止。從而，衍生一個值得思考之問題，若是由「法院、檢察署或司法警察機關」以書面通報銀行將可疑帳戶列為警示，則此書面之通知，是否屬於行政處分？有若是行政處分，是否有法源之依據？

一、「法院、檢察署或司法警察機關」通報銀行將帳戶列為警示之書面通告是否為行政處分？

按行政處分，係指行政機關就公法上具體事件所為之決定或其他公權力措施，而對外直接發生法律效果之單方行政行為，行政程序法第92條第1項定有明文。而通報銀行警示帳戶之書面通知是否符合行政處分之定義，有以下二個爭議要解決：

#### 1. 通報之主體是否符合行政機關之資格？

司法警察機關本屬行政機關之範疇並無疑問。然而，若檢察署、法院處理

<sup>104</sup> 行政院金融監督管理委員會銀行局之行政資訊目錄（9404），[http://www.fscey.gov.tw/lp\\_search.asp](http://www.fscey.gov.tw/lp_search.asp)，（2006/Mar/5）。

「偵查、審判」以外之業務，則仍屬實質意義之行政<sup>105</sup>，故檢察署、法院為書面通知警示人頭帳戶之主體時，亦應屬廣義之「行政機關」。

## 2. 通報之機關發出書面通知給金融機構後，是否已經對外發生法律效果？

當金融機構收到此份書面通知時，原則上應是以此書面通知做為將帳戶列為警示之依據，換言之，即不論在「異常帳戶管理辦法」發布前警示帳戶機制實際運作之情形，抑或是從發布之管理辦法內容以觀，金融機構均會依據通報機關之認定，而將帳戶警示並將帳戶交易功能全部或部分停止，似無拒絕或予以變更之權利。從而，我們可以說，當通報之機關發出書面通知給金融機構後，因為金融機關會逕依該通報將帳戶警示，故當金融機構收到此書面通知後，即會變更金融機構與該特定存戶間之契約關係，即此書面通知所產生之法律效果，乃是使存戶與銀行間之「金錢消費寄託契約」、「委任契約」全部或部分終止<sup>106</sup>，而金融機構之暫停帳戶全部或部分之交易功能，可說是契約全部或部分終止後，提供委任之一方並無義務提供服務之當然結果。準此，一旦通報之機關發出書面通知給金融機構後，即已經對金融機構及特定存戶發生變更契約之法律效果。因此，「法院、檢察署、司法警察機關」等通報機關之書面通知，應屬行政法上定義之行政處分。

何況，該管理辦法第9條第2項明白指出：「警示帳戶之開戶人對其存款帳戶被列為警示如有疑義，由開戶人洽原通報機關處理，銀行於必要時並應提供協助。」，換言之，由該管理辦法內容可知，金融機構對於原通報機關之通報應依法尊重，且不可能有所變更，即存戶當事人權益受損實際上係因原通報機關之行為所致，故存戶當事人若有不服，應直接向原通報機關請求救濟，而非向金融機構提起，因為金融機構並無決定之權限。依此，該管理辦法之規定，更可以證明「法院、檢察署、司法警察機關」等通報機關之書面通知階段，已屬發生對外法律效力之行政處分。

## 二、此行政處分是否有法源依據？

按「契約自由原則」(Freedom of Contract)的內涵包括，締約的自由(是否締結契約的自由)、對象選擇的自由(與誰締結契約的自由)、內容的自由(訂立什麼內容的契約的自由)及方式的自由(以何種方式訂立契約的自由)<sup>107</sup>。而契約自由為個人自主發展與實現自我之重要機制，並為私法自治之基礎，除依契約之具體內容受憲法各相關基本權利規定保障外，亦屬憲法第22條所保障其他自由權利之一種。惟國家基於維護公益之必要，尚非不得以法律對之為合理之限制<sup>108</sup>。簡言之，即個人之間的契約關係，應根據契約當事人自由意思決定，而不得受到國家的干涉，若欲對人民之契約自由權利加以限制，必須符合憲法第23條所定必要程序，並以法律定之或經立法機關明確授權由行政機關以命令訂定<sup>109</sup>。

<sup>105</sup>參吳庚，行政法之理論與實務，增訂4版，第9頁，自版，1998年。

<sup>106</sup>按行政處分需直接對外發生法律上效果，而此法律上效果不必限於公法上效果，產生私法上效果者，亦屬行政處分。見前揭註書第294頁。

<sup>107</sup>陳聰富，定型化契約的管制，台大校友雙月刊，<http://www.alum.ntu.edu.tw/read.php?num=25&sn=438>，(2006/May/26)。

<sup>108</sup>2004年4月23日之司法院大法官解釋第576號解釋文。

<sup>109</sup>參前揭註105，第77、83、88、92頁。

而如前所述，「法院、檢察署或司法警察機關」通報銀行將帳戶列為警示之書面通告是一種行政處分，則此行政處分之法源依據為何？乍看之下，廣義之行政機關為通報警示之依據，似為行政院監督管理委員會銀行局發布之「異常帳戶管理辦法」第3條第3款、第4條，然而，此行政命令是否有逾越母法之授權範圍、目的？不無疑問。

2005年5月18日修正公布銀行法第45條之2第2項規定：「銀行對存款帳戶應負善良管理人責任。對疑似不法或顯屬異常交易之存款帳戶，得予暫停存入或提領、匯出款項」，此係對人民契約內容自由之限制。又行政院金管會銀行局於2006年4月27日發布之「異常帳戶管理辦法」，固係依照銀行法第45條之2第3項之授權所為之行政命令，惟參諸銀行法第45條之2第2項之原意，是銀行基於善良管理人之責任，對可疑帳戶有拒絕提供契約服務之權利，而此可疑帳戶之認定應由帳戶之所屬金融機構為之，且此認定之統一標準應由主管機關訂定，然而，在該管理辦法中第4條屬於第2類之認定標準、分類，及第9條第2項規定若警示帳戶之開戶人對帳戶被列為警示有疑義，由開戶人洽原通報機關處理等情可知，依照通報被列為警示帳戶之認定，並非為各金融機構為之，而是委由原通報之機關來認定，且開戶人僅能對原通報機關聲明不服或提起救濟。從而，此處便涉及「再委任」之合法性問題，即銀行法授權各金融機構在發現有可疑帳戶之情形時，有權得限制人民之契約自由，但在銀行法授權所定之行政命令卻又將此認定權限委任其他機關為之，顯然違反行政法之受任者不得再委任之法理<sup>110</sup>。

從上所言，「異常帳戶管理辦法」規定得由「法院、檢察署、司法警察機關」通報銀行將帳戶警示，即將認定可疑帳戶之責任，再委任「法院、檢察署、司法警察機關」為之，並無法律明文授權，顯有違背授權母法之授權範圍、目的。倘「法院、檢察署、司法警察機關」依照該管理辦法所為之通報，均係無權限所為之違法行政處分。不論是該管理辦法，抑或是該違反行政處分，均有無效或得撤銷之原因。

### 3.1.6 警示帳戶內款項之處置

一、2006年4月27日「異常帳戶管理辦法」發布前之作法：

依行政院金融監督管理委員會2004年7月28日金管銀(一)字第0931000499號函：「金融機構『警示帳戶』中屬遭歹徒持偽(變)造或他人之身分證件冒名開立者<sup>111</sup>，若有被害人在被詐騙後請求返還滯留於『警示帳戶』內之剩餘款項，金融機構於確認被害人所匯(轉)入之款項尚有未被提領(轉出)者，經被害人提示下列文件，請求返還時，請金融機構斟酌協助：(一)刑事案件報案三聯單。(二)匯(轉)入款項之證明文件。(三)申請不實致金融機構受有損失，由被害人負一切法律責任之同意書等文件」。簡言之，即遭他人持偽造、變造證件冒名申請帳戶

<sup>110</sup>受任者不得再委任(Postestas delegata non delegatur)法理，係指如憲法或授權法律本身並無許可再委任之規定，一般主張視為再委任之禁止，見前揭註105，第262頁。

<sup>111</sup>依中央銀行業務局88年6月3日(八八)台央業字第○二○○七七一號函釋，因被冒名本人與金融業者並無訂立存款契約之意思，故該存款契約自始無效，金融業者不論該帳戶係屬支票存款、活期(儲蓄)存款或定期(儲蓄)存款皆應結清該帳戶，而其餘額則應俟依法可領取者申請給付時，再予處理。

之「警示帳戶」之被害人，得依前揭函示備妥相關文件後，直接請求銀行返還所匯入之款項。至於係自願性交付帳戶供他人使用而被金融機構列為「警示帳戶」的情形，則需由匯款之被害人向法院提起不當得利返還之民事訴訟<sup>112</sup>，始能依法院之確定判決請求銀行返還所匯款項<sup>113</sup>。

## 二、「異常帳戶管理辦法」發布後之作法：

存款帳戶經通報為「警示帳戶」或經認定為「衍生管制帳戶」者，金融機構均會將帳戶內匯入之款項逕以退匯方式退回匯款行，既不需人民提出相關文件請求，亦不待法院之確定判決即可為之。又經通報為「警示帳戶」且將匯入款項退回匯款行後尚有餘額時，則依照管理辦法第 11 條第 2 項規定，金融機構應依開戶資料聯絡開戶人，並協商發還上剩餘款項事宜，若無法聯絡開戶人，則由金融機構透過匯（轉）出行通知被害人檢具相關資料發還剩餘款項。但是，若有第 11 條第 3 項各款之情形，則金融機構得逕行結清該警示帳戶，並將剩餘款項轉列其他應付款，俟依法可領取者申請給付時處理之。

### 3.1.7 警示帳戶之解除

#### 一、「異常帳戶管理辦法」發布前：

內政部邀集金管會、刑事局等單位舉行跨部會第 2 次「反詐騙聯防平台會議」之決議中，金管會銀行局提案：建請警察機關對於警示帳戶應限期偵結移送法辦，並研議一定期限後，解除警示帳戶；另對於警示帳戶臨櫃提領或找到人頭戶時，經偵訊後，如確認無涉案嫌疑者，亦應儘速解除該警示帳戶。決議內容為<sup>114</sup>：「1. 經查證該帳戶係遭冒名或偽（變）造者，由警察機關行文恢復其金融信用，惟該遭冒名申請之帳戶仍應繼續警示，至於該警示帳戶應可臨櫃提領，其詳細提領作業程序請由行政院金融監督管理委員會銀行局與內政部警政署研擬相關措施另案函送相關單位參辦。2. 偵辦中之案件則俟司法程序終結（不起訴處分、無罪判決、罰金、判刑執行完畢後），由警察機關依據當事人提出解除警示之要求行文金融機構辦理解除，並恢復其金融信用。3. 有關未破案或未有民眾出面主張該警示帳戶遭誤設之案件，因未有嫌疑人，故無法限期移送地檢署偵辦，且此類案件因涉及帳戶內款項問題，牽涉廣泛，應持續設立警示帳戶為宜。4. 對於遭詐騙集團利用

<sup>112</sup> 參台灣桃園地方法院 94 年訴字第 33 號判決。

<sup>113</sup> 我國目前實務作法，是被害人以原告身分，向帳戶名義人請求返還詐騙之金額，而非直接以銀行為被告請求返還，然而，日本實務作法與我國不盡相同，是由原告直接對銀行提起不當得利返還之訴訟。2005 年 3 月 30 日日本東京地方裁判之判決，原告是被害人，被告是銀行，訴之聲明：原告要求將其所被騙匯入被告銀行某帳戶之金額返還，先位之訴，是依據不當得利請求權請求銀行返還款項，備位之訴，是由原告依據不當得利請求權，代位帳戶之名義人向銀行請求返還匯入之金錢。而法院之判決認為，先位之訴之聲明無理由，因為銀行是基於與存款戶間契約而受領被害人匯入之款項，故銀行取得金錢並非無法律上之原因。至於備位之訴，因為原告係受詐騙集團詐騙而匯入至銀行之帳戶，而存款帳戶名義人與原告間並無法律關係存在，故存款名義人受領金錢顯係無法律上原因而受有利益，故由原告代位原存款帳戶名義人向銀行請求返還金錢，應認有理由。參見「いわゆる振り込め詐欺の被害者が振込先口座の預金者に対する不當利得返還請求権を被保全債権として同預金者の銀行に対する預金返還請求権を代位元行使することが認められた事例（東京地判 17.3.30）」，判例特報，1895 期，第 44 頁，2005 年 8 月 11 日。

<sup>114</sup> 謝宏滿，「警示帳戶」相關問題之處理機制，未公開發表之內部報告。

之善意第三者 (如詐騙集團先至購物網站上標得物件並以欲匯款之名義套取無辜第三者之帳號，再以此帳號向另一名被害人稱有物品欲出售，要求其將款項匯入該帳號，同時騙得先前向無辜第三者標得之物件)，經查證屬實者，由警察機關行文設立警示帳戶之金融機構解除警示，並恢復其金融信用。」

## 二、「異常帳戶管理辦法」發布後：

依「異常帳戶管理辦法」規定，警示帳戶之解除情形有二，第一，警示帳戶之期限屆滿：警示帳戶之警示期限自每次通報時起算，逾5年自動失其效力（第9條第1項）；第二、依原通報機關之通報解除者（第10條第1項）。又因警示帳戶所產生之「衍生管制帳戶」，經金融機構查證疑似不法或顯屬異常情形消滅時，即應解除相關限制措施。又依管理辦法第5條規定：存款帳戶如屬偽冒開戶者，金融機構應結清該帳戶，其剩餘款項則俟依法可領且者申請給付時處理。惟若存款帳戶經警示後，始發現為冒名申請者，則該辦法對於遭冒名申請之帳戶是否仍應繼續警示，並未明文規定。

### 3.1.8 被誤列為警示帳戶之救濟管道

#### 一、「異常帳戶管理辦法」發布前：

在「異常帳戶管理辦法」發布前，是由警調機關認定帳戶是否為可疑帳戶，倘警調機關之初步查證有誤認之情形，則誤被認定並列為「警示帳戶」之帳戶使用人，是否有救濟之管道？是否有國家賠償之適用？實務上確實曾發生誤認為可疑帳戶之情形，即詐騙集團先至拍賣網站上標得物品、佯裝欲匯款，而取得賣方之銀行帳號後，再於網路上向不知情之人誣稱欲出賣標得之物，並要求對方將款項匯入原先賣方之銀行帳戶，而無償詐得標賣之物件。從而，該無辜之原先標賣者即賣方，會被最後標買者誤認為是詐騙行為人。又實務上另一案例為<sup>115</sup>：網路經營商品之同業者，為打擊某甲網站商業信譽，從網路拍賣之網站得知某甲網站經營者之銀行帳號後，另以虛偽之姓名、身分證字號等資料向台灣億貝股份有限公司之拍賣網站（e-Bay）申設帳號後，並刊登欲拍賣電腦物品之不實廣告，致標得者匯入款項後而取不到貨款。標得者則不甘被騙而報警處理，被詐騙集團利用之某甲使用之帳戶遂被警察視為疑似帳戶，之後逕而被銀行列為「警示帳戶」。從以上實例可知，於現實生活中，確實有無辜之帳戶持有人，會被誤認或遭陷害而被警方認定為可疑之帳戶，且倘進一步被金融機構列為「警示帳戶」，則該帳戶使用人應如何主張其權利？不無疑問。

依照跨部會第二次「反詐騙聯防平台會議」之決議，對於遭詐騙集團利用之善意第三人之帳戶，若查證屬實並非應列為警示之帳戶，則警察機關應行文予設立該警示帳戶之金融機構請求解除警示，並恢復其金融信用。

又各金融機構依照「警示通報機制」列為警示帳戶，而認定之依據，均是依警調機關之初步查證認定為可疑帳戶後，始依警調之請求列為「警示帳戶」。是故，倘警調有誤認之情形，帳戶使用人自得依行政訴訟法第8條之一般給付之訴的規

<sup>115</sup> 桃園地方法院檢察署 94 年度偵字第 7795 號不起訴處分書。

定<sup>116</sup>，請求警調機關將函予各金融機構請求列為警示帳戶之函文作廢，另請求警調機關函文予該金融機構表示前揭認定為可疑帳戶尚有誤會並請予解除警示帳戶之設置。再者，一旦被認定為警示帳戶後，則帳戶使用人喪失臨櫃交易以外之使用權限，則其行使財產權之權利，難謂尚未受影響，故若警調機關有故意或過失之情形，則帳戶使用人亦應有依照國家賠償法第 2 條第 2 項前段規定，聲請國家賠償之權利。

## 二、「異常帳戶管理辦法」發布後：

該管理辦法第 9 條第 2 項明白指出：警示帳戶之開戶人對其存款帳戶被列為警示如有疑義，由開戶人洽原通報機關處理，銀行於必要時並應提供協助。然而，存款帳戶之申請人應如何向原通報機關請求救濟卻未加以規定或說明。

### 3.1.9 「異常帳戶管理辦法」之適法性問題

如前所述，管理辦法就警示帳戶之認定，已違反行政法再委任禁止之法理，此部分辦法之發布即有瑕疵。此外，從銀行法第 45 條之 2 第 2、3 項：「銀行對存款帳戶應負善良管理人責任。對疑似不法或顯屬異常交易之存款帳戶，得予暫停存入或提領、匯出款項。」、「前項疑似不法或顯屬異常交易帳戶之認定標準，及暫停帳戶之作業程序及辦法，由主管機關定之」可知，授權命令除不得逾越母法外，其內容僅能就母法對於「可疑帳戶認定標準」及「該可疑帳戶之暫停帳戶程序」有關之細節性、技術性事項加以規定<sup>117</sup>。即銀行法之母法，僅限制人民契約締結後契約何時終止、契約變更等之契約內容自由，然授權訂定之行政命令，竟於管理辦法第 13 條第 2 款列出銀行應拒絕人民「開戶」的事項，即在某些情況下，限制金融機構與人民締結契約之自由，此辦法不僅明白限制人民之自由權利，且違反銀行法授權之範圍、目的，而行政院監督管理員銀行局發布管理辦法第 13 條第 2 款之內容顯然欠缺法律授權之依據，亦有無效或得撤銷之原因。

## 3.2 限制轉帳方式之適法性

### 3.2.1 限制轉帳之由來與歷程

內政部警政署表示，透過自動櫃員機（ATM）轉帳詐騙的報案案件，平均一天有 110 件，一個月 3000 件，總金額約三億元，有加以防堵之必要<sup>118</sup>。行政院反詐騙聯防平台會議於 2005 年 4 月 12 日之會議中，決議將 ATM 提款機的非約定轉帳金額從每天 10 萬元<sup>119</sup>降至 1 萬元。然此自動櫃員機（ATM）非約定轉帳額度 1 萬元上限之法

<sup>116</sup>人民與中央或地方機關，因公法上原因發生財產上之給付或請求作成行政處分以外之其他非財產上之給付，得提起給付訴訟，行政訴訟法第 8 條第 1 項前段定有明文。又按人民在公法上享有之給付請求權，並不以財產上之給付為限，尚包括請求行政機關應為作為，忍受或不作為之其他非財產上給付的請求權在內，例如請求閱覽卷宗，請求將特定資料作廢，請求撤回妨害名譽的主張，均屬之，有該立法理由可參。

<sup>117</sup>參前揭註第 105，第 260 頁。

<sup>118</sup>聯合報，A1 版要聞，2005 年 4 月 15 日。

<sup>119</sup>金融監督管理委員會會議決議於 2004 年 5 月 10 日起，金融機構之金融卡非約定轉帳金額，每日不得超過新台幣十萬元，有台財融（一）字第 0931000318 號函及 2004 年 4 月 27 日「研商防制利用自動櫃員機詐財案件」會議紀錄可參，<http://www.banking.gov.tw/ct.as?xItem=63796&ctNode=1580>，

策引發民怨，故行政院長於 2005 年 4 月 14 日下達指示後改弦更張，提高轉帳限額至 3 萬元，行政院金融監督管理委員會旋於當日開會，研商配合自 2005 年 6 月 1 日起，ATM 非約定帳戶轉帳單日轉帳限額降為新台幣三萬元之執行事項及相關因應方案，並於翌日即同年 4 月 15 日以金管銀(二)字第 094200027 號函銀行公會轉知所屬會員機構關於自 2005 年 6 月 1 日起實施「金融卡非約定帳戶轉帳單日限額調降為 3 萬元」措施，並將公用事業費率(含水、電、瓦斯)、國公營機構(國稅局)以及自有帳戶三大類，排除於非約定轉帳 3 萬元限制之外<sup>120</sup>。

刑事局長侯友宜認為限制 ATM 轉帳金額，還不能徹底防制詐騙犯罪，一度建議銀行完全取消非約定轉帳功能，但未獲同意<sup>121</sup>。在行政院反詐騙聯防平台會議的決策過程中，法務部曾主張建議金融機構延遲自動櫃員機轉帳入帳時間，以確保被詐財民眾之財產損失，惟金管會認為，若採取延遲轉帳之方案將會造成帳務系統混亂，且必須修改系統，成本太高<sup>122</sup>；而目前 ATM 轉帳總筆數，八成五的金額不到 3 萬元(84.3%)<sup>123</sup>，僅一成五超過 3 萬元<sup>124</sup>，故採取降低轉帳限額之方式措施顯較延遲轉帳為可行。又行政院亦表示，各國銀行多設有 ATM 轉帳金額限制，包括：香港渣打銀行新台幣 4 萬元，新加坡 DBS 銀行約 2 萬元，美國銀行(亞洲地區分行)約新台幣 2 萬元<sup>125</sup>。故最後在該次決議中決議調降非約定轉帳之每日上限來遏阻詐欺之氾濫。

據 TVBS 民調中心自 2005 年 4 月 14 日連續兩天民調比較發現<sup>126</sup>，在剛宣布轉帳金額上限 1 萬元時，51%受訪者表示反對，41%贊成；上限放寬為 3 萬元後，不贊成的比例由 51%降低為 32%，贊成的比例由 41%提高到 59%，可見在轉帳上限放寬後，民眾的反對聲浪隨之降低。又調查顯示，如果可以選擇，40%民眾希望轉帳金額限制提高至 5 萬元，30%贊成 3 萬元的額度，只有 10%贊成降低為 1 萬元。另有 3%民眾認為要維持原來的 10 萬元上限，17%沒意見。從以上之民調結果可知，民眾肯定金融卡非約定轉帳上限降低有助於防堵詐騙之犯罪，但上限金額訂為多少，將影響民眾之生活便利性。

而此限制轉帳制度之實施，是否真的能降低詐騙，成效值得懷疑<sup>127</sup>。又有反對意見認為，因為 ATM 轉帳較臨櫃轉帳之成本低且增加民眾時間成本<sup>128</sup>，且立法委

---

(2006/Mar/10)。

<sup>120</sup>參見行政院金融監督管理委員會銀行局 94 年 4 月份大事紀要及行政資訊目錄。

<sup>121</sup>陳一雄，聯合報，A5 版話題，2005 年 4 月 13 日。

<sup>122</sup>台財融字第 0931000331 號函及「研商遲延自動櫃員機轉帳入帳時間防制利用自動櫃員機轉帳功能進行詐騙事宜」會議紀錄，該會決議認為：延遲自動櫃員機轉帳入帳時間之作法，雖可能保護少數被詐財之民眾，卻使得每日高達一百萬筆以上正當使用 ATM 轉帳之消費者受到影響，顯不符比例原則，見 <http://www.banking.gov.tw/ct.asp?xItem=63800&ctNode=1580>，(2006/Mar/10)。

<sup>123</sup>卓榮泰，經濟日報，A4 版金融新聞，2005 年 4 月 15 日。

<sup>124</sup>同前揭註。

<sup>125</sup>行政院回覆曾華德立法委員之書面質詢，見立法院公報，94 卷，第 40 期，第 97 頁。

<sup>126</sup>此次調查於 14 日晚間以電話訪問進行，共接觸 1088 位 20 歲以上台灣地區民眾，其中拒訪為 66 人，拒訪率 6%，成功訪問有效樣本 1022 人，在 95%的信心水準下，抽樣誤差為正負 3.1。見聯合報，2005 年 4 月 16 日。

<sup>127</sup>楊文琪、邱金蘭，經濟日報，A4 版金融新聞，2005 年 4 月 14 日。

<sup>128</sup>陸倩瑤，聯合報，A3 版焦點，2005 年 4 月 15 日。

員劉億如計算認為將增加 260 億元之成本<sup>129</sup>，再者，金管會雖然是銀行之主管機關，但是依法似乎並未有此權限，故有未依法行政之疑問<sup>130</sup>。

### 3.2.2 限制轉帳之適法性

行政院金管會銀行局於 2005 年 4 月 15 日以金管銀（二）字第 094200027 號函銀行公會轉知所屬會員機構關於自 2005 年 6 月 1 日起實施「金融卡非約定帳戶轉帳單日限額調降為 3 萬元」措施。金管會銀行局對各金融機構為前揭函文內容之指示，實際上是利用不具法律強制力之指導方式，促請各金融機構為一定之作為或不作為。又金融監督管理委員會銀行局亦認定：其於 2005 年 4 月 15 日金管銀（二）字第 0942000227 號函因銀行公會轉知所屬會員機構於自同年 6 月 1 日起實施「金融卡非約定轉帳單日限額調降為 3 萬元」措施，係一種「行政指導」。

由上可知，行政院金管會銀行局係利用函令透過銀行公會要求各銀行等金融機構約束各金融機構實行「限制轉帳」之機制，而如前在警示帳戶機制章節談過，目前銀行公會對主管機關之指示，均會遵照辦理，而金融監督管理委員會銀行局之函令，實為行政機關規避依法行政的迂迴手法，確有可議之處。

## 3.3 洗錢防制法之修法

### 3.3.1 洗錢防制法之修法

洗錢防制法於 1997 年 4 月 23 日立法公布實行時規定，掩飾或隱匿因自己或他人重大犯罪所得財物或財產上利益者，為洗錢態樣之一，應處 5 年以下有期徒刑，得併科新臺幣 300 萬元以下罰金，第 2 條第 1 款、第 9 條第 1 項定有明文。即並未嚴格區分係為掩飾、隱匿「自己」或「他人」之重大犯罪所得，均以同條款來處罰。

而洗錢防制法乃於 2003 年 2 月 6 日修正公布，並於同年 8 月 6 日施行，將掩飾「他人」重大犯罪所得財物或財產上利益之洗錢態樣，特別移列到同條第 2 款，並提高刑罰為「處七年以上有期徒刑，得併科新臺幣五百萬元以下罰金」，參其立法目的為<sup>131</sup>：「為明確區分犯罪行為人之洗錢行為之態樣係為自己或為他人，而以第二條第一款規範犯罪者將自己犯罪所得加以漂白之行為，至於他人幫助重大犯罪者漂白黑錢之行為，則規範於同法第二條第二款。又提高刑度，以求達到有效嚇阻及制裁犯罪之效果。」。本文將新舊法條文之比較製作附表，參如下表 7。

<sup>129</sup>陳素玲、黃國樑，聯合晚報，1 版要聞，2005 年 4 月 14 日。

<sup>130</sup>易明秋，聯合報，A15 版/民意論壇，2005 年 4 月 15 日。

<sup>131</sup>參見立法院議案關係文書，院總第 1692 號政府提案第 8848 號，案由：行政院函請審議「洗錢防制法修正草案」，2002 年 10 月 30 日印發。

表 7 洗錢防制法第 2、9 條修正前後對照表

現行條文	修正前條文
<p>第二條 本法所稱洗錢，係指下列行為： 一、掩飾或隱匿因自己重大犯罪所得財物或財產上利益者。 二、掩飾、收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益者。</p>	<p>第二條 本法所稱洗錢係指下列行為： 一、掩飾或隱匿因自己或他人重大犯罪所得財物或財產上利益者。 二、收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益者。</p>
<p>第九條（第一至三項） 犯第二條第一款之罪者，處五年以下有期徒刑，得併科新臺幣三百萬元以下罰金。 犯第二條第二款之罪者，處七年以下有期徒刑，得併科新臺幣五百萬元以下罰金。 以犯前二項之罪為常業者，處三年以上十年以下有期徒刑，得併科新臺幣一百萬元以上一千萬元以下罰金。</p>	<p>第九條（第一至二項） 洗錢者，處五年以下有期徒刑，得併科新臺幣三百萬元以下罰金。 以犯前項之罪為常業者，處一年以上七年以下有期徒刑，得併科新臺幣一百萬元以上一千萬元以下罰金。</p>

### 3.3.2 販賣人頭帳戶犯罪之適用法律疑問

提供帳戶予他人使用之犯罪型態，可謂是詐欺案件之衍生、前置犯罪，已如前述。目前我國審判實務對於單純提供帳戶予他人從事詐欺犯罪行為者，均肯認成立犯罪，惟對販賣人頭帳戶者之行為成立何種罪名則有不同意見，然而，處罰販賣人頭帳戶者所得適用之刑罰法律，不外乎為刑法之詐欺幫助犯及洗錢防制法第 9 條之規定。審判實務之法院認為提出帳戶予他人從事詐欺集團之不法行為，所可能觸犯之刑罰，有以下幾種看法，整理表格如下表 8：

表 8 法院論罪整理表

編號	觸犯之罪名	法院判決之理由
一	幫助詐欺取財罪（刑法第 339 條） <sup>132</sup>	帳戶名義人將其所有之帳戶等物借予他人用以詐騙財物，顯係基於幫助他人詐欺取財之犯意，且所為提供帳戶存摺、提款卡及密碼等物之行為，屬刑法詐欺取財構成要件以外之行為，其既以幫助他人犯罪之意思而參與構成要件以外之行為，係犯刑法第 30 條第 1 項前段、第 339 條第 1 項之幫助詐欺取財罪。
二	幫助常業詐欺取財罪 <sup>133</sup>	提供帳戶之行為人明知綽號「阿良」等人向其收購帳戶，係供作該等詐欺集團詐騙他財物之匯款使用，仍將所收購之人頭帳戶之存摺、印章、提款卡等物轉售予「阿良」等人，彼等所屬詐欺集團再據以為詐欺取財之匯款帳戶，並以之為常業，提供帳戶之人自有幫助該等詐欺集團遂行常業詐欺之確定故意，且係參與提供取得常業詐欺取財犯罪所得款項工具，對此犯行施以助力，為常業詐欺取財構成要件以外之行為，應以常業詐欺取財罪之幫助犯論之。
三	違反修正前洗錢防制法第 9 條第 1 項 <sup>134</sup>	按掩飾或隱匿因自己或他人重大犯罪所得財物或財產上利益，係屬（修正前）洗錢防制法第 2 條第 1 款規定所稱之「洗錢」；又依同法第 3 條第 1 項第 5 款規定，刑法第 340 條之常業詐欺罪，係屬該法所稱「重大犯罪」。而自政府開放金融業申請設立後，金融機構大量增加，使一般人申請存款帳戶極為容易且便利，未設有資格限制。故除非存款帳戶使用人欲將存款帳戶充作犯罪之用，否則一般充作正常使用之存款帳戶，並無向他人收購或借用之必要，此乃人民均知之常識。況坊間新聞媒體，對於不肖犯罪集團常大量收購或借用存款帳戶後，再持以供作犯罪使用，藉此逃避檢警查緝之情事，亦多所報導。準此，提供帳戶之人對於：其將上開郵政劃撥儲金帳戶及郵政存簿儲金帳戶之印章、存摺及金融卡，交付予他人使用，而該他人係欲將之充作掩飾或隱匿因自己或他人犯罪所得財物或財產上利益之用等情，實難難諉為不知。從而，人頭帳戶名義人所為，應係涉犯洗錢防制法第 9 條第 1 項洗錢罪。

<sup>132</sup>台灣高等法院台中分院 94 年度金訴字第 311 號判決

<sup>133</sup>台灣高等法院 93 年度金訴字第 1314 號判決

<sup>134</sup>有台灣高等法院台中分院 92 金上訴字第 1081 號判決可資參照。

表 8 法院論罪整理表（續）

編號	觸犯之罪名	法院判決之理由
四	違反洗錢防制法第 9 條第 1 項幫助犯 <sup>135</sup>	有犯罪意圖者，非有正當理由，使用他人提供之帳戶，客觀上自可預見其目的係供為某筆資金之存入，後再行領出之用，且該筆資金之存入及提領過程係有意隱瞞其流程及行為人身分曝光之用意，一般人本於一般認知能力應均易於瞭解。是依一般人之社會生活經驗，若見他人不以自己名義申請帳戶，反向他人收集存款帳戶為不明用途使用或流通，衡情對於該等帳戶可能供洗錢等不法目的之使用，當有合理之預期，且利用不相識之人之帳戶從事詐欺所得財物洗錢之用，早為傳播媒體廣為報導，被告為一有社會經驗之成年人，其應可預見交付其名義之帳戶存摺及金融卡等物件予不相識之人流通，有幫助從事常業詐欺犯行之人利用該等帳戶掩飾該常業詐欺集團成員因自己犯罪所得財物或財產上利益之可能。是帳戶名義人將帳戶物件提供予他人，而使某犯罪集團於實施常業詐欺之重大犯罪時得以利用該等帳戶供掩飾因自己重大犯罪所得財物之用之行為（提供帳戶非洗錢犯罪之構成要件行為），顯有幫助洗錢之不確定犯意，故係犯現行洗錢防制法第 9 條第 1 項、刑法第 30 條第 1 項前段之幫助掩飾因自己重大犯罪所得財物罪。
五	幫助常業詐欺及違反修正前洗錢防制法第 9 條第 1 項 <sup>136</sup>	帳戶名義人明知交付存簿、金融卡予他人將掩飾他人常業詐欺所得之財物，然其為達個人利益，仍將存簿等物交付他人，足見其對掩飾他人常業詐欺所得之財物之事實，預見其發生，而其發生並不違背其本意，核其所為係犯幫助常業詐欺及修正前洗錢防制法第 9 條第 1 項之洗錢罪。
六	幫助常業詐欺及違反修正前洗錢防制法第 9 條第 1 項之幫助洗錢 <sup>137</sup>	帳戶名義人之帳戶為詐欺集團利用，而該等詐欺集團向被害人詐騙金錢後欲再提領現金之行為，應屬洗錢防制法所稱掩飾、隱匿因他人重大犯罪所得財物或財產利益之行為，則帳戶提供者基於不確定故意而提供帳戶作為詐欺集團洗錢之用，應係幫助他人洗錢之行為，是其所為係犯刑法第 30 條第 1 項前段、第 340 條之幫助常業詐欺罪及刑法第 30 條第 1 項前段、修正前洗錢防制法第 9 條第 1 項之幫助洗錢罪。

<sup>135</sup> 台灣高等法院 93 年度上訴字第 2973 號判決。

<sup>136</sup> 台灣高等法院高雄分院 93 年度上訴字第 409 號判決。

<sup>137</sup> 台灣高等法院台中分院 92 金上訴第 1748 號判決。

表 法院論罪整理表（續）

編號	觸犯之罪名	法院判決之理由
七	幫助常業詐欺及違反洗錢防制法第 9 條第 1 項之幫助犯 <sup>138</sup>	人頭帳戶名義人將所有之帳戶物件交付予不詳姓名、年籍之成年人，而使某犯罪集團得以便於實施常業詐欺之重大犯罪，利用帳戶名義人提供之帳戶作掩飾、隱匿因自己重大犯罪所得財物之用，其所為係犯刑法第 340 條、第 30 條第 1 項前段之幫助常業詐欺罪及現行洗錢防制法第 9 條第 1 項、刑法第 30 條第 1 項前段之幫助掩飾、隱匿因自己重大犯罪所得財物罪。
八	幫助常業詐欺及違反洗錢防制法第 9 條第 2 項 <sup>139</sup>	帳戶名義人提供帳戶之行為，係以幫助之意思為詐欺集團之常業詐欺犯行施以助力，核其所為係犯刑法第 30 條第 1 項、第 340 條之幫助常業詐欺罪。又帳戶名義人將其在金融機構之帳戶，連同存摺及金融卡提供他人，供常業詐欺集團將詐欺所得財物過帳之用，其行為應屬洗錢防制法第 2 條第 2 款為他人掩飾犯罪所得之構成要件行為。而常業詐欺罪，依洗錢防制法第 3 條第 1 項第 5 款之規定，係屬該法所稱之重大犯罪，則此部分之行為，又犯洗錢防制法第 9 條第 2 款之洗錢罪。
九	幫助常業詐欺及違反洗錢防制法第 9 條第 2 項幫助犯 <sup>140</sup> 。	帳戶名義人多次出賣存摺、提款卡等物件予姓名、年籍不詳之他人，其對於他人將利用該等存摺、提款卡等物，充作轉向第三人常業詐欺及掩飾常業詐欺所得贓款之工具，顯有認識並能預見，且亦不違反彼等本意，堪認帳戶名義人確有幫助他人常業詐欺及幫助該等人掩飾常業詐欺所得贓款(常業洗錢)之情事。

綜觀以上法院判決之結果可知，審判實務上，對於提供帳戶予他人從事不法行為者究應如何適用法律，發生歧見之原因，不外乎係就以下幾個法律上問題，有不同之看法：第一，人頭帳戶之名義人是構成幫助詐欺或幫助常業詐欺之罪名。第二，人頭帳戶之名義人是否同時涉犯洗錢防制法之罪嫌，此部分又有以下幾點爭議：1.出賣或出借帳戶予他人之行為是否構成洗錢防制法之「洗錢」行為。2.若認為符合「洗錢」之定義，則人頭帳戶名義人是洗錢之正犯或幫助犯。3.又若是幫助犯，則人頭帳戶名義人是幫助「自己」或「他人」掩飾犯罪所得。是以，因為以上幾點法律觀點、見解之不同，導致實務上之法律適用莫衷一是，迄今各高等法院既未有一致之見解，最高

<sup>138</sup> 台灣高等法院 94 年度上訴字第 296 號判決。

<sup>139</sup> 台灣高等法院 93 年度上訴字第 2759 號判決。

<sup>140</sup> 台灣高等法院 91 上訴字第 2263 號判決。

法院就此部分亦未有明確之統一看法，是本文即有加以探討、整理之必要。本文以下分別就前開各個法律爭議，整理法院之不同基本論點，進而提出個人之淺見。

#### 一、相關法條之說明

在整理法院不同見解之前，先就提供帳戶者所可能涉及之法律條文簡單說明如下。第一部份，關於刑法之相關規定：刑法第 339 條第 1 項規定：「意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處五年以下有期徒刑、拘役或科或併科一千元以下罰金」。刑法第 340 條：「以犯前條之罪為常業者，處一年以上七年以下有期徒刑，得併科五千元以下罰金」。刑法第 30 條第 1、2 項：「幫助他人犯罪者，為從犯。不知幫助之情者，亦同」、「從犯之處罰，得按正犯之刑減輕之。」。第二部分，關於洗錢防制法之規定簡述如下：1996 年 10 月 3 日，立法院第 3 屆第 2 會期第 7 次會議，通過洗錢防制法，而於同年 10 月 23 日由總統公布<sup>141</sup>，並自公布後 6 個月施行，亦即自 1997 年 4 月 23 日正式開始施行。該法第 2 條、第 9 條第 1、2 項分別規定：「本法所稱洗錢，係指下列行為：一、掩飾或隱匿因自己或他人重大犯罪所得財物或財產上利益者。二、收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益者」；「洗錢者，處五年以下有期徒刑，得併科新臺幣三百萬元以下罰金」、「以犯前項之罪為常業者，處一年以上七年以下有期徒刑，得併科新臺幣一百萬元以上一千萬元以下罰金。」。又刑法第 340 條之常業詐欺罪屬洗錢防制法第 3 條第 1 項第 5 款所明訂之重大犯罪。然而，洗錢防制法已於 2003 年 2 月 6 日修正公布<sup>142</sup>，並於同年 8 月 6 日施行，而此次修正共 10 條條文，新增 2 條條文，而修正後第 2 條、第 9 條第 1、2、3 項分別修正為「本法所稱洗錢，係指下列行為：一掩飾或隱匿因自己重大犯罪所得財物或財產上之利益者。二、掩飾、收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益者」；「犯第二條第一款之罪者，處五年以下有期徒刑，得併科新臺幣三百萬元以下罰金」、「犯第二條第二款之罪者，處七年以下有期徒刑，得併科新臺幣五百萬元以下罰金」、「以犯前二項之罪為常業者，處三年以上十年以下有期徒刑，得併科新臺幣一百萬元以上一千萬元以下罰金。」，惟刑法第 340 條之常業詐欺罪仍屬洗錢防制法第 3 條第 1 項第 5 款所明訂之重大犯罪，合先敘明。另製表格參照如下表 9：

<sup>141</sup>1996 年 10 月 23 日總統（85）華總（一）義字第 08500251110 號令制定公布全文 15 條。

<sup>142</sup>2003 年 2 月 6 日總統（92）華總（一）義字第 09200019300 號令制定公布全文 15 條。

表 9 販賣人頭帳戶犯罪之適用條文表

一	刑法	<p>第 339 條第 1 項：意圖為自己或第三人不法之所有，以詐術使人將本人或第三人之物交付者，處五年以下有期徒刑、拘役或科或併科一千元以下罰金。</p> <p>第 340 條：以犯前條之罪為常業者，處一年以上七年以下有期徒刑，得併科五千元以下罰金。</p> <p>第 30 條第 1、2 項：幫助他人犯罪者，為從犯。不知幫助之情者，亦同。</p>
二	洗錢防制法	<p>修法前</p> <p>第 2 條：本法所稱洗錢，係指下列行為：一、掩飾或隱匿因自己或他人重大犯罪所得財物或財產上利益者。二、收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益者。</p> <p>第 9 條第 1 項：洗錢者，處五年以下有期徒刑，得併科新臺幣三百萬元以下罰金。</p> <p>第 9 條第 2 項：以犯前項之罪為常業者，處一年以上七年以下有期徒刑，得併科新臺幣一百萬元以上一千萬元以下罰金。</p> <p>現行法</p> <p>第 2 條：本法所稱洗錢，係指下列行為：一、掩飾或隱匿因自己重大犯罪所得財物或財產上之利益者。二、掩飾、收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益者。</p> <p>第 9 條第 1 項：犯第二條第一款之罪者，處五年以下有期徒刑，得併科新臺幣三百萬元以下罰金。</p> <p>第 9 條第 2 項：犯第二條第二款之罪者，處七年以下有期徒刑，得併科新臺幣五百萬元以下罰金。</p> <p>第 9 條第 3 項：以犯前二項之罪為常業者，處三年以上十年以下有期徒刑，得併科新臺幣一百萬元以上一千萬元以下罰金。</p>

二、提供人頭帳戶之行為人構成幫助詐欺或幫助常業詐欺之罪名

若無足夠證據證明利用人頭帳戶從事詐欺取財之人為詐欺行為之常業犯，則法院在認定僅提供帳戶予他人之被告時，多以帳戶名義人將其所有之帳戶等物借予他人用以詐騙財物，顯係基於幫助他人詐欺取財之犯意，且所為提供帳戶存摺、提款卡及密碼等物之行為，屬刑法詐欺取財構成要件以外之行為，其既以幫助他人犯罪之意思而參與構成要件以外之行為，係犯刑法第 30 條第 1 項前段、第 339 條第 1 項之幫助詐欺取財罪<sup>143</sup>。倘卷證之證據資料足以認定使用人頭帳戶之詐欺

<sup>143</sup>台灣高等法院台中分院 94 年度金上訴字第 311 號判決。

集團確實為詐欺之常業行為，則法院均會以幫助常業詐欺取財罪來認定提供帳戶者之罪責<sup>144</sup>。

### 三、提出帳戶予他人使用是否成立洗錢罪

出賣或出借帳戶予他人之行為，是否構成洗錢防制法第2條所謂「掩飾或隱匿」之構成要件行為，針對台灣高等法院、台灣高等法院台中分院、台灣高等法院高雄分院及台灣高等法院花蓮分院之判決所表示之見解，臚列如下：

#### (一) 認為不成立洗錢罪之基本論點：

##### 1. 從構成要件而言，有以下幾種見解：

##### (1) 無證據證明被告單純提供帳戶之行為有掩飾他人重大犯罪之財產所得或利益：

洗錢防制法第9條第2項罪必以所掩飾、寄藏者，為他人犯常業詐欺所得財物，始足當之，若他人所犯係普通詐欺罪，或行為人並不知他人所犯係常業詐欺罪，即難以該罪相繩<sup>145</sup>。簡言之，即無證據證明他人為常業詐欺之行為，故提供帳戶者僅成立幫助詐欺罪行<sup>146</sup>。

##### (2) 被告提供帳戶供詐欺集團之被害人匯入帳戶之用，該等行為原係詐欺取財行為之一部分，並非另為掩飾、隱匿詐欺集團犯罪所得之行為：

所謂洗錢行為（自己洗錢），係指行為人完成犯罪行為後，對於犯罪所得財物或財產上利益所另為掩飾或隱匿等行為，若行為本身即係該洗錢防制法第3條所稱重大犯罪之取得財物之犯罪方法或手段，此等行為即為該條所稱重大犯罪行為之一部分，並非行為人因為該條所稱重大犯罪行為並取得犯罪所得財物或財產上利益後，所另為掩飾或隱匿犯罪所得財物或財產上利益之行為，自難認為是洗錢行為。而為他人洗錢則係指掩飾或隱匿、收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益者，亦均指於他人因重大犯罪所得財物或財產上利益後，所另為之掩飾或隱匿、收受、搬運、寄藏、故買或牙保等行為。被告提供銀行帳戶供詐欺集團作為詐欺犯罪時被害人匯款之用，被害人的匯款動作，即為詐欺集團等人常業詐欺犯行有關「使人將本人或第三人之物交付」之行為，本為詐欺取財犯罪行為的一部分，並非另為掩飾或隱匿犯罪所得財物或財產上利益之行為。換言之，即該筆詐欺取財所得之款項匯入被告提供之銀行帳戶後，並未產生掩飾或隱匿「重大犯罪所得財物或財產上利益」之效果，偵查機關隨時均能發現該帳戶係詐欺取財之犯罪行為人供被害人匯款之用，惟一能掩飾或隱匿者，乃「誰是犯罪行為人」，顯然並不符合洗錢防制法第2條規定之洗錢行為<sup>147</sup>。

<sup>144</sup>台灣高等法院93年度金訴字第1314號判決。

<sup>145</sup>台灣高等法院台中分院94年度金上訴字第311號。

<sup>146</sup>台灣高等法院台中分院93年度上易字第1139號；台灣高等法院台中分院93年度金上訴字第1314號。

<sup>147</sup>台灣高等法院台中分院93年度金上訴字第1493、1494號。台灣高等法院93年度上重訴字4號。台灣高等法院台中分院93年度金上訴字第1494號：「按洗錢防制法所稱洗錢，係指下列行為：一、掩飾或隱匿因自己或他人重大犯罪所得財物或財產上利益者；二、收受、搬運、寄藏、故買或牙保他

人因重大犯罪所得財物或財產上利益者。洗錢防制法第二條有明文。(註：九十二年二月六日修正公布之洗錢防制法全文，依該法第十五條規定自公布後六個月施行，故本案仍應就修正公布前之洗錢防制法相關條文加以檢討，應予敘明)。亦即所謂洗錢，依洗錢防制法第二條規定係以掩飾或隱匿因自己或他人重大犯罪所得財物或財產上利益為其要件，而無論掩飾或隱匿行為，均為行為人於完成犯罪行為後，為利用或確保此一前行為之不法犯罪所得財物或財產上利益所為之另一行為，應屬一種處分犯罪所得財物或財產上利益之行為(處分贓物之行為)，此觀諸同條第二款將收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益等贓物之犯罪行為，亦同列為洗錢行為甚明。就行為人而言，此種處分贓物行為，原係不罰之後行為之一種；而所謂不罰之後行為，係行為人於完成其犯罪後，對於其所侵害法益之另一次侵害，不另構成犯罪之情形。即前行為與後行為間並無行為發展之階段關係，僅處罰前行為即已兼及後行為者，該後行為即為前行為所吸收，不再視其為獨立之犯罪；例如將竊盜或搶奪取得之財物據為己有或出賣等行為，不能再論以侵占罪等。亦即洗錢行為(自己洗錢)，係指行為人完成犯罪行為後，對於犯罪所得財物或財產上利益所另為掩飾或隱匿等行為，該行為在刑罰體系上原係不罰之後行為，然因特殊社會防衛之需要(為防制洗錢，追查重大犯罪，洗錢防制法第一條參照)，始予以刑罰化；若行為本身即係該洗錢防制法第三條所稱重大犯罪之取得財物之犯罪方法或手段，此等行為即為該條所稱重大犯罪行為之一部分，並非行為人因為該條所稱重大犯罪行為並取得犯罪所得財物或財產上利益後，所另為掩飾或隱匿犯罪所得財物或財產上利益之行為，自難遽認係洗錢行為。為他人洗錢則係指掩飾或隱匿、收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益者，亦均指於他人因重大犯罪所得財物或財產上利益後，所另為之掩飾或隱匿、收受、搬運、寄藏、故買或牙保等行為。被告陳水秀提供同案被告朱榮結郵局、銀行活期儲蓄存款帳戶供「陳錫祺」及另名不詳姓名成年女子作為詐欺犯罪時被害人匯款之用，被害人的匯款動作，即為「陳錫祺」及另名不詳姓名成年女子常業詐欺犯罪有關「使人將本人或第三人之物交付」之行為，本為詐欺取財犯罪行為的一部分，並非另為掩飾或隱匿犯罪所得財物或財產上利益之行為。且被害人就其匯款之郵局、銀行活期儲蓄存款帳戶之戶名、帳號，均知之甚詳。換言之，該筆詐欺取財所得之款項匯入朱榮結提供之郵局、銀行活期儲蓄存款帳戶後，並未產生掩飾或隱匿「重大犯罪所得財物或財產上利益」之效果，偵查機關隨時均能發現該帳戶係詐欺取財之犯罪行為人供被害人匯款之用，惟一能掩飾或隱匿者，乃「誰是犯罪行為人」，顯然並不符合洗錢防制法第二條規定之洗錢行為。「陳錫祺」及另名不詳姓名成年女子利用朱榮結提供之郵局、銀行帳戶作為被害人匯款之用，本身既非洗錢防制法第二條第一、二款規定之洗錢行為，尤難論被告以洗錢防制法之罪，關於上開被害人匯款至朱榮結帳戶部分，應變更改條論被告以幫助詐欺罪已如前述，至於公訴意旨所指被害人楊天頻於九十二年二月二十五日匯款七萬二千元至朱榮結帳戶有誤(該七萬二千元係匯至案外人黃育智帳戶，而黃育智帳戶無事證明與被告有關)，被告此節犯罪不能證明部分，公訴意旨認與前開論罪部分有實質上一罪關係，按審判不可分原則，不另為無罪之諭知。九十二年二月六日修正公布之洗錢防制法全文，依該法第十五條規定自公布後六個月施行，故本案仍應就修正公布前之洗錢防制法相關條文加以檢討，應予敘明)。亦即所謂洗錢，依洗錢防制法第二條規定係以掩飾或隱匿因自己或他人重大犯罪所得財物或財產上利益為其要件，而無論掩飾或隱匿行為，均為行為人於完成犯罪行為後，為利用或確保此一前行為之不法犯罪所得財物或財產上利益所為之另一行為，應屬一種處分犯罪所得財物或財產上利益之行為(處分贓物之行為)，此觀諸同條第二款將收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益等贓物之犯罪行為，亦同列為洗錢行為甚明。就行為人而言，此種處分贓物行為，原係不罰之後行為之一種；而所謂不罰之後行為，係行為人於完成其犯罪後，對於其所侵害法益之另一次侵害，不另構成犯罪之情形。即前行為與後行為間並無行為發展之階段關係，僅處罰前行為即已兼及後行為者，該後行為即為前行為所吸收，不再視其為獨立之犯罪；例如將竊盜或搶奪取得之財物據為己有或出賣等行為，不能再論以侵占罪等。亦即洗錢行為(自己洗錢)，係指行為人完成犯罪行為後，對於犯罪所得財物或財產上利益所另為掩飾或隱匿等行為，該行為在刑罰體系上原係不罰之後行為，然因特殊社會防衛之需要(為防制洗錢，追查重大犯罪，洗錢防制法第一條參照)，始予以刑罰化；若行為本身即係該洗錢防制法第三條所稱重大犯罪之取得財物之犯罪方法或手段，此等行為即為該條所稱重大犯罪行為之一部分，並非行為人因為該條所稱重大犯罪行為並取得犯罪所得財物或財產上利益後，所另為掩飾或隱匿犯罪所得財物或財產上利益之行為，自難遽認係洗錢行為。為他人洗錢則係指掩飾或隱匿、收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益者，亦均指於他人因重大犯罪所得財物或財產上利益後，所另為之掩飾或隱匿、收受、搬運、寄藏、故買或牙保等行為。被告陳水秀提供同案被告朱榮結郵局、銀行活期儲蓄存款帳戶供「陳錫祺」及另名不詳姓名成年女子作為詐欺犯罪時被害人匯款之用，被害人的匯款動作，即為「陳錫祺」及另名不詳姓名成

(3) 被告提供帳戶之時，尚無重大犯罪之行為存在，則自無重大犯罪所得財物可資掩飾、隱匿：

被告於交付帳戶物件予他人之時，就其提供之帳戶物件而言，尚無所謂之常業詐欺之重大犯罪存在，則其提供交付帳戶物件行為自難認屬上引法條所稱之「掩飾」或「隱匿」行為，即尚無常業詐欺重大犯罪所得財物可資掩飾、隱匿，故被告單純提供帳戶予他人流通之行為，並非洗錢防制法第 2 條第 1 款或第 2 款之洗錢犯罪之構成要件行為<sup>148</sup>。

2. 從洗錢行為之本質及洗錢之立法目的、保護法益而言，有以下之看法：

(1) 未合法化犯罪所得或利益之來源，而能一目了然來源之不法性，即非洗錢防制法所規範之對象：

洗錢防制法之制定，旨在規範特定重大犯罪不法所得之資金或財產，藉由洗錢行為，轉換成為合法來源之資金或財產，以切斷資金與當初犯罪行為之關連性，俾便於隱匿其犯罪行為或該資金不法來源或本質，以逃避追訴、處罰，故若非先有犯罪所得或利益，再加以掩飾或隱匿，而係取得犯罪所得或利益之犯罪手段，或未合法化犯罪所得或利益之來源，而能一目了然來源之不法性，即非洗錢防制法所規範之對象<sup>149</sup>。

(2) 掩飾、隱匿之行為，須旨在避免追訴、處罰而使其所得財物或利益之來源

---

年女子常業詐欺犯行有關「使人將本人或第三人之物交付」之行為，本為詐欺取財犯罪行為的一部分，並非另為掩飾或隱匿犯罪所得財物或財產上利益之行為。且被害人就其匯款之郵局、銀行活期儲蓄存款帳戶之戶名、帳號，均知之甚詳。換言之，該筆詐欺取財所得之款項匯入朱榮結提供之郵局、銀行活期儲蓄存款帳戶後，並未產生掩飾或隱匿「重大犯罪所得財物或財產上利益」之效果，偵查機關隨時均能發現該帳戶係詐欺取財之犯罪行為人供被害人匯款之用，惟一能掩飾或隱匿者，乃「誰是犯罪行為人」，顯然並不符合洗錢防制法第二條規定之洗錢行為。台灣高等法院 93 年度上重訴字 4 號：「陳錫祺」及另名不詳姓名成年女子利用朱榮結提供之郵局、銀行帳戶作為被害人匯款之用，本身既非洗錢防制法第二條第一、二款規定之洗錢行為，尤難論被告以洗錢防制法之罪，關於上開被害人匯款至朱榮結帳戶部分，應變更法條論被告以幫助詐欺罪已如前述，至於公訴意旨所指被害人楊天頻於九十二年二月二十五日匯款七萬二千元至朱榮結帳戶有誤（該七萬二千元係匯至案外人黃育智帳戶，而黃育智帳戶無事證明與被告有關），被告此節犯罪不能證明部分，公訴意旨認與前開論罪部分有實質上一罪關係，按審判不可分原則，不另為無罪之諭知。被告提供帳戶供常業詐欺集團之用，而該等詐欺集團利用所被告之人頭帳戶，要求被害人將款項直接匯入該帳戶中，其行為本即係該常業詐欺集團為實施其詐欺行為之犯罪手段，即詐欺行為構成要件中「使人將本人之物交付」之取財行為，並非於取得財物後，另為掩飾、隱匿其詐欺所得之行為，才轉入該人頭帳戶，本非洗錢防制法第二條所規範之洗錢行為。」

<sup>148</sup>台灣高等法院 94 年度上訴字 296 號判決：「查被告提供帳戶予他人流通之行為，並非洗錢防制法第二條第一款規定之「掩飾或隱匿因自己重大犯罪所得財物或財產上之利益者」或同條第二款規定之「掩飾他人因重大犯罪所得財物或財產上之利益者」之洗錢犯罪之構成要件行為。蓋被告本案行為能被評價成立犯罪者，僅係其交付帳戶物件予他人之行為而已，且於其提供交付帳戶物件時，就其提供之帳戶物件而言，尚無所謂之常業詐欺之重大犯罪存在，則其提供交付帳戶物件行為自難認屬上引法條所稱之「掩飾」或「隱匿」行為（尚無常業詐欺重大犯罪所得財物可資掩飾、隱匿），所謂之「掩飾」、「隱匿」，應係指實施常業詐欺之人告知被害人將金錢轉入指定之帳戶並利用該等帳戶洗錢之行為。又由於無證據證明被告有參與某犯罪集團之常業詐欺犯行之構成要件犯行，亦無證據證明其有出面領得詐得款項之行為，檢察官之起訴書及移送併辦意旨亦認被告僅有交付帳戶物件之行為，自尚難認被告有將實施常業詐欺犯行之人所為之常業詐欺犯行及「掩飾、隱匿」之洗錢犯罪構成要件行為視為自己犯行之自己共同犯罪之意思，僅能認被告係基於幫助之不確定犯意而為交付帳戶物件之行為。」

<sup>149</sup>台灣高等法院 94 年度上訴字第 922 號判決。

合法化，或改變該財物或利益之本質之犯意：

洗錢防制法第2條第1款之洗錢行為，除利用不知情之合法管道（如金融機關）所為之典型行為外，固尚有其他掩飾、藏匿犯特定重大犯罪所得財產或利益之行為，但仍須有旨在避免追訴、處罰而使其所得財物或利益之來源合法化，或改變該財物或利益之本質之犯意，始克相當。而被告販賣自己帳戶供犯罪集團提領被害人所匯款項之用，其目的在順利取得贓款、逃避警方或被害人之追查，並無使該贓款來源合法化或改變該財產或利益性質之作用，核與洗錢防制法之規範目的有間<sup>150</sup>。

（二）認為成立洗錢罪之見解：

被告提供帳戶之行為，已為洗錢防制法第二條之掩飾他人重大罪所得財物或財產上利益之「掩飾」行為，支持此說之判決有台灣高等法院高雄分院93年度上訴字第326號、台灣高等法院台中分院92年度金上訴字第1303號判決，而該等判決之理由分別如下：「查金融帳戶為個人理財之工具，申請開設金融帳戶並無任何特殊之限制，一般民眾皆能自由申請開戶，並得同時在不同金融機構申請多數存款帳戶使用，乃眾所週知之事實。依一般人之社會生活經驗，倘係合法收入，本可自行向金融行庫開戶使用，而無向他人購買帳戶之必要。苟見陌生人不以自己名義申請開戶，而向不特定人蒐集、收購他人之金融機構帳戶使用，衡情應能懷疑收購帳戶之人目的在於掩飾犯罪所得之錢財。而被告既不知悉向其收購帳戶者之真實姓名、年籍、住居所、聯絡電話等資料，業經其供認在卷，竟輕易同意出售金融機構帳戶予此人使用，並收受報酬，顯見其早已預見所出售之帳戶將供他人掩飾重大犯罪所得財物，而不違反其本意，自有洗錢之不確定故意；惟按被告提供帳戶供犯罪所得者存領款項，已參與「掩飾」之構成要件行為，應成立共同正犯<sup>151</sup>。」、「被告將其帳戶、存摺及提款卡交付

<sup>150</sup>台灣高等法院台中分院93年度金上訴字第1908號、92年度金上訴字第2369號。台灣高等法院台中分院93年度金上訴字第1908號：「洗錢防制法之制定，旨在規範特定重大犯罪不法所得之資金或財產，藉由洗錢行為，轉換成為合法來源之資金或財產，以切斷資金與當初犯罪行為之關連性，俾便於隱匿其犯罪行為或該資金不法來源或本質，以逃避追訴、處罰。該法之制定背景，主要係針對預防鉅額贓款，經由洗錢行為轉變為合法來源，造成資金流向之中斷，使偵查機關無法藉由資金之流向，追查不法前行為之犯罪行為人。足見其所保護之法益為國家對特定重大犯罪之追訴及處罰，此觀該法第一條已明定：「為防制洗錢，追查犯罪，特制定本法」，而對不法之前行為其所侵害之一般法益，因已有該當各行為之構成要件加以保護，自非該法之立法目的甚明。又該法第二條第一款之洗錢行為，除利用不知情之合法管道（如金融機關）所為之典型行為外，固尚有其他掩飾、藏匿犯特定重大犯罪所得財產或利益之行為，但仍須有旨在避免追訴、處罰而使其所得財物或利益之來源合法化，或改變該財物或利益之本質之犯意，始克相當（最高法院九十二年度台上字第三六三九號判決參照）。就本件而言，被告販售自己之帳戶供犯罪集團提領被害人所匯款項之用，其目的在順利取得贓款、逃避警方或被害人之追查，並無使該贓款來源合法化或改變該財物或利益性質之作用，核與洗錢防制法之規範目的有間，尚難以洗錢罪相繩。」

<sup>151</sup>台灣高等法院高雄分院93年度上訴字第326號判決：「查金融帳戶為個人理財之工具，申請開設金融帳戶並無任何特殊之限制，一般民眾皆能自由申請開戶，並得同時在不同金融機構申請多數存款帳戶使用，乃眾所週知之事實。依一般人之社會生活經驗，倘係合法收入，本可自行向金融行庫開戶使用，而無向他人購買帳戶之必要。苟見陌生人不以自己名義申請開戶，而向不特定人蒐集、收購他人之金融機構帳戶使用，衡情應能懷疑收購帳戶之人目的在於掩飾犯罪所得之錢財。而被告既不知悉向其收購帳戶者之真實姓名、年籍、住居所、聯絡電話等資料，業經其供認在卷，竟輕易同

他人使用，而該詐欺集團以簡訊詐使被害人陷於錯誤後，始依提示匯款至被告提供之帳戶，以掩飾、隱匿詐得之財物，自屬洗錢之行為」。

四、若認為成立洗錢罪，則提供人頭帳戶之人是洗錢罪之正犯或幫助犯

(一) 成立洗錢罪之正犯<sup>152</sup>：

1. 提供帳戶之行為，已構成洗錢防制法第 2 條之「掩飾」行為：

在客觀上，被告提供帳戶存摺、提款卡及密碼供詐欺集團向被害人詐騙金錢後，再提領詐得款項之行為，堪認係掩飾或隱匿因他人重大犯罪所得財物或財產上利益，並藉以逃避警察追緝之行為<sup>153</sup>；在主觀上，被告既預見他人向其收購帳戶，可能作為常業詐欺犯罪被害人匯款之用，並作為掩飾或隱匿詐欺集團犯罪所得款項之用，而該他人嗣後利用該帳戶，實施常業詐欺犯罪，並藉該帳戶掩飾犯罪所得，又不違被告本意，顯有掩飾他人重大犯罪所得之不確定故意<sup>154</sup>。故被告提供帳戶供犯罪者存領款項，既已直接掩飾他人犯重大犯罪所得，而與洗錢防制法第 2 條之「掩飾」構成要件相當，自屬正犯，要無再以幫助洗錢罪之餘地<sup>155</sup>。

2. 提供帳戶之行為，係為掩飾「他人」常業詐欺所得財物之行為：

被告將其在金融機構之帳戶，連同存摺及金融卡提供他人，供常業詐欺集團將詐欺所得財物過帳之用，其行為應屬洗錢防制法第 2 條第 2 款為他人掩飾犯罪所得之構成要件行為。又洗錢防制法於 2003 年 2 月 6 日修正公布，該法第 2 條立法理由為<sup>156</sup>：「為明確區分犯罪行為人之洗錢行為之態樣係為自己或為他人，而以第 2 條第 1 款規範犯罪者將自己犯罪所得加以漂白之行為，至於他人

---

意出售金融機構帳戶予此人使用，並收受報酬，顯見其早已預見所出售之帳戶將供他人掩飾重大犯罪所得財物，而不違反其本意，自有洗錢之不確定故意；惟按被告提供帳戶供犯罪所得者存領款項，已參與「掩飾」之構成要件行為，應成立共同正犯。」

<sup>152</sup>支持此說之判決有：台灣高等法院台中分院 92 年度金上訴字 1081 號、台灣高等法院台中分院 93 年度金上訴字第 2107 號判決、台灣高等法院台中分院 92 年度金上訴字第 1303 號判決、台灣高等法院 92 年度金上訴字第 1988 號判決、台灣高等法院高雄分院 93 年度上訴字第 874 號判決、台灣高等法院高雄分院 93 年度上訴字第 326 號判決、台灣高等法院高雄分院 93 年度上訴字第 409 號判決、台灣高等法院 93 年度上訴字第 2759 號判決。

<sup>153</sup>台灣高等法院高雄分院 93 年度上訴字第 874 號判決：「被告提供帳戶存摺、提款卡及密碼供詐欺集團向被害人詐騙金錢後，在提領詐得款項之行為，堪認係掩飾或隱匿因他人重大犯罪所得財物或財產上利益之行為，應為從事洗錢之構成要件之行為，自屬正犯。台灣高等法院台中分院 92 年度金上訴字第 1303 號判決：被告交付存摺、提款卡及密碼，供常業詐欺集團罪為犯罪之用，藉以掩飾、隱匿所得財物，逃避檢察查緝，係犯掩飾他人重大犯罪所得財物之罪。」

<sup>154</sup>台灣高等法院台中分院 93 年度金上訴字第 2107 號判決：「被告既預見他人向其收購帳戶，可能作為常業詐欺犯罪被害人匯款之用，並作為掩飾或隱匿詐欺集團犯罪所得款項之用，而該他人嗣後利用該帳戶，實施常業詐欺犯罪，並藉該帳戶掩飾犯罪所得，又不違被告本意，核其所為係掩飾他人因重大犯罪所得財物之罪。」

<sup>155</sup>台灣高等法院 92 年度金上訴字第 1988 號判決：「被告提供帳戶予他人為詐欺犯罪使用，既已直接掩飾他人犯重大犯罪所得，而該當洗錢防制法之為他人洗錢行為，要無再以幫助洗錢論罪之餘地。台灣高等法院高雄分院 93 年度上訴字第 326 號判決：被告提供帳戶供犯罪者存領款項，已參與洗錢防制法第二條之『掩飾』構成要件，應成立正犯。台灣高等法院 93 年度上訴字第 2759 號判決：被告將其在金融機構之帳戶，連同存摺及金融卡提供他人，供常業詐欺集團將詐欺所得財物過帳之用，其行為應屬洗錢防制法第二條第二款為他人掩飾犯罪所得之構成要件行為。」

<sup>156</sup>參立法院議案關係文書，院總 1692 號政府提案第 8848 號，案由：行政院函請審議「洗錢防制法修正草案」案。

幫助重大犯罪者漂白黑錢之行為，則規範於同法第二條第二款」。是同法第 2 條第 2 款之掩飾他人重大犯罪所得財物之行為，本質上已含有幫助他人洗錢之性質，從而，被告提供帳戶為他人掩飾常業詐欺所得財物之行為，自應以同法第 9 條第 2 項論處<sup>157</sup>。

(二) 成立洗錢之幫助犯<sup>158</sup>：

1. 此說法之主要論點有：

(1) 提供帳戶之行為，並非直接掩飾、隱匿因他人重大犯罪所得：

被告提供之帳戶為詐欺集團做為被害人匯入款項之用，則該詐欺集團向被害人詐騙金前後再行提領之行為，應屬洗錢防制法所稱掩飾、隱匿因他人重大犯罪所得財物或財產上利益之行為<sup>159</sup>。而被告單純提供帳戶供人使用之行為，並不同於向被害人施以欺罔之詐術行為，亦非等同於使用上開帳戶掩飾重大犯罪所得之洗錢行為<sup>160</sup>，即被告並未實施洗錢防制法第 2 條洗錢犯罪之構成要件行為。

(2) 行為人提供帳戶之時，尚無重大犯罪之存在：

被告於交付帳戶物件予他人之時，就其提供之帳戶物件而言，尚無所謂之常業詐欺之重大犯罪存在，則其提供交付帳戶物件行為自難認屬上引法條所稱之「掩飾」或「隱匿」行為，即尚無常業詐欺重大犯罪所得財物可資掩飾、隱匿，故被告單純提供帳戶予他人流通之行為，並非洗錢防制法第 2 條第 1 款或第 2 款之洗錢犯罪之構成要件行為<sup>161</sup>。

2. 認為提供帳戶之行為成立幫助洗錢幫助犯，是幫助「自己」或「他人」掩飾犯罪所得，又有不同見解，分述如下：

(1) 成立幫助「自己」洗錢罪<sup>162</sup>：

被告提供之帳戶遭他人以詐欺手法使被害人將款項轉帳匯入該等帳戶內，則利用該等帳戶掩飾常業詐欺犯罪所得財物之「他人」，應係利用該等帳戶掩飾其「自己」常業詐欺犯罪所得財物，而此利用該等帳戶掩飾其「自己」常業詐欺犯罪所得財物之正犯應成立之罪名，係洗錢防制法第

<sup>157</sup> 台灣高等法院 93 年度上訴字第 2759 號判決。

<sup>158</sup> 贊成此論點之判決有：台灣高等法院 92 年度金上訴字第 1748 號判決、台灣高等法院高雄分院 93 年度上訴字第 924 號判決、台灣高等法院 94 年度上訴字第 1489 號判決、台灣高等法院 94 年度上訴字 296 號判決、台灣高等法院 91 年度上訴字第 2263 號判決、台灣高等法院 92 年度上訴字第 862 號判決。

<sup>159</sup> 台灣高等法院 92 年度金上訴字第 1748 號判決：「被告提供之帳戶為詐欺集團做為被害人匯入款項之用，則該詐欺集團向被害人詐騙金前後再行提領之行為，應屬洗錢防制法所稱掩飾、隱匿因他人重大犯罪所得財物或財產上利益之行為。而被告基於不確定故意提供該等帳戶供詐欺集團洗錢之用，應係幫助他人洗錢之行為。」

<sup>160</sup> 台灣高等法院高雄分院 93 年度上訴字第 924 號判決：「被告單純提供自己及他人帳戶供人使用之行為，並不同於向被害人施以欺罔之詐術行為，亦非等同於使用上開帳戶掩飾重大犯罪所得之洗錢行為，且亦無證據證明其有參與常業詐欺及洗錢犯行之構成要件，是被告所為係犯幫助常業詐欺及洗錢防制法第九條第二項幫助他人洗錢罪」

<sup>161</sup> 台灣高等法院 94 年度上訴字 296 號判決。

<sup>162</sup> 贊成此說法之判決有：台灣高等法院 94 年度上訴字 296 號判決、台灣高等法院 93 年度上訴字第 2973 號判決、台灣高等法院 94 年度上訴字第 1489 號判決。

9 條第 1 項之掩飾因自己重大犯罪所得財物罪。而提供帳戶予他人使用而構成洗錢犯罪幫助犯之行為人，則應從屬於正犯之犯罪，成立幫助掩飾因自己重大犯罪所得財物罪，並非成立法定刑度較正犯為重之幫助掩飾他人因重大犯罪所得財物罪<sup>163</sup>。

(2) 成立幫助「他人」洗錢罪<sup>164</sup>：

被告提供之帳戶為詐欺集團做為被害人匯入款項之用，則該詐欺集團向被害人詐騙金錢後再行提領之行為，應屬洗錢防制法所稱掩飾、隱匿因他人重大犯罪所得財物或財產上利益之行為。而被告基於不確定故意提供該等帳戶供詐欺集團洗錢之用，應係幫助他人洗錢之行為<sup>165</sup>。

## 五、論罪與適用法條

以上分項說明法律爭點之不同見解，現在進一步整理、歸納以上實務法院判決對於出賣帳戶行為人如何論罪及適用法條之問題，有以下之不同情形：

- (一) 若證據不能足以證明使用人頭帳戶從事詐欺之行為人有為常業詐欺之行為，亦無法證明帳戶名義人與施用詐術之人，有共同犯意之聯絡，則僅能論以幫助詐欺取財之罪<sup>166</sup>。
- (二) 倘使能證明利用人頭帳戶者從事詐欺之行為者為常業詐欺之人，則依法院認為提供帳戶之行為是否為洗錢之構成要件行為，而有所區別：
  1. 認為是洗錢行為，有二種論罪情形：
    - (1) 部份法院認為僅論以涉犯洗錢防制法之掩飾他人重大犯罪所得罪<sup>167</sup>。
    - (2) 另部份法院則認為，提供帳戶者應論以常業幫助犯及洗錢防制法之正犯<sup>168</sup>。
  2. 認為提供帳戶之行為，非洗錢行為之構成要件，則又區分為以下四種論罪的型態：
    - (1) 僅論以常業詐欺幫助犯<sup>169</sup>。
    - (2) 僅論以洗錢防制法第 9 條第 1 項之幫助犯<sup>170</sup>。
    - (3) 被告提供帳戶之行為，應涉犯常業詐欺幫助犯及違反洗錢防制法第 9 條第 1 項之幫助犯<sup>171</sup>。
    - (4) 被告提供帳戶之行為，應涉犯常業詐欺幫助犯及違反洗錢防制法第 9 條第

<sup>163</sup> 台灣高等法院 93 年度上訴字第 2973 號判決、台灣高等法院 94 年度上訴字 296 號判決。

<sup>164</sup> 贊成此說法之判決有：台灣高等法院 92 年度金上訴字第 1748 號判決、台灣高等法院高雄分院 93 年度上訴字第 924 號判決、台灣高等法院 91 年度上訴字第 2263 號判決、台灣高等法院 92 年度上訴字第 862 號判決。

<sup>165</sup> 台灣高等法院 92 年度金上訴字第 1748 號判決

<sup>166</sup> 台灣高等法院台中分院 94 年度金訴字第 311 號、93 年度金訴字第 1493 及 1494 號、93 年度上易字第 1139 號、台灣高等法院高雄分院 93 年度上訴字第 746 號、台灣高等法院 94 年度上訴字第 922 號。

<sup>167</sup> 台灣高等法院台中分院 92 年度金訴字第 1081 號、92 年度金訴字第 1303 號、92 年度上訴字第 701 號、台灣高等法院高雄分院 93 年度上訴字第 326 號

<sup>168</sup> 台灣高等法院台中分院 92 年度金訴字第 2107 號、92 年度金訴字第 1988 號、92 年度上訴字第 882 號、台灣台中地方法院 91 年度易字第 1138 號、台灣高等法院高雄分院 93 年度上訴字第 874 號、台灣高等法院高雄分院 93 年度上訴字第 409 號、台灣高等法院 93 年度商訴字第 2759 號。

<sup>169</sup> 台灣高等法院台中分院 93 年度金訴字第 1314 號、92 年度金訴字第 2369 號。

<sup>170</sup> 台灣高等法院 93 年度上訴字 2973 號、94 年度上訴字 1489 號。

<sup>171</sup> 台灣高等法院 93 年度上訴字 2973 號、94 年度上訴字第 296 號、94 年度上訴字第 4 號。

## 2 項之幫助犯<sup>172</sup>。

### 六、評釋

在審判實務上，對於被告之犯罪事實行為，需依卷內之證據來認定之，法院再依據證據認定之事實來適用之法條。故單純提供帳戶予他人，而該他人用以從事詐騙行為，則提供帳戶之行為人到底應如何論罪，因提供帳戶行為人於各案之涉案情節並不相同，故不能一概而論，故以下本文提出個人淺見。

(一) 提供帳戶之行為，因卷內證據資料證明之程度不同，而有不同之認定：

按行為人業已參與實施犯罪構成要件之行為，或以自己共同犯罪之意思，參與實施犯罪構成要件以外之行為者，均為共同正犯，此乃實務上一致認為正犯之定義<sup>173</sup>。而就提供帳戶予他人使用之行為人而言，就其所辯稱：僅是提供帳戶，並不知悉用來從事不法行為等語，是否可信，仍應依證據加以認定。換言之，倘若卷證資料僅能證明被告僅提供帳戶，並未直接參與對被害人實施犯罪構成要件之行為，且易無證據證明被告係為自己之利益而有共同犯罪之犯意聯絡，則在此情況下，始有討論單純提供帳戶者是否另涉有幫助犯或觸犯其他法律之必要，否則直接論以犯罪之正犯即可。

再按刑法之幫助犯，必以幫助他人犯罪之意思而參與犯罪，其所參與者又為構成要件以外之行為<sup>174</sup>。幫助犯成立之要件，除需有幫助行為外，須行為人有幫助之故意，而其故意內涵，除需行為人對其所實施幫助行為有違法性之認識或有認識之可能外，尚須對於正犯所實施犯罪行為有具體之認識或有認識之可能性，亦即從犯對於正犯所實施之全部犯罪構成要件該當性之時應有所認識或有認識之可能性。又按幫助他人犯罪者，為從犯；從犯之處罰，得按正犯之刑減輕之，刑法第 30 條第 1 項前段、第 2 項定有明文。是我國刑法之幫助犯，並無獨立性，而係從屬於正犯之犯罪而成立。而按金融帳戶為個人之理財工具，一般民眾均可辦理金融帳戶存摺使用，且得同時在不同金融機構申請多數存款帳戶使用，實無借用他人帳戶使用之必要。加之，金融存款帳戶，攸關存戶個人財產權益之保障，其專有性甚高。一般人均有妥為保管及防止任意使用之認識。故衡諸常理，若非與本人有密切關係者，不可能出借個人帳戶，縱有交付個人帳戶予他人使用之特殊情形，亦必會先行瞭解他人使用帳戶之目的始行提供。再者，以簡訊通知中獎、刮刮樂或其他類似之不法詐騙份子，為掩飾其等不法行徑以避免執法人員循線查緝，經常利用他人存款帳戶、印章、提款卡以確保犯罪所得，類此案件在社會上層出不窮，亦屢經報章雜誌及其他新聞媒體再三披露，避免此等專有性甚高之物品被不明人士利用為與財產有關之犯罪工具，亦為一般生活認知所應有之認識。

而實務上被告將帳戶、存摺等資料提供予不認識之他人使用，多係因缺錢花用，又被告於交付前開帳戶資料時，尚無證據證明其知悉他人用以詐欺取財

<sup>172</sup> 台灣高等法院台中分院 92 年度金訴字第 1748 號、92 年度金訴字第 2378 號、台灣高等法院高雄分院 93 年度上訴字第 924 號、台灣高等法院 92 年度上訴字第 862 號。

<sup>173</sup> 大法官會議解釋第 109 號。

<sup>174</sup> 最高法院 25 年上字第 2253 號判例。

犯罪之用（如已明知而為，即成立共同正犯）。然其已可預見以若干之代價將上開帳戶提供不認識之第三人使用，將被不法之徒用於犯罪贓款之匯入流出，竟不違反其本意，猶仍將上開帳戶、提款卡等物出售詐欺集團成員，容任詐欺行為之發生，其有幫助他人詐欺之不確定故意至為明確。從而，被告提供帳戶予他人，而該他人將該帳戶作為詐騙被害人匯款帳戶之用的情形，在審判實務上，係以幫助詐欺罪來論處，若能證明詐欺集團有多次施用詐術之常業行為，則認被告為常業詐欺之幫助犯，尚屬合理。然有不少情況，是被告交付帳戶、存摺等資料之他人，係從事詐欺以外之不法行為，如：擄人勒贖、恐嚇取財等，則被告對於正犯所實施犯罪行為是否有具體之認識或能否有認識之可能性，即非無疑。此種類型之提供帳戶的幫助行為，確為實務上值得探討之部分。

承接前面之問題，該問題之爭點在於，提供帳戶予他人者，若無證據證明其有參與正犯之犯罪行為之構成要件，亦無法認定其確有以自己犯罪之意思，而提供帳戶之助力行為，則該提供帳戶之行為人，無法論以正犯從事犯罪行為之共同正犯，則是否能逕以幫助犯之地位予以處罰，不能一以蓋之。易言之，倘能證明提供帳戶之人對於正犯所實施之犯罪行為有認識之可能性，則提供帳戶之人以正犯行為之幫助犯罪責相繩，應無不妥；然而，倘若在無法證明提供帳戶者對於正犯所實施之犯罪行為有認識可能性之情形下，則該提供帳戶之助力行為，既無法論以實施犯罪行為之正犯，亦不符合幫助犯之構成要件時，則此種單純提供帳戶等資料的行為，是否即無其他法律可加以規範，則需深入討論。

(二)「單純提供帳戶，以利正犯用以收取犯罪所得財物」之行為，是否能以「洗錢防制法」之相關規定來處罰：

單純提供帳戶供他人從事不法行為，是否能以洗錢防制法之相關規定來論處，探討此法律爭議首要之務，在於需先探究該提供帳戶之行為是否屬於洗錢防制法之「洗錢行為」。按洗錢防制法第2條有規定：「本法所稱洗錢，係指下列行為：一、掩飾或隱匿因自己重大犯罪所得財物或財產上之利益者。二、掩飾、收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益者」，換言之，即適用該法之二大前提：第一，應先認定提供帳戶之行為，是否符合該條規定「掩飾」、「隱匿」之構成要件而斷；第二，行為人掩飾、隱匿財產或利益，必須是因「重大犯罪」所得。然而關於第二個要件，是否為「重大犯罪」，要以洗錢防制法第3條第1項所列舉者為其範圍，此部分並無太大爭議。然較有爭議在於「單純提供帳戶，以利正犯用以收取犯罪所得財物」之行為，是否符合前該第一個「洗錢」之定義。

在法學方法論上之法律解釋，時至今日，仍是以德國學者 Friedrich Carl von Savigny<sup>175</sup>所提出的文義解釋、歷史解釋、體系解釋及目的論解釋<sup>176</sup>等四種方法

<sup>175</sup>甘添貴，體系刑法各論第一卷侵害個人專屬法益之犯罪，第10頁，自版，1999年9月初版。

<sup>176</sup>「文義解釋」，指依照法文用語之文義及通常使用方式而為解釋。「歷史解釋」：參照立法文獻等資料來探究法律規範之原意。「體系解釋」：以法律條文在法律體系上之地位，即依其編章條節項款之前後關連位置，或相關法條之法意，闡明規範意旨之解釋方法。「目的解釋」：係指以法律規範目的，

為主要解釋方式，而此種方式並非相互排斥，亦並非均要全部加以運用才能達成法律解釋之目的，而是依據所要解釋的法律概念，透過適當的方法加以運用，相輔相成，以達正確解釋法律的目標<sup>177</sup>。又法律解釋方法之順序，文義解釋具有初步優先性，在文義解釋的解果有多種解釋可能性時，則輔以體系解釋、歷史解釋及目的解釋以達適用法律之正確性。

本文於此，先以文義解釋方法討論之，即學說上對於洗錢防制法第2條所稱「掩飾」、「隱匿」之見解，李傑清<sup>178</sup>認為：掩飾係指操作任何事實上或法律上之行為，足以讓人無法覺察真正所在之行為；隱匿則指依刑法第165條湮滅刑事罪證罪之解釋為「隱蔽藏匿使其不易為人發現」之意義外，尚應擴及以消極之事實或法律行為顯示目標物「似乎不存在」。又如蘇南桓<sup>179</sup>謂掩飾即偽裝財產之真實性質、來源、所在地、所有權等之謂，亦即積極加工之行為，以偽飾該財產免遭察覺；另所謂隱匿，乃積極藏匿使不易發覺之謂。如依前揭文義之解釋，即將重大犯罪所得匯入或移轉至被告提供之人頭帳戶，應屬「偽裝財產真實所有權」及「足以讓人無法覺察真正所在」的「掩飾重大犯罪所得」行為，而應符合洗錢防制法之洗錢定義。

再從歷史解釋之方法討論，即從立法史、立法資料探求立法之理由為何，來認定「單純提供帳戶，以利正犯用以收取犯罪所得財物」之行為，是否原為洗錢防制法所欲規範之範疇。所謂洗錢，依洗錢防制法第2條規定係以掩飾或隱匿因自己或他人重大犯罪所得財物或財產上利益為其要件，而無論掩飾或隱匿行為，均為行為人於完成犯罪行為後，為利用或確保此一前行為之不法犯罪所得財物或財產上利益所為之另一行為，應屬一種處分犯罪所得財物或財產上利益之行為（處分贓物之行為），此觀諸同條第2款將收受、搬運、寄藏、故買或牙保他人因重大犯罪所得財物或財產上利益等贓物之犯罪行為，亦同列為洗錢行為甚明。就行為人而言，此種處分贓物行為，原係不罰之後行為之一種。而所謂不罰之後行為，係行為人於完成其犯罪後，對於其所侵害法益之另一次侵害，不另構成犯罪之情形，即前行為與後行為間並無行為發展之階段關係，僅處罰前行為即已兼及後行為者，該後行為即為前行為所吸收，不再視其為獨立之犯罪，例如：將竊盜或搶奪取得之財物據為己有或出賣等行為，不能再論以侵占罪等。而洗錢行為（自己洗錢），係指行為人完成犯罪行為後，對於犯罪所得財物或財產上利益所另為掩飾或隱匿等行為，該行為在刑罰體系上原係不罰之後行為，然因特殊社會防衛之需要（為防制洗錢，追查重大犯罪，洗錢防制法第1條參照），始予以刑罰化。又洗錢防制法於2003年2月6日修正公布<sup>180</sup>，該法第2條立法理由為：「為明確區分犯罪行為人之洗錢行為之態樣係為自己或為他人，而以第二條第一款規範犯罪者將自己犯罪所得加以漂白之行為，至於他人幫助重大犯罪者漂白黑錢之行為，則

---

闡釋法律疑義之方法。參楊仁壽，法學方法論，第123、130、154頁，三民書局，1994年。及黃茂榮，法學方法與現代民法，第308頁，自版，1993年。

<sup>177</sup> 莊哲維，刑事法規解釋之問題研究—兼論刑法秘密罪之解釋，

<http://www.ntpu.edu.tw/law/paper/01/2001a/8971502a.PDF>，(2006/Mar/13)。

<sup>178</sup> 李傑清，「洗錢罪保護法益及處罰」，月旦法學，第115期，第23頁，2004年11月。

<sup>179</sup> 蘇南桓，洗錢防制理論與實務，第200頁，自版，1997年10月初版。

<sup>180</sup> 參前揭註131。

規範於同法第二條第二款。」，是同法第 2 條第 2 款之掩飾他人重大犯罪所得財物之行為，本質上已含有幫助他人洗錢之性質。從而，綜觀上開立法、修法之原始資料可知，若將金融機構之帳戶，連同存摺及金融卡提供他人，供他人從事常業詐欺等重大犯罪行為，其行為應屬洗錢防制法之為他人掩飾犯罪所得之構成要件行為，是以，提供帳戶為他人掩飾重大犯罪所得財物之行為，自應以同法第 9 條第 2 項論處，始符合立法之原意及目的。又最高法院 92 年度台上字第 5781 號、93 年度台上字第 4967 號及 94 年度台非字第 185 號判決均同此是認，即最高法院分別認為：「上訴人可預見該『陳先生』收購帳戶，係供彼等常業詐欺犯罪之被害人匯款，並掩飾或隱匿犯罪所得款項之用，猶提供帳戶，幫助彼等遂行常業詐欺犯罪，並掩飾該重大犯罪所得財物犯行，核屬刑法第三百四十條常業詐欺罪之幫助犯及洗錢防制法第二條第一款掩飾他人重大犯罪所得財物之洗錢罪」<sup>181</sup>、「被告明知交付郵局存簿、金融卡予他人，將掩飾他人常業詐欺所得之財物，乃為達個人利益，而將郵政存簿、金融卡交付予『長腳』，其對掩飾他人常業詐欺所得之財物之事實，顯預見其發生，而其發生並不違背其本意，就掩飾詐欺集團常業詐欺所得財物之行為，係犯洗錢防制法之洗錢罪」、「被告可預見提供自己帳戶予他人使用，足供他人掩飾或隱匿其犯常業詐欺取財等重大犯罪所得財物之用，竟仍不違反其本意，因缺錢花用，而基於幫助他人實施常業詐欺之不確定故意，以新台幣二千五百元之代價，將其所有之帳戶存摺、提款卡、身分證、印章等物賣給他人，則被告之幫助該犯罪集團掩飾、隱匿犯罪所得之行為，除犯有幫助常業詐欺外，尚有違反洗錢防制法之規定」等情，足以認定最高法院亦支持「單純提供帳戶，以利正犯用以收取犯罪所得財物」之行為，係構成掩飾、隱匿他人重大犯所得或利益之看法。

至於台灣高等法院、台灣高等法院台中分院部分法院否認「單純提供帳戶，以利用正犯用以收取犯罪所得財物」之行為，構成洗錢防制法第 2 條所為「掩飾」、「隱匿」之構成要件，其理由不外以下幾點：第一點，單純提供帳戶之行為，無證據證明有掩飾他人重大罪之財產所得或利益。第二點，提供帳戶供詐欺集團之被害人匯入帳戶之用，該等行為原係詐欺取財行為之一部分，並非另為掩飾、隱匿詐欺集團犯罪所得之行為。第三點，行為人提供帳戶之時，尚無重大犯罪之行為存在，則自無重大犯罪所得財物可資掩飾、隱匿。第四點，掩飾、隱匿之行為，須旨在避免追訴、處罰而使其所得財物或利益之來源合法化，或改變該財物或利益之本質之犯意。而單純販賣帳戶供犯罪集團提領被害人所匯款項之用，其目的在順利取得贓款、逃避警方或被害人

<sup>181</sup>最高法院 92 年度台上字第 5781 號判決：「上訴人所為將其所申請之郵局及銀行共九家之存摺、提款卡及密碼，以一本一千元（新台幣）之代價，出售提供予真實姓名不詳之成年男子「陳先生」使用之供詞，參酌被害人陳秀鳳之指述，以及卷附存簿更換密碼資料、郵局掛失止付申請書、上開帳戶交易明細資料及郵政國內匯款執據與卷內其他證據調查之結果，本於審理所得心證，認該「陳先生」與自稱「康才華」之成年男子等人，均屬常業詐騙集團之成員，共同基於為自己不法所有之犯意，以假中獎真詐財之方式，施用詐術，使被害人陳秀鳳及其他不特定被害人等多人陷於錯誤，而將本人之財物交付，應成立常業詐欺罪。上訴人可預見該「陳先生」收購帳戶，係供彼等常業詐欺犯罪之被害人匯款，並掩飾或隱匿犯罪所得款項之用，猶提供帳戶，幫助彼等遂行常業詐欺犯罪，並掩飾該重大犯罪所得財物犯行，核屬刑法第三百四十條常業詐欺罪之幫助犯及洗錢防制法第二條第一款掩飾他人重大犯罪所得財物之洗錢罪。」

追查，並無使該贓款來源合法化或改變該財產或利益性質之作用，核與洗錢防制法之規範目的有間。

然而，金融帳戶為個人理財之工具，申請開設金融帳戶並無任何特殊之限制，一般民眾皆能自由申請開戶，並得同時在不同金融機構申請多數存款帳戶使用，乃眾所週知之事實。依一般人之社會生活經驗，倘係合法收入，本可自行向金融行庫開戶使用，而無向他人購買帳戶之必要。苟見陌生人不以自己名義申請開戶，而向不特定人蒐集、收購他人之金融機構帳戶使用，衡情應能懷疑收購帳戶之人目的在於掩飾犯罪所得之錢財。倘行為人既不知悉向其收購帳戶者之真實姓名、年籍、住居所、聯絡電話等資料，竟輕易同意出售金融機構帳戶予此人使用，並收受報酬，顯見其早已預見所出售之帳戶將供他人掩飾重大犯罪所得財物，而不違反其本意，自有洗錢之不確定故意。再者，被告提供帳戶供犯罪所得者存領款項，不僅係正犯從事犯罪行為之一部分，亦已參與「掩飾」他人重大犯罪所得之構成要件行為，從而，上開第一、二點否認之理由，即非有據。

又洗錢防制法第2條2款之掩飾他人重大犯罪所得財物之行為，本質上已含有幫助他人洗錢之性質，已如前述。是此條款之規定，係幫助行為的獨立化處罰，換言之，即該款之行為本身之屬性，本為幫助犯之性質，僅因為立法目的之特殊性，而就罪責之部分，將之視為獨立之正犯為處罰，而不再依循傳統刑法從犯之理論來處理。是以，被告提供帳戶予他人後，他人始從事重大不法之犯罪行為，則此種行為於概念上即屬「事前之幫助行為」，猶如：被告以幫助他人犯罪之意思，提供一把西瓜刀予他人為殺人之行為，縱使他人於被告提供助力之時，尚無殺人之重大犯罪行為存在，然仍無礙於被告幫助殺人罪之成立。準此，即令行為人提供帳戶行為之時，尚無重大犯罪行為存在，然依前所述，洗錢防制法第2條第2款本即包含幫助犯行為之性質，是以提供帳戶之行為仍是構成該款之構成要件，並無疑問。惟前揭否定見解第三點之理由，認為因被告提供帳戶之時，尚無重大犯罪之行為存在，則自無重大犯罪所得財物可資掩飾、隱匿，從而，並無構成掩飾、隱匿他人重大犯罪所得之要件，顯係對法律適用及解釋之誤認。

另有部分法院依目的解釋之方法論認為：洗錢防制法之制定，旨在規範特定重大犯罪不法所得之資金或財產，藉由洗錢行為，轉換成為合法來源之資金或財產，以切斷資金與當初犯罪行為之關連性，俾便於隱匿其犯罪行為或該資金不法來源或本質，以逃避追訴、處罰。故認為行為人販賣自己帳戶供犯罪集團提領被害人所匯款項之用，其目的在順利取得贓款、逃避警方或被害人之追查，並無使該贓款來源合法化或改變該財產或利益性質之作用，核與洗錢防制法之規範目的有間，而認為不符合掩飾、隱匿他人重大犯罪所得之要件。然查，從前開文義解釋、歷史解釋，均足以認定「單純提供帳戶，以利正犯用以收取犯罪所得財物」之行為，確實已屬於洗錢防制法第2條第2款掩飾他人重大犯罪所得之構成要件行為，則該部份法院竟利用「目的之解釋」，加諸法條構成要件以外之限制，而認為該行為不符合該條款之規定，此種條文之解釋，是否允當，已非無疑。何況，重大犯罪行為人利用人頭帳戶從事不法行為，不僅「偽裝財產之真實所有權」，亦藉以切斷檢警依循人頭帳戶資料繼續查緝之可能，且重大犯

罪行為人利用人頭帳戶者所交付之存摺、提款卡等物，在他處任意提領犯罪所得之款項，以切斷資金與當初犯罪行為之關連性，此種種行為，在在均為達到逃避追訴、處罰之目的，難認被告提供帳戶之行為，尚未達掩飾、隱匿他人之重大罪行為的程度。從而，前開否定說第四點之理由，顯無充足之理由而確有瑕疵可指。

綜上所言，單純提供帳戶以利他人用以收取犯罪所得財物，不論該他人係從事常業詐欺或是洗錢防制法第3條第1項所列舉之重大犯罪，此提供帳戶之行為，即是掩飾「他人」重大犯罪所得財物之行為，亦符合洗錢防制法所規範之洗錢罪之構成要件。從而，此次修法將此種提供人頭帳戶之幫助犯性質之犯罪，提升為正犯之性質來處罰，並且提高法定刑，顯係藉由提高刑罰之手段，來遏止人頭帳戶不法使用之氾濫。而此刑罰之提高，亦應屬我國藉由查緝人頭帳戶犯罪來防制詐欺之防制策略。



## 四、從實證面檢驗犯罪防制策略對網路詐欺之成效

### 4.1 本章之研究方法

#### 一、事件研究法

利用「事件研究法」觀察特定犯罪防制政策之實施，是否會改變理性犯罪者之決策，進而影響所欲遏止之特定犯罪之犯罪量的變化。本文應用「事件研究法」的第一步驟，即是確定研究事件及「事件日」。本文所欲研究之事件，即「警示帳戶通報機制」、「非約定帳戶之轉帳限制」及「洗錢防制法第9條修法」三種犯罪防制之政策。而此三種防制政策實施之時點，分別為2003年7月、2005年6月1日、2003年8月6日。第二步驟，在確立本文研究之事件及「事件日」後，是針對研究事件做樣本選擇與觀察期間之設定。其中之觀察期間包括「事件期」、「估計期」之設定，本文所設定之「事件期」是指某一防制犯罪政策實施之當日及之後的一段期間；而「估計期」則是在防制犯罪政策實施之前的一段期間，此段時間是獨立於事件期間的，也就是不受研究事件影響干擾的一段時間。又本文觀察之「非約定帳戶之限制轉帳」事件，因發生時點較其他事件晚約將近二年，礙於研究時間、人力、經費及採集樣本是否足夠等諸多限制，此事件之觀察期間只能限於2005年12月31日為止，且三個事件研究之樣本資料之採集均亦截至2005年12月31日，故三個事件之觀察期間分別參如下圖4至圖6。「事件研究法」之第三步驟，即是對於本文研究目的所建立「此三種犯罪防制策略能有效降低網路詐欺犯罪之發生率」之假設，觀察「事件期」與「估計期」之犯罪量變化，進行統計分析以及數據之說明。

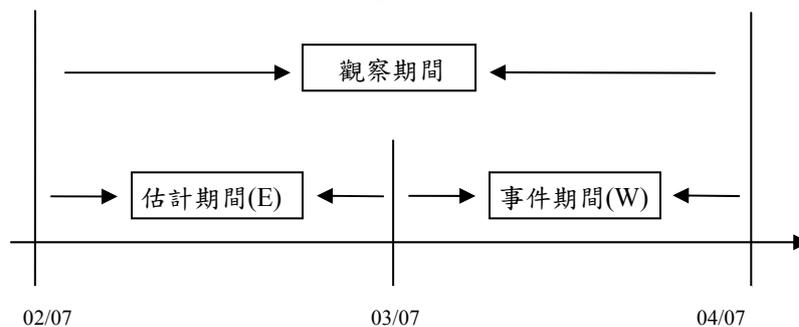


圖 5 「警示帳戶通報機制」事件之觀察期間

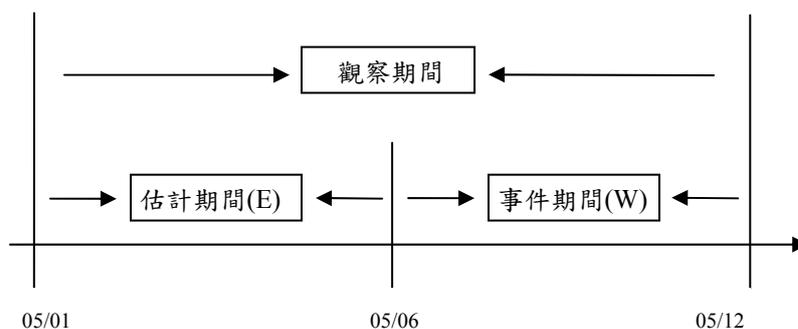


圖 6 「非約定帳戶之限制轉帳」事件之觀察期間

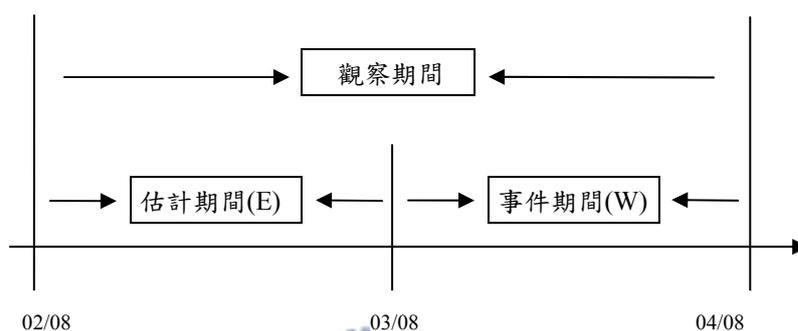


圖 7 「洗錢防制法第 9 條修法」事件之觀察期間

此外，本文利用事件研究法觀察「事件期」與「估計期」犯罪量變化之同時，亦借用統計學中之曼-惠特尼 U 檢驗法 (Mann-Whitney U Test)，來說明數據之分佈差異。Mann-Whitney U Test 屬於一種無母數統計，是利用誤差的概念。而 Mann-Whitney U Test，是適用在比較兩個隨機樣本之差異，例如：檢驗實驗組與控制組的實驗數據顯示兩組的結果是否有明顯差異。若經過檢定後之觀察值 (P 值) 小於 0.1 之臨界值，則這兩個樣本的觀察值有明顯差異，表示這兩組樣本的分配不一樣，白話地說就是這兩組觀察值認為是不一樣的。而本文中用此檢定方法，來觀察事件日前、後犯罪量 (觀察值) 之數值，是否有明顯之差異。

## 二、法律之經濟分析

本文除以實證統計方式來分析目前實務採取防制詐欺之手段，是否足以達到嚇阻網路詐欺之犯罪量外，亦借用法律之經濟分析 (economic analysis of law) 方式<sup>182</sup>，來檢視防制詐欺手段實施之實際狀況，以此來觀察是否能落實當初選擇此手段來降低犯罪量之目的。以下簡要介紹本文有適用到之法律經濟學之基本觀念。

犯罪學古典學派論點之基本假設為人是理性的、具有驅樂避苦與精於計算的特性，犯罪則是計算成本與獲益後的理性行為。換言之，犯罪行為係行為人深思熟慮之後，認為犯罪比不犯罪有利，進而發諸行動的一種事件。因此，犯罪行為是一種理性

<sup>182</sup>法律之經濟分析乃係 1950 年代後期萌始於美國，且已在英美法係之法學取得不可忽視的地位，參見 Posner, Richard A, Economic Analysis of Law (5<sup>th</sup> ed, 1998); The New Palgrave Dictionary of Economics and the Law (1998).

選擇的結果，從「理性選擇理論」(Rational Choice)來看，犯罪就如同其他經濟行為一樣，是個人的一種選擇<sup>183</sup>。

經濟學之「選擇理論」，認為人類之各項行為本質上均係斟酌選擇之結果，而法學與經濟學都在嘗試提供人類利益發生衝突時之解決方法，此二者即有共通性存在，從而，將經濟學之分析方法帶入法學領域，當然可以成為法學之不同思維角度的切入點<sup>184</sup>。又法律之經濟分析是以「理性選擇理論」核心為基礎，研究各種法律規範之理論效果是否符合經濟效益，亦即檢視法律對吾人可能選擇範圍所為之限制，是否符合經濟效率<sup>185</sup>。

經濟學對犯罪之定義，並未嘗試跳脫或推翻傳統法學對犯罪所下之定義，而是從人類理性(rational)、自利(self-interest)之行為理論假設出發，結合「成本」、「外部性」、「需求理論」等概念來解釋犯罪行為之趨向。因此，對於經濟學之解釋與分析而言，假設犯罪者是個理性且道德中立之人，並不會因罪惡感或內心良知所束縛，而改變從事不法行為之決意，換言之，犯罪是犯罪者在諸多限制條件下，進行的一種選擇行為，此種選擇行為即「在決定犯罪之當下，經過理性之評估，認為犯罪所獲得之利益大於犯罪所需的成本，則決意從事犯罪行為」，而該選擇之過程，以經濟學之觀點而言，即係經過成本效益分析後所做之決擇的行為。經濟學家 Becker 指出<sup>186</sup>：一種能行之有效的犯罪理論，只是經濟學常用之「選擇理論」之擴展，無需以諸如：道德的頹廢、心裡機能的缺陷或遺傳基因的生物特質等因素來解釋犯罪行為。

當行為人從事犯罪行為時，定會預期到將來會被法律制裁之可能，而制裁是存有機率性的，犯罪行為人可能逃過偵查、未獲逮捕、或被逮捕但未被認定有罪。而犯罪行為人面對預期之制裁情形，理性、不受道德拘束之決策者，在思考是否進行犯罪行為時，會將受到制裁的機率納入考慮，亦即只要犯罪之利益高於預期制裁之成本，理性之決策者將會選擇從事犯罪行為。經濟學家 Becker 曾提出以下理性犯罪者之目標方程式<sup>187</sup>：

$$\max\pi(x) = y(x) - p(x)f(x)$$

以上方程式中變數(x)表示犯罪之嚴重程度(以金錢為單位)。y是犯罪後之利得、p是受制裁的機率、f為制裁的程度即罰金刑。簡言之，y-pf為犯罪淨利得，此即理性犯罪者追求犯罪淨利得極大<sup>188</sup>。而依上開理性犯罪模型可知，降低犯罪量之方法，不外乎降低犯罪利得、提高受制裁機率及提高刑罰等手段。又其上p受制裁的機率，依據美國經濟學家 Isaac Ehrlich 之觀點<sup>189</sup>，更精確地說：f(受制裁之機率) = 被

<sup>183</sup> 許春金，犯罪學，修訂3版，第174至185頁，自版，2000年8月。

<sup>184</sup> 熊秉元，熊秉元漫步法律，第20至37頁，時報文化出版，2003年。

<sup>185</sup> 陳彥希，「效率、正義與契約」，日新警察半年刊，第5期，第10頁，內政部警政署印製，2005年9月。

<sup>186</sup> Becker, Gary, "Crime and punishment: An economic approach", *Journal of Political Economy* 76, page 169, 1968。

<sup>187</sup> 同前揭註。

<sup>188</sup> 同前揭註 13，第550頁。

<sup>189</sup> 同前揭註 13，第588頁。

逮捕率（逮捕犯罪者之數項÷犯罪報案之總數量）×定罪率（犯罪者有罪認定之數量÷逮捕犯罪者之數項）×執行率（被執行之總數量÷犯罪者有罪認定之數量）。

Posner 認為犯罪行為是一種非自願性的交易，且形成負的外部性<sup>190</sup>。當人類之個別行為對社會造成負的外部性時，此負的外部性之「存在」，產生必須經由一定機制加以處理之「需求」，此需求即是法律制度存在之目的。又犯罪加諸於社會的成本可分為犯罪所造成之淨損失以及預防費用之支出<sup>191</sup>。而國家發動刑罰制裁犯罪之終極目的在於，藉由嚇阻犯罪達到預防犯罪之結果，故認為事後制裁犯罪者之費用，應包括在預防費用之社會成本支出在內。故前揭討論社會成本中之預防費用之支出，實際上應包括事前預防犯罪之費用及事後制裁犯罪者之費用。又事後制裁犯罪者之費用，可再細分為：1.查獲或逮捕之費用（警察調查局等機關之費用）；2.定罪之費用（司法機關之費用）；3.執行之費用（執行罰金刑、觀護人及監獄系統之費用）。從而，可以導出一個公式為：社會成本＝犯罪淨損失＋預防費用之支出（應包括事前預防犯罪之費用＋事後制裁犯罪者之費用【查獲或逮捕之費用＋定罪之費用＋執行之費用】）。經濟學者在討論犯罪制裁手段時，多以具體效率、成本等概念分析該法律制度或手段之採取，是否是有效率的。在經濟學之角度，何謂是有效率的？常見的三種效率（efficiency）之定義，第一種：社會剩餘極大化（social surplus maximization）。第二種，社會成本極小化（social cost minimization），又稱成本有效性（cost effectiveness）。第三種，Pareto 效率（Pareto efficiency），又稱 Pareto 最適。有經濟學者認為：社會成本＝犯罪淨損失＋預防費用之支出，而最適的犯罪量或是最有效率的嚇阻程度，應該與犯罪所造成的社會成本取得平衡。因此當損失總和等於預防成本時，刑事政策之犯罪成本將極小化<sup>192</sup>。

依前開 Becker 提出之理性犯罪模型可知，假設犯罪是一種理性選擇的結果，則降低犯罪量之方法有三：降低犯罪利得、提高定罪率及提高刑罰。而犯罪學也以同樣的「犯罪是一種理性選擇的結果」假設前提下，發展出許多犯罪預防的策略<sup>193</sup>，其中由美國犯罪學者克拉克(Ronald Clarke)<sup>194</sup>主張之「情境犯罪預防策略」(situational crime preventions)認為，犯罪預防之策略可從以下四大方面著手：增加犯罪困難度、提升犯罪風險、降低犯罪利得及促使產生犯罪的罪惡感或羞恥心。因此，本文欲借用其中「降低犯罪利得」之相關內涵，即克拉克認為降低犯罪利得之手段應包含：「犯罪對象之移除」、「減少誘惑」及「減少利益」。又「犯罪對象之移除」係指：以相關措施移除犯罪者對潛在被害人所施用之犯罪手法，使犯罪者無法對潛在被害人進行犯罪行為；「減少誘惑」為：減少設置、實施易導致刺激犯罪發生之物品或措施；「減少利益」係以相關措施使犯罪者無法順利達成其實施犯罪行為所預期之目標<sup>195</sup>。而本章實證研究之犯罪

<sup>190</sup> Richard A. Posner 著，法律的經濟分析，蔣兆康譯，第 292 頁，中國大百科全球出版社，1997 年。

<sup>191</sup> 同前揭註 13，第 556 頁。

<sup>192</sup> 同前揭註 13，第 556 頁。

<sup>193</sup> 理性選擇理論之基礎下所發展出之犯罪預防策略有：情境犯罪預防、一般嚇阻策略、特殊嚇阻策略及長期監禁策略，參前揭註 183，第 204 頁。

<sup>194</sup> Clarke, R. V and R. Home(1997). A Revised Classification of Situational Crime Prevention Techniques. In S.P.Lab (ed): Crime Prevention at a Crossroads. Anderson.

<sup>195</sup> 同前揭註 50，第 83 頁。

防制策略中之「警示帳戶機制」<sup>196</sup>，是將可疑帳戶之臨櫃提領以外之功能終止，迫使詐欺集團無法再行利用該列為警示之帳戶進行詐財行為，故此警示帳戶機制之防制犯罪手法，可謂是降低犯罪利得中之「犯罪對象移除」之方式；另犯罪預防措施之「非約定帳戶之轉帳限制」，乃是為減少、降低被害人受騙轉帳之金額，亦即降低犯罪者控制、管理之人頭帳戶內詐騙金額之不法利益，故應係「降低犯罪利得」中之「減少利益」之手段；至於「提高洗錢防制法刑罰」之策略，則屬理性犯罪模型中之提高刑罰之手段。理論上，從經濟學角度而言，不論是降低犯罪利得，抑或是提高刑罰之防制手段，均應能有效降低犯罪之發生率。因此，本文從實證統計方式來驗證此一經濟犯罪模型之理論。

## 4.2 實證研究結果

### 4.2.1 警示帳戶通報機制執行之成果

#### 一、警示帳戶數目逐年增加

理論上，警示帳戶之實施，應會在某種程度造成詐欺集團從事詐騙行為取款之阻礙。依據內政部刑事局之資料統計，2003年7月30日至2005年止，全國警示帳戶已達54,238筆<sup>197</sup>，其中2003年7月至12月總計警示帳戶共239件、2004年全年計26,209件、2005年全年有27,790件，然而，前開統計數據卻又顯示人頭帳戶之發生件數仍在不斷增加中。則本文進一步探討，此警示帳戶之運作機制是否能確能嚇阻詐欺案件之發生。

#### 二、事件研究法

本文此節主要探討「警示通報機制」政策宣告實施後，對於一般詐欺及網路詐欺案件犯罪量之影響，事件發生是在2003年7月，並以此為基準，觀察事件發生前、後一年犯罪量月資料之變化，即觀察期間為2002年7月至2004年7月。

##### 1. 樣本選擇：法院審理販賣帳戶用以詐欺案件之審理件數

我國司法實務上，法院審理販賣人頭帳戶之情形，多是帳戶名義人出賣、出租帳戶後，轉由詐欺集團或成員利用以騙誘被害人匯入款項，因被害人不甘受騙進而報警為警查獲之案件佔多數。又法院審理販賣之帳戶用以詐欺之案件中，犯罪時間若是在警示帳戶機制實施之後者，均是經警員初步查證被害人匯入款項之帳戶為「可疑帳戶」，始會將案件移送至各法院地檢署，再由檢察官起訴至法院審理，故法院審理之前開個案中之帳戶，均會在為警查獲並認定為「可疑帳戶」時，一併由警察以傳真方式請求金融機構將可疑帳戶列為「警示帳戶」。故本文認為直接觀察設立警示帳戶機制前、後各一年「法院審理販賣帳戶用以詐欺案件」之案件量變化，來檢視「警示帳戶機制之實施」是否有降低「利用人頭帳戶從事詐欺犯罪」之犯罪量，應是有效驗證警

<sup>196</sup>因為此部分之觀察期間為2002年7月至2004年7月止，係在「異常帳戶管理辦法」發布前，故此觀察期間之警示帳戶機制，是將警示帳戶停止臨櫃提領以外之功能。

<sup>197</sup>此資料為內政部警政署刑事局所提供，資料未公開。

示帳戶機制執行是否有效之實證方法。因內政部警政署設立警示通報機制之時間點為 2003 年 7 月，故本文採集案件是「犯罪時間」為 2002 年 7 月到 2004 年 7 月之販賣人頭帳戶案件，並限定是利用人頭帳戶進行詐騙之犯罪類型，進行統計<sup>198</sup>，調查統計結果參圖 8。

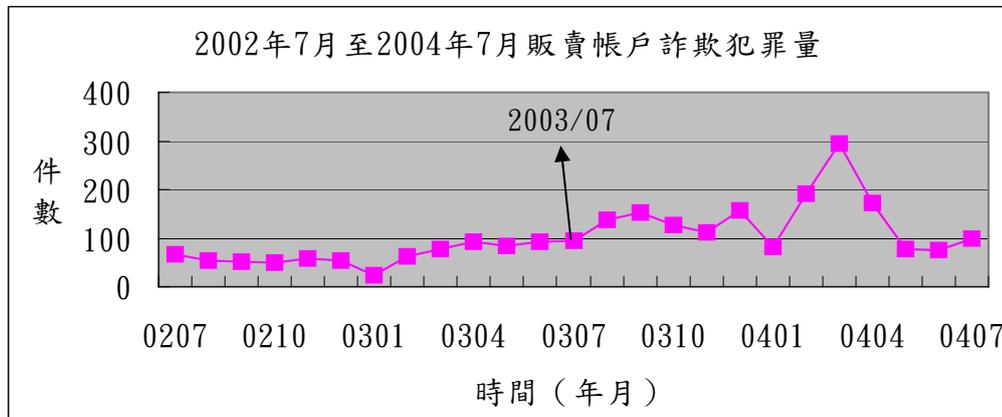


圖 8 販賣帳戶用以詐欺之犯罪量圖

從法院審理販賣人頭帳戶案件量之月資料來觀察，2003 年 7 月以後之件數，除 2004 年 1、5 月之月件數較 2003 年 7 月略少外，其餘月份之件數均高於 2003 年 7 月，而且 2003 年 7 月起至 2004 年 7 月呈現一個案件量明顯上升的趨勢。另經使用 Mann-Whitney U Test 統計檢定<sup>199</sup>事件發生前後之案件，2003 年 7 月之前每月平均件數 63.75 件，同年 7 月以後平均每月為 141.15 件，販賣人頭帳戶案件量之增多在 5% 水準下已具之顯著性 ( $U=149.0$ ;  $P<0.001$ )。

從以上「警示帳戶數量」、「法院審理販賣帳戶用以詐欺案件之審理件數」之數據，可看出警示帳戶數及法院審理之件數，均有上升的現象，而此現象有可能是因為販賣人頭帳戶之犯罪量確實增加，也有可能是警方努力執行查緝人頭帳戶的結果。故為檢驗以上「警示帳戶數量」、「法院審理販賣帳戶用以詐欺案件之審理件數」之增多，到底是因為販賣人頭帳戶犯罪量之增加，抑或是警方提高查緝之結果，本文再進一步觀察網路詐欺及其他詐欺之發生數，因為若是警方確實有提升查獲率，則使用人頭帳戶為主之網路詐欺及其他詐欺之犯罪量勢必下降。

## 2. 樣本選擇：內政部警政署統計網路詐欺等之「發生數」

本文先觀察的對象為內政部警政署所提供台灣地區電腦網路犯罪中案類別為「詐欺」之逐月發生數，觀察期間為 2002 年 7 月到 2004 年 7 月，而此「發生數」乃民眾報案之件數，並非警方破獲、查緝到的件數，先予說明。

<sup>198</sup>本文統計全國各地方法院判決，而採集判決之方式為，利用司法院網站之裁判書查詢，網址為：<http://jirs.judicial.gov.tw/FJUD/index.htm>。搜尋期間為判決宣判日期 1996 年 1 月 1 日至 2005 年 12 月 31 日止，搜尋關鍵字「帳戶&詐欺」，並逐一過濾不符合之案件。

<sup>199</sup>Mann-Whitney U Test 檢定之網站 <http://eatworms.swmed.edu/~leon/stats/utest.cgi>，而統計檢定之 P 值小於 0.1 時，有顯著差異。

而在觀察電腦網路犯罪相關資料的同時，發現有一可能干擾之變數，即在台灣地區電腦網路犯罪之各案類別下「妨害電腦使用」發生數之變化。簡言之，即我國網路詐欺之態樣中佔 32.79%之「網路遊戲詐欺」，在 2003 年 6 月 25 日刑法修正公布「妨害電腦使用」罪章後，只要網路詐欺牽涉與網路遊戲相關者，內政部警政署之統計即會將此種詐欺案件之發生數，歸入台灣地區電腦網路犯罪之各案類別下之「妨害電腦使用」。因此，2003 年 7 月以後網路詐欺案件發生數之下降，即有可能是因為部分應歸類於網路詐欺之案件，因修法後適用法律之不同而導致歸類於其他類型之案件，而產生有發生數下降的結果。為此，本文進行對移送至地檢署而案由為「妨害電腦使用罪章」之案件抽樣統計，統計結果發現其中有 24%<sup>200</sup>的案件亦應屬網路詐欺之網路遊戲詐欺類型。所以，本文試圖將「妨害電腦使用罪」之發生數乘上 24%後加回「網路詐欺」之發生數來觀察，如圖 9：

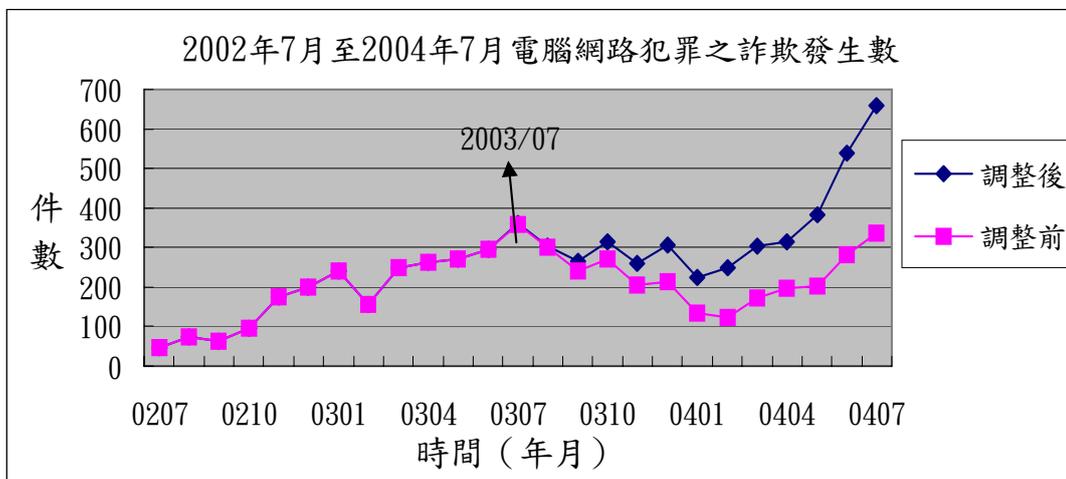


圖 9 網路詐欺之犯罪發生數圖  
(資料來源：內政部警政署)

調整前發生數曲線，是依照警政署提供「詐欺發生數」之統計數據所製作，而 2003 年 7 月前、後每月平均之發生數分為 177.25、233.46 件，實施警示通報機制後之每月發生數較之前多出 31.71%。調整後發生數之曲線，是「詐欺發生數」加上 24%之「妨害電腦使用罪」發生數後加總數據之結果。而從調整後之發生數可以看出，實際上網路詐欺之案件，應是比原統計網路詐欺發生數呈現一個略微上揚之趨勢，且經使用 Mann-Whitney U Test 檢定事件發生前後之案件，2003 年 7 月之前每月平均件數 177.33，同年 7 月以後平均每月件數為 344.56，網路詐欺之案件量之增多在 5% 水準下已具顯著性 ( $U=142.0$ ； $P<0.001$ )。

另外，再行觀察 2002 年 7 月至 2004 年 7 月全部詐欺案件發生數之逐月

<sup>200</sup>以「刑法第三百五十八條」、「刑法第三百五十九條」為關鍵字，搜尋士林等 12 個地檢署於 2005 年 1 月 1 日至同年 6 月 30 日止偵查終結之案件，發現在所有觸犯刑法第 358 條的案件中，約有 24% 的案件在修法前適用的法條應為刑法 339 條之詐欺罪，因修法而改為適用行法第 358 或 359 條。

變化，從全部詐欺逐月發生數之犯罪量曲線，可看出詐欺案件發生總數在 2003 年 7 月之後不僅並未降低，且再使用前開同樣的統計檢定發現，2003 年 7 月之前每月平均件數 2650.42，同年 7 月以後平均每月件數為 3246.23，全部詐欺之案件量在 5% 水準下亦有顯著性 ( $U=123.0$ ； $P=0.01$ )。如下圖 10：

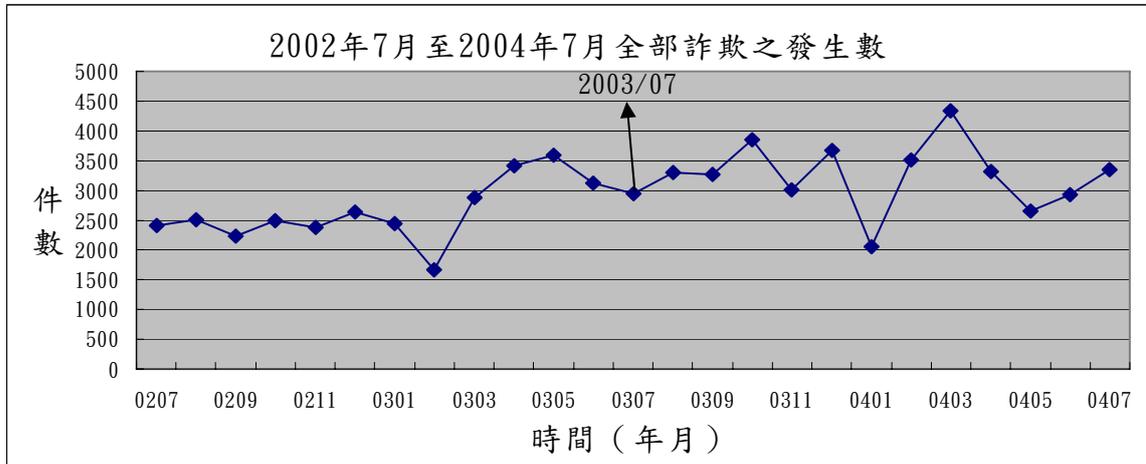


圖 10 全部詐欺發生數圖  
(資料來源：內政部警政署)

綜上觀察，實施「警示帳戶通報機制」對防制詐欺或網路詐欺而言，並無數據證明有降低詐欺或網路詐欺犯罪之發生數，甚至其中網路詐欺之發生數是有顯著上升。依此，本文認為之前觀察「警示帳戶數量」、「法院審理販賣帳戶用以詐欺案件之審理件數」變多之原因，應係販賣人頭帳戶犯罪量實際之增加，而非警方加強查緝之結果，否則不論是內政部警政署統計之詐欺或是網路詐欺之「發生數」，應該會有降低之趨勢。因此，本文觀察認為警示帳戶之實施對降低人頭帳戶及網路詐欺均無實際成效。

從經濟學之理性犯罪模型而言，警示帳戶機制之施行，已移除犯罪者利用人頭帳戶取款之手段，理論上，在某種程度造成詐欺集團從事詐騙行為取款之阻礙，應能降低詐欺或是網路詐欺之犯罪量。然而，從前開警示帳戶成效性之實證分析可知，卻又證明此防制策略確實對於一般詐欺及網路詐欺並未產生降低犯罪量之結果。而犯罪量並未降低之原因，我們推測可能有以下幾種原因：可能是執行機關破獲率過低；也有可能是刑罰不高所導致；另外，也可能是因為在此警示通報機制實施後，詐騙集團改變以往「收購」人頭帳戶之方式，變成以每週出租之方式「租借」人頭帳戶，以此方式來降低取得人頭帳戶之犯罪成本，並避免使用之人頭帳戶一旦列為「警示帳戶」而遭到損失<sup>201</sup>，也就是詐騙集團改變取得人頭帳戶之方式來自我降低犯罪之成本，使犯罪之預期利得並未因此而有所減損，故理性犯罪者衡量犯罪利得大於犯罪預期成本後，在有利可圖的情況下，仍會繼續從事犯罪行為。

<sup>201</sup>據報載，警方近來發現，自從警方與金融業者連線，將詐騙集團匯款之「指示帳戶」列為「警示帳戶」後，詐騙集團改以「承租」方式包攬人頭戶，以十天為一期，每期租金二千元，以避免人頭帳戶一旦被列為「警示帳戶」遭到損害。見民調大陸女口音十之八九詐騙，WEBS-TV 新聞，<http://news.web-tv.net/index.php>，(2006/Jan/5)。

#### 4.2.2 限制轉帳之實行結果及有效性

##### 一、自動櫃員機（ATM）轉帳交易次數、金額之分析

依照行政院金管會銀行局公佈「自動化服務機器概況」之統計資料製作表格如下表 10：

表 10 自動櫃員機轉帳交易次數、金額

2005 年	1 月	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月	10 月	11 月	12 月
轉帳 次數	61979(千 次，以下 同)	49050	63654	57232	64693	60758	60238	63837	61927	61588	60383	61896
轉帳 金額	790603( 百萬，以 下同)	717102	817617	719537	809910	741985	746419	799740	754738	728812	725217	722031

（資料來源：行政院金管會銀行局）

發現 2005 年 5 月之 ATM 轉帳交易次數、金額均佔該年度之冠，有可能是因為同年 6 月 1 日將實施每日非約定轉帳上限 3 萬元之限制，人民利用制度實施前之空檔多加利用 ATM 進行轉帳、匯款等功能。又 2005 年 6 月之轉帳金額、件數確實明顯較同年 5 月為低。另 ATM 轉帳交易次數、金額之月平均數見表 11。

表 11 自動櫃員機轉帳交易次數、金額之月平均表

時間	總轉帳次數 (千次)	總轉帳金額 (百萬)	平均每月轉帳次數 (千次)	平均轉帳金額 (百萬)
2005 年 1 至 5 月	296608	3854769	59321.6	770953.8
2005 年 6 至 12 月	430627	5218942	61518.1	745563.1

（資料來源：行政院金管會銀行局）

依該統計資料發現，在 2005 年 6 月之後之平均每月轉帳次數較之前為多，多出 3.70%，但平均每月轉帳金額卻減少 3.40%，整年度趨勢詳見下圖 11、12。由此可見，民眾確實因此而多花成本。

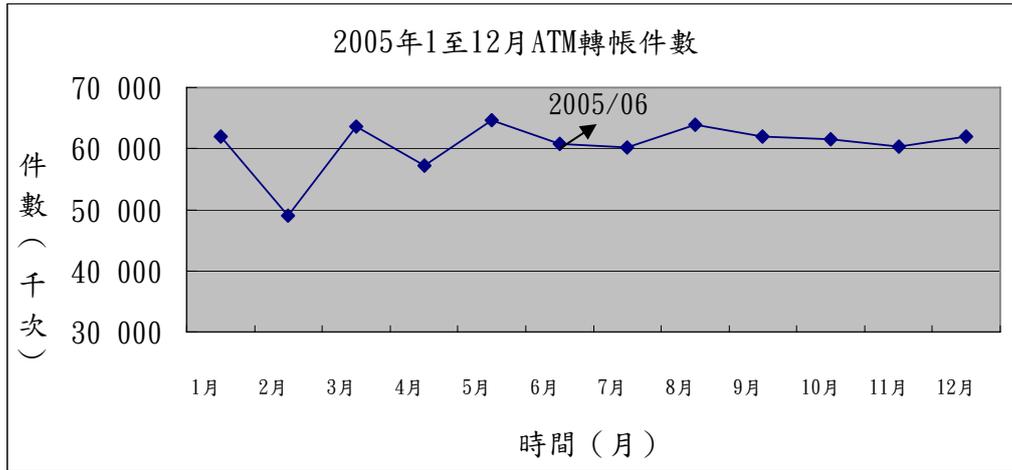


圖 11 2005 年自動櫃員機轉帳件數逐月曲線圖  
 (資料來源：行政院金管會銀行局)

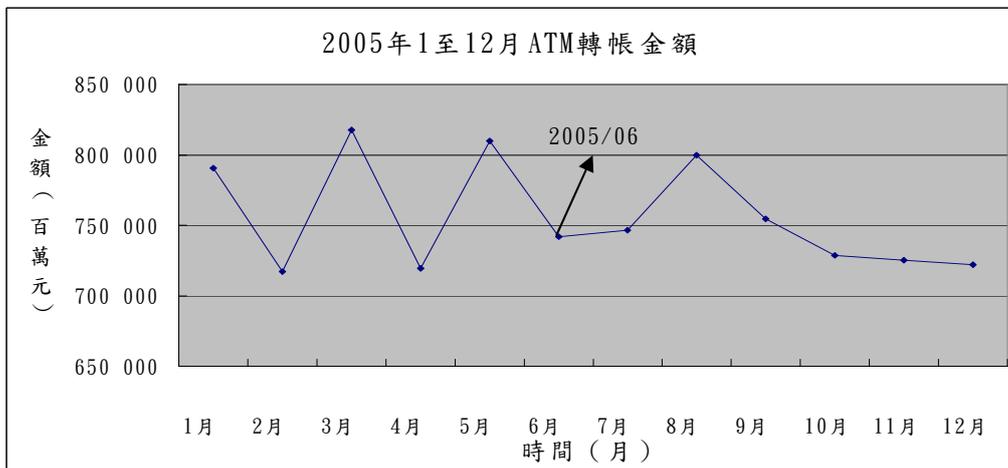


圖 12 2005 年自動櫃員機轉帳金額逐月曲線圖  
 (資料來源：行政院金管會銀行局)

二、事件研究法：

1. 樣本選擇：2005 年警察單位受理各類型詐欺發生數

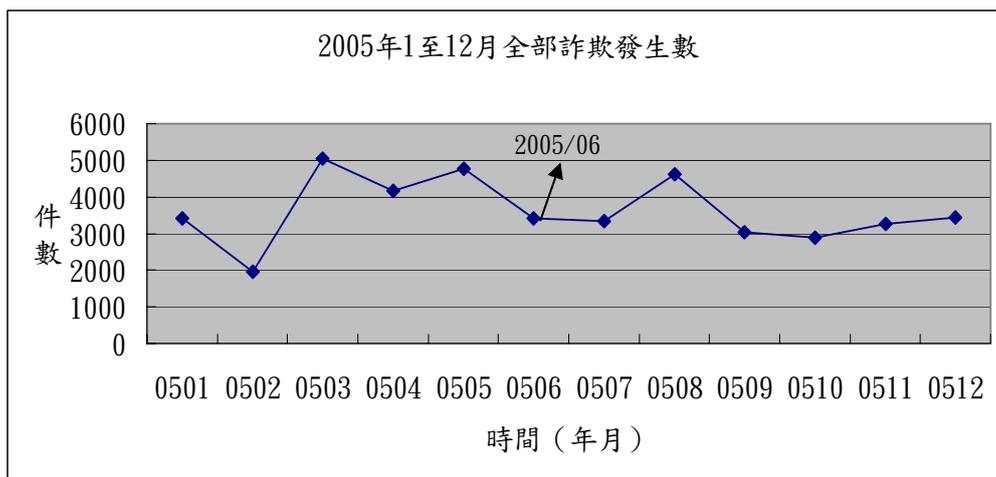


圖 13 2005 年全部詐欺逐月曲線圖  
(資料數據來源：內政部警政署)

經使用 Mann-Whitney U Test 檢定事件發生前後之案件，2005 年 1 至 5 月之前每月平均 3870 件；同年 6 月以後平均每月件數為 3427.43 件，全部詐欺之案件量雖略微降低，但並無顯著性 (U=24.5；P=0.26)。

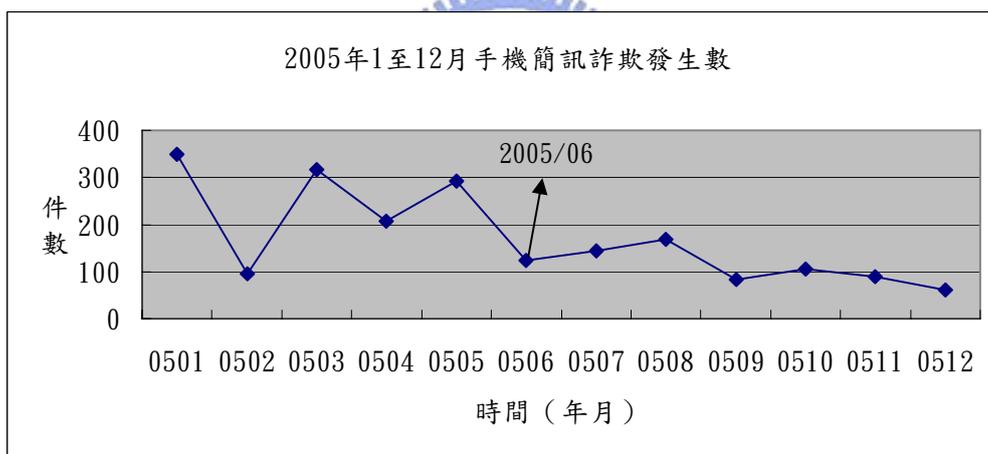


圖 14 2005 年手機簡訊詐欺逐月曲線圖  
(資料數據來源：內政部警政署)

經使用 Mann-Whitney U Test 檢定事件發生前後之案件，2005 年 1 至 5 月之前每月平均件數 252 件；同年 6 月以後平均每月為 110.43 件，手機簡訊詐欺案件量之降低在 5% 水準下已具顯著性 (U=32.0；P=0.01)。

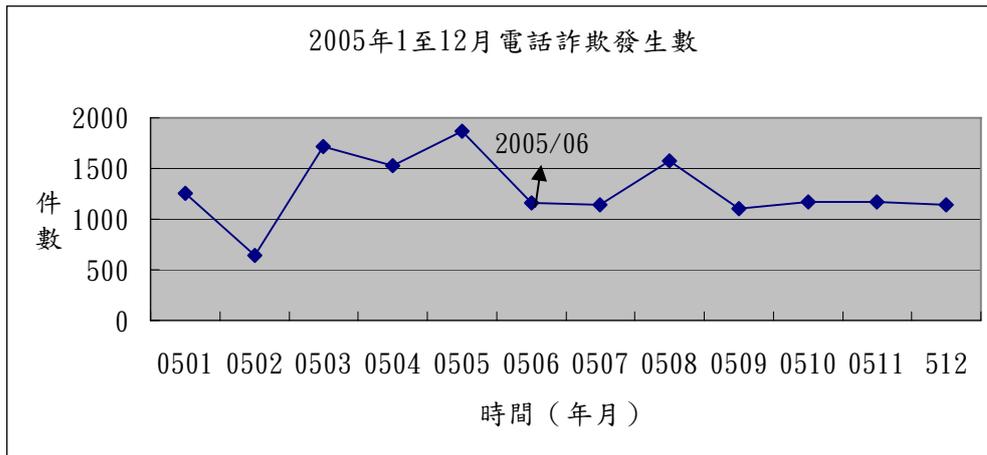


圖 15 2005 年全部詐欺逐月曲線圖  
(資料數據來源：內政部警政署)

經使用 Mann-Whitney U Test 檢定事件發生前後之案件，2005 年 1 至 5 月之前每月平均件數 1402.8 件；同年 6 月以後平均每月件數為 1208.57 件，電話詐欺案件量雖有降低，惟並未具有顯著性 ( $U=26.0$ ； $P=0.17$ )。

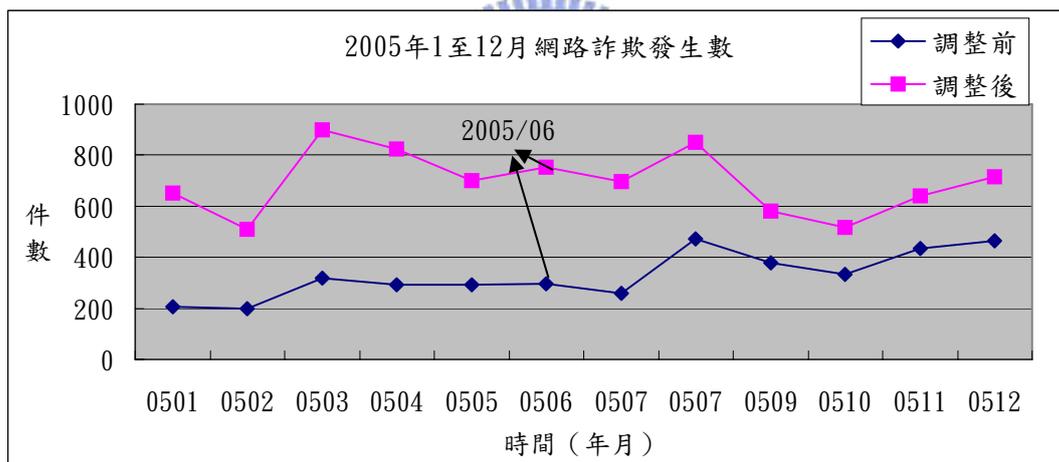


圖 16 2005 年網路詐欺逐月曲線圖  
(資料數據來源：內政部警政署)

經使用 Mann-Whitney U Test 檢定事件發生前後之網路詐欺案件，調整前之情形為：2005 年 1 至 5 月之前每月平均 261.2 件，同年 6 月以後平均每月件數為 377.43 件，網路詐欺案件量不僅未降低反而提高，且案件量之變多已有顯著差異 ( $U=31.0$ ； $P=0.03$ )。雖然加上 24% 之「妨害電腦使用罪」之發生數，即調整後之網路詐欺件數該年度前 5 月之月平均件數為 716.67 件，而 6 月以後之月平均反而略為下降至 661.14 件，但件數減少尚未具顯著性 ( $U=20.0$ ； $P=0.68$ )。故不論是觀察調整前、調整後之網路詐欺發生數，我們都可以說非約定帳戶之轉帳限制對於特定之網路詐欺並無明顯成效。

由以上圖及統計檢定之說明可知，非約定轉帳之限制，對於手機簡訊此類

之詐欺確實有成效。然而，網路詐欺之件數並未因為限制轉帳而有顯著降低，這可能是因為網路詐欺雖然大都與人頭帳戶有關，但是平均每筆轉帳金額較低，所以限制轉帳金額為三萬元對其用途不大。

為檢驗限制轉帳措施對降低網路詐欺犯罪量之效果不彰的假設，本文觀察 2005 年全國地院之檢察署偵查終結網路詐欺之案件<sup>202</sup>，統計平均轉帳金額、筆數（表 12）。

表 12 網路詐欺平均轉帳金額、件數及人頭帳戶件數表

詐欺轉帳金額	匯款數及百分比		匯款進入人頭帳戶	
	金額（元）	筆數	百分比	筆數
10000 以下	883	58.36%	599	57.87%
10000-20000	235	15.53%	213	20.58%
20001-30000	84	5.55%	59	5.70%
30001-40000	61	4.03%	39	3.76%
40001 以上	250	16.52%	202	19.51%
全部合計	1513	100%	1035	100%

統計觀察結果：1.全部網路詐欺之平均每件轉帳金額為 23,553.6 元，且每筆轉帳金額未超過 1 萬元之件數超過五成（58.36%），而轉帳金額未超過 3 萬元之件數佔 79.44%，由此可以看出網路詐欺被騙金額「小額性」之現象。2.又網路詐欺中轉帳金額未超過 3 萬元之 1202 件中，有 871 件是利用人頭帳戶之案件，即轉入之帳戶為人頭帳戶佔 72.46%。3.從上可知，2005 年 6 月 1 日宣布調降金融機構 ATM 每日非約定轉帳上限為 3 萬元之政策，對於大部分欲使用網路從事詐欺之潛在犯罪者來說並無影響，因為網路詐欺之每筆被騙金額約八成均在 3 萬元以下。

從經濟分析的角度而言，犯罪之邊際成本會因為犯罪量之增加而遞增，則犯罪之邊際成本會因為犯罪量之增加而遞減，當犯罪邊際成本等於邊際收益時，則是理想之犯罪量。而如我們統計犯罪時間點在 2005 年 6 月 1 日前網路詐欺案件之結果發現，有 79.44%之案件每筆轉帳金額不超過 3 萬元，則這些詐欺案件之邊際成本、邊際收益皆小於 3 萬元，則 2005 年 6 月 1 日宣布非約定轉帳上限為 3 萬元之防制策略，對於這類之案件是無效的限制式。以圖形表示如下圖 17，圖中之 MC 表示犯罪之邊際成本，MR 表示犯罪之邊際收益， $Q_0$  犯罪最適量。

<sup>202</sup>採樣標的為全國地檢署於 2005 年 1 月 1 日至同年 12 月 31 日偵查終結之網路詐欺案件，利用法務部部內網站以「網路&詐欺」、「網站&詐欺」、「網際網路&詐欺」關鍵字搜尋過濾後共 924 件，並剔除犯罪時間點為 2005 年 6 月 1 日以後發生之案件。

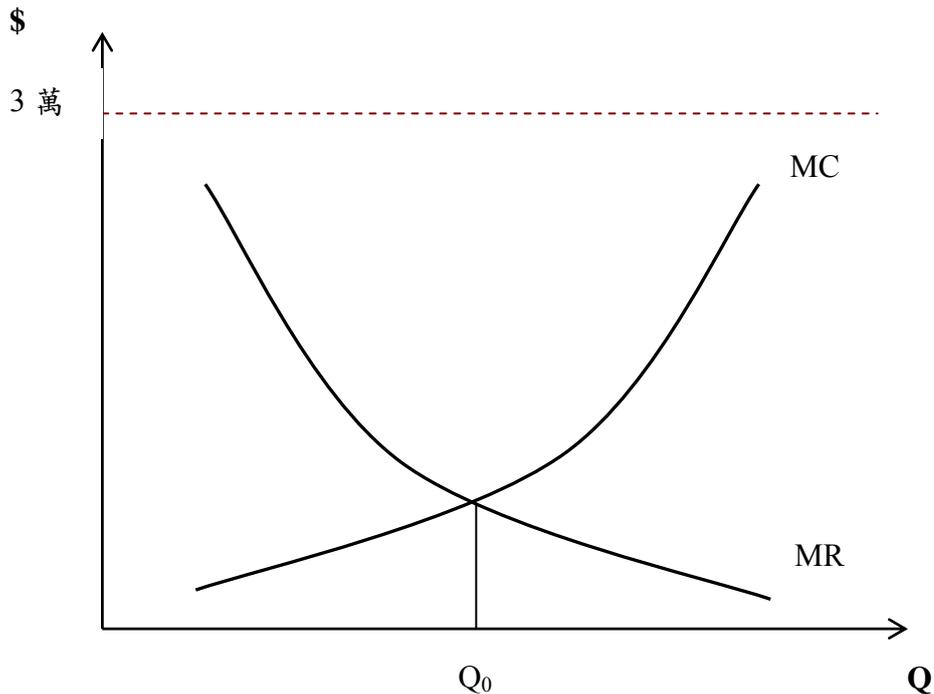


圖 17 非約定轉帳限制對網路詐欺之影響圖

#### 4.2.3 提高刑罰之有效性

洗錢防制法於 2003 年 2 月 6 日修正公布，並於同年 8 月 6 日施行，將幫助他人洗錢之犯罪行為提升到正犯地位來處罰，並將法定刑之上限提高，應係藉由查緝人頭帳戶犯罪來防制詐欺之防制策略，已如前述，故本文以下試從實證統計、分析之角度，來探討提高刑罰手段之有效性。

##### 一、販賣人頭帳戶之偵查終結情形、定罪率及執行率

法務部統計室於 2005 年起就販賣「人頭帳戶」之案件製作統計資料，在此之前之資料則付之闕如。而從 2005 年 1 月到 12 月份之統計資料可看出，終結之被告總數為 3417 人<sup>203</sup>，其中認為無犯罪嫌疑而為不起訴處分有 482 件；認為有犯罪嫌疑者有 1967 人，其中依通常程序起訴有 605 人、聲請簡易判決有 1314 人、緩起訴處分有 45 人、職權處分有 3 人<sup>204</sup>，參下表 13。

<sup>203</sup> 資料來源：法務部統計處，製表日期：2006 年 1 月 18 日，資料未公開。

<sup>204</sup> 除上述外，尚有其他終結情形（可能包括：簽結、移轉管轄、併案等）被告總數為 968 人。

表 13 人頭帳戶案件偵查終結情形表

檢察官終結情形		被告人數：3417 人
不起訴或緩起訴處分	不起訴處分	482
	職權不起訴處分	3
	緩起訴處分	45
向法院提起公訴	聲請簡易判決處刑	1314
	通常程序起訴	605
其他		968

(資料數據來源：法務部統計處統計資料)

案件向法院起訴、聲請簡易判決處後，經判決確定之被告總數為 816 人，其中判處有罪之被告有 789 人：包括判處罰金 2 人、拘役 92 人、有期徒刑 6 月以下有 650 人、有期徒刑逾 6 月而未滿 1 年有 29 人、有期徒刑逾 1 年而未滿 2 年有 10 人、有期徒刑逾 2 年而未滿 3 年有 1 人、有期徒刑逾 3 年而未滿 5 年有 3 人、有期徒刑逾 5 年而未滿 7 年有 2 人，無罪有 3 人，免訴及不受理共有 24 人，參表 14。

表 14 人頭帳戶案件判決確定情形表

法院判決終結情形		被告人數：816 人
有罪	罰金	2
	拘役	92
	有期徒刑 6 月以下	650
	有期徒刑逾 6 月而未滿 1 年	29
	有期徒刑逾 1 年而未滿 2 年	10
	有期徒刑逾 2 年而未滿 3 年	1
	有期徒刑逾 3 年而未滿 5 年	3
	有期徒刑逾 5 年而未滿 7 年	2
無罪		3
免訴、不受理		24

(資料數據來源：法務部統計處統計資料)

再案件確定後經執行之被告有 378 人，其中執行罰金有 1 人、執行拘役共 46 人、執行六月以下有期徒刑 318 人、執行六月以上有期徒刑 13 人(參表 15)。

表 15 人頭帳戶案件執行情形表

案件確定執行情形		被告人數：378 人
執行罰金		1
執行拘役	拘役	15
	易科罰金	31
執行六月以下有期徒刑	徒刑	171
	易科罰金	147
執行六月以上有期徒刑	有期徒刑逾 6 月而未滿 1 年	7
	有期徒刑逾 1 年而未滿 2 年	6

(資料數據來源：法務部統計處統計資料)

從以上法務部 2005 年度之統計資料可知，販賣人頭帳戶案件之定罪率為 55.69%<sup>205</sup>、而案件確定後之執行率為 19.86%<sup>206</sup>。而 2005 年度案件確定執行人數偏低，有可能是因為有效預期執行率低，也有可能是應執行案件之被告仍在傳喚、拘提中或是在分期繳納易科之罰金，但是，因為法務部之統計並未做案件追蹤之統計，故不得而知。

## 二、法院審理販賣人頭案件之情形

本文採集各地方法院判決作為實證之研究資料，並以統計、分析方式，觀察洗錢防制法第 9 條第 2 項之法定刑罰提高後，是否確能達到該條立法理由明白揭示之「提高刑度，以求達到有效嚇阻及制裁犯罪之效果」目的。而本文從兩個實證面向來檢視：

### 1. 修法前、後法院審理販賣人頭帳戶案件「宣判刑度」之比較：

本文統計之方法為搜尋各地方法院至 2005 年 12 月 31 日宣判之販賣人頭帳戶案件的一審判決（包括簡易案件），並過濾無法統計之案件<sup>207</sup>。再將案件依照犯罪時間順序排列，取 2003 年 8 月之修法時點前、後各 1793 件之案件，並計算各法院之平均刑度，統計結果如下表 16：

<sup>205</sup> (犯罪者有罪認定之數量÷逮捕犯罪者之數項 = [ 45 + 3 + (605 + 1314) × (789 ÷ 816) ] ÷ 3417) = 55.69%

<sup>206</sup> (被執行之總數量÷犯罪者有罪認定之數量 = [ 45 + 3 + (605 + 1314) × (789 ÷ 816) ] ÷ 378) = 19.86 %

<sup>207</sup> 本文統計全國各地方法院判決，而採集判決之方式為，利用司法院網站之裁判書查詢，網址為：<http://jirs.judicial.gov.tw/FJUD/index.htm>。搜尋期間為判決宣判日期 1996 年 1 月 1 日至 2005 年 12 月 31 日止，搜尋關鍵字「帳戶&詐欺」，並逐一過濾不符合「將帳戶販賣予他人從事詐欺」之案件。

表 16 修法前後販賣人頭帳戶宣判刑度統計比較表

時間	採樣案件	平均刑度 (月)	平均販賣帳戶數	平均每賣一本之刑度(月/ 本)
修法前	1793	4.44	1.81	2.45
修法後	1793	4.11	1.85	2.22

從統計結果可看出修法前每個被告之平均刑度為 4.44 個月，修法後刑度為 4.11 個月，修法前、後被告每賣一本之刑度分別為 2.45、2.22 個月<sup>208</sup>。而修法前、後每個被告平均販賣帳戶之數量分別為 1.81、1.85 本<sup>209</sup>，整理如下表 17：

表 17 販賣人頭帳戶宣判刑度比較變動百分比

販賣人頭帳戶案件	修法前	修法後	修法後/修法前	變動百分比
平均刑度(月)	4.44	4.11	92.57%	-7.43%
平均販賣本數(本)	1.81	1.85	102.21%	2.21%
每本平均量刑(月/本)	2.45	2.22	90.61%	-9.39%

由上述統計結果顯示，若以 2003 年 8 月洗錢防制法修法之修正為區分基準，在不考慮其他因素而單純僅考慮刑度時，修法後每個被告的平均刑度較修法前降低了 7.43%。若加入「販賣帳戶件數」的因素一併考慮時，因每個被告所販賣之帳戶數目比修法前略高了 2.21%，故每個被告販賣每個帳戶之平均刑度，在修法後較修法前降低 9.39%<sup>210</sup>。足見法院在修法後，審理同樣販賣一本之被告平均量處刑度，不僅未有提高之現象，反有略微下降之趨勢。

而修法前、後每個帳戶之價格分別為 3188.02、2638.60 元，則計算修法前、後每個被告在該案件中之平均犯罪利得為 6188.66、5378.36 元，表格如下表 18：

<sup>208</sup>總刑度÷總帳戶本數=每賣一本之平均刑度。

<sup>209</sup>總帳戶本數÷總件數(統計係以「一被告一案件」計算，此係配合刑事訴訟法之案件概念)  
=每被告販賣之平均本數。

<sup>210</sup>但另一方面，因修法後每個帳戶平均賣得金額較修法前為低(修法前為 3188.02 元，修法後為 2638.60 元)，若以平均每賣得一元所判處之徒刑來觀察，修法前為 0.000769 月/元，修法後為 0.000841 月/元，兩者相較，修法後量刑似乎較高。但販賣帳戶之所得之金額，一般而言，係單純由被告單方面之自白而得知，並無其他求證管道，所以若被告否認販賣帳戶，即無法得知被告真實之販賣帳戶所得金額，即令被告承認販賣帳戶，依照人情之常，被告也會傾向於承認較低金額以求得法官較輕之量刑，故本文以為「所得金額」，並不適合做為比較量刑輕重之依據，因此，仍以客觀上得以確定之「販賣帳戶本數」做為衡量依據較為合理。

表 18 販賣人頭帳戶之平均販賣本數及犯罪利得比較表

販賣人頭帳戶案件 <sup>211</sup>	修法前	修法後
總件數	1793	1793
總本數	3246	3323
總本數中代價不詳之本數	466	515
不詳本數佔總本數之比例	14.36%	15.50%
平均販賣一本之報償(元)	3188.02	2638.60
平均每被告販賣之本數(本)	1.81	1.85
平均每被告之犯罪利得(元)	6188.66	5378.36

## 2. 修法前、後法院審理販賣人頭帳戶案件「客觀犯罪量」之變化

本文此部分亦採用「事件研究法」來觀察洗錢防制法於修法後，地方法院審理販賣人頭帳戶案件之件數，是否較修法前有減少之現象。然就「事件研究法」之事件日的確定，應是指市場「接收」到該事件相關資訊之時點，而非事件實際發生的事點。洗錢防制法第 9 條之修法實行日固然為 2003 年 8 月 6 日，然販賣人頭帳戶之犯罪市場，是否立即接收到該修法提高刑罰之資訊，我們在進行採集樣本前必須考慮此點。依據理性犯罪模型，假設潛在犯罪者會自行衡量預期制裁與預期利益，故法律刑罰之提高，當然會影響潛在犯罪者是否決意發動犯罪行為。然因潛在犯罪者並非熟忍法律之人，並非洗錢防制法一旦修法後，潛在犯罪者即知同型態之犯罪因修法而提高刑罰，故本文於統計修法前、後一年法院受理案件時，為求數據之有效性及穩定性，剔除犯罪時間點為修法前、後半年之判決，試圖觀察修法前後犯罪量的變化<sup>212</sup>。

統計結果發現：修法前（2002 年 9 月至 2003 年 2 月）之件數為 299，平均每月之件數為 49.83 件；修法後（2004 年 3 月至 8 月）之件數竟高達 932 件，平均每月之發生件數為 155.33 件，即修法後之法院審理件數確實較修法前之件數為多。由上開統計結果可以看到修法後之販賣人頭帳戶之案件量，相較於修法前同一時間之案件量，明顯提高 211.72%，且經使用 Mann-Whitney U Test 統計檢定，在 5% 水準下確實已具有顯著差異性（ $U=36.0$ ； $P<0.01$ ）。然此有可能是販賣人頭帳戶之犯罪量實際增多，也有可能是警方努力查緝之結果。

本文為驗證法院審理之案件量增多，是肇因於販賣人頭帳戶之犯罪量增多之原因，故再利用相同之「事件研究法」採集內政部警政署所提供台灣地區電腦網路犯罪中案類別為「詐欺」案件發生數之次級資料進行觀察，結果如下圖

<sup>211</sup> 此之「案件」是指一被告一案件。

<sup>212</sup> 本文統計全國各地方法院判決，而採集判決之方式為，利用司法院網站之裁判書查詢，網址為：<http://jirs.judicial.gov.tw/FJUD/index.htm>。搜尋期間為判決宣判日期 1996 年 1 月 1 日至 2005 年 12 月 31 日止，搜尋關鍵字「帳戶&詐欺」，並逐一過濾不符合「將帳戶販賣予他人從事詐欺」之案件。

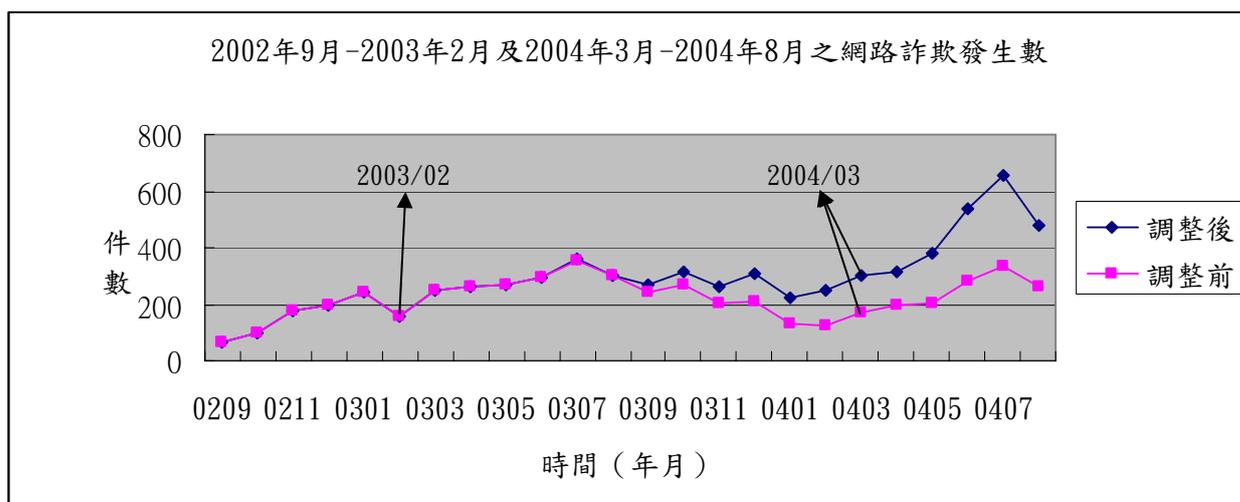


圖 18 網路詐欺逐月發生數圖  
(資料數據來源：內政部警政署)

觀察發現：網路詐欺案件修法前（2002年9月至2003年2月）之發生件數為930，平均每每月之發生件數為155件；修法後（2004年3月至8月）之發生件數竟高達1450件，若同前加上電腦網路犯罪下「妨害電腦使用罪」發生數之24%後，實際網路詐欺之發生數為2680.96件，調整前、後平均每每月之發生件數分別為241.67、446.83件，較修法前同時期之件數各多出55.91%、188.28%。而且，修法後2004年3至8月網路詐欺之發生數，不論是調整前、後之件數，均有逐月提高之現象。由此可知，修法後法院審理販賣人頭帳戶之數量，相較於修法前同時期之數量多達三倍之多，顯然應非是警方提高查緝之成果，而是販賣人頭帳戶犯罪激增之結果，否則使用人頭帳戶比例甚高之網路詐欺應有下降之現象。

### 3. 統計分析結果：

從經濟學角度而言，利用提高刑罰的手段來嚇阻犯罪量應是比較節省成本、有效果的，且1973年美國經濟學者Ehrlich所做實證研究亦發現<sup>213</sup>：平均定罪率每增加1%，則犯罪之數量即降低0.99%；而平均之有期徒刑每增加1%，則犯罪量降低1.12%，亦可為此佐證。然而，綜合以上實證分析之結果，可以看出法院在修法後，審理同樣販賣一本之被告平均量處刑度，不僅未有提高之現象，反有略微下降之趨勢。且法院審理販賣人頭帳戶之案件數於修法後較修法前激增三倍之多，顯見提高刑度之預防犯罪手段，並未達到當初修法時「提高刑度，以求達到有效嚇阻及制裁犯罪之效果」的目的。換言之，提高刑罰之犯罪的手段，既無法降低人頭帳戶之犯罪量，自無法達到從防制「人頭帳戶」的角度來防制詐欺之目的，況且，前開數據亦證明網路詐欺之發生率，並沒有

<sup>213</sup>Ehrlich, Isaac, "Participation in Illegitimate Activity: A Theoretical and Empirical Investigation", Journal of Political Economy, Vol. 81, No. 3 (May - Jun., 1973), page 521-565.

因修法提高刑度而有降低之現象，反而有顯著增加犯罪量的趨勢。至於提高刑罰之犯罪防制策略，無法降低人頭帳戶犯罪量之原因，本文試分析如下：

#### (一) 法院普遍之刑度並未因修法而提高

從理性犯罪者之角度而言，如法院宣判之刑度確有因為修法而普遍提高刑罰，則潛在犯罪者在知悉的狀況下，才會發生預期之嚇阻作用。然而，從前開統計修法前後法院實際宣判之刑度來觀察，同樣是被告每賣一個帳戶之刑度，法院普遍之刑度並未因修法之提高法定刑度而提高，反而略為降低。而歸納法院量刑於修法後並未提高之原因，不外乎有以下幾點：第一，法院適用法條之紊亂：實務個案審理販賣人頭帳戶案件之部分法官有的認為販賣人頭帳戶並不會構成洗錢防制法，有的法官又認為僅為構成洗錢防制法第 9 條第 1 項之幫助犯，而從統計結果發現，地方法院之法官在犯罪時間點為修法後之個案上<sup>214</sup>，適用洗錢防制法第 9 條第 1 項之案件有 13.21%，而適用第 9 條第 2 項之案件僅有 0.91%，大部分之地院法官只適用普通刑法之規定，導致個案審理之法官不見得均會適用洗錢防制法修法之法條，更遑論會考量到洗錢防制法第 9 條第 2 項提高法定刑之修法目的。第二，因為修法時洗錢防制法第 9 條第 2 項法定刑提高之方式，是提高有期徒刑處罰之「上限」，並非採取將法定刑設定下限之方式來提高刑罰，故依我國法官量刑採自由心證之方式，法院法官在審理修法後始發生販賣人頭帳戶之案件時，不提高判決之刑度，亦不會有違背法令之情形。

簡言之，即修法後法院之量刑上，對於每賣一本帳戶之被告所處之刑度相對於修法前低，顯然並未依照修法之要求而提高刑度，理論上，即難產生對潛在犯罪者有嚇阻之作用。

#### (二) 預期制裁犯罪成本過低

刑事制裁是有機率的，故當懲罰程度等於犯罪利得即犯罪嚴重程度時，對潛在犯罪者是沒有嚇阻的效果。所以，理想的懲罰應該超過 45 度線之完全賠償線到實際懲罰線之間（如圖 19），則若預期懲罰曲線下降至完全賠償線以下，在犯罪嚴重性於 S1 與 S2 範圍間之內，犯罪預期利益超過犯罪行為人可能面對的損失，則犯罪對潛在犯罪者是有利可圖的，在此情況下，犯罪將會發生（如圖 20）。因此，我們可以知道懲罰的嚴厲或提高受制裁之機率，均可迫使潛在犯罪者放棄從事犯罪。

<sup>214</sup> 犯罪時間點為 2003 年 8 月修法後之販賣人頭帳戶案件，始有適用洗錢防制法第 9 條第 2 項之情形，否則在修法後而個案審理之犯罪時間點在 2003 年 8 月前，則依目前刑法「從輕從新」原則，無從適用提高法定刑之新法。

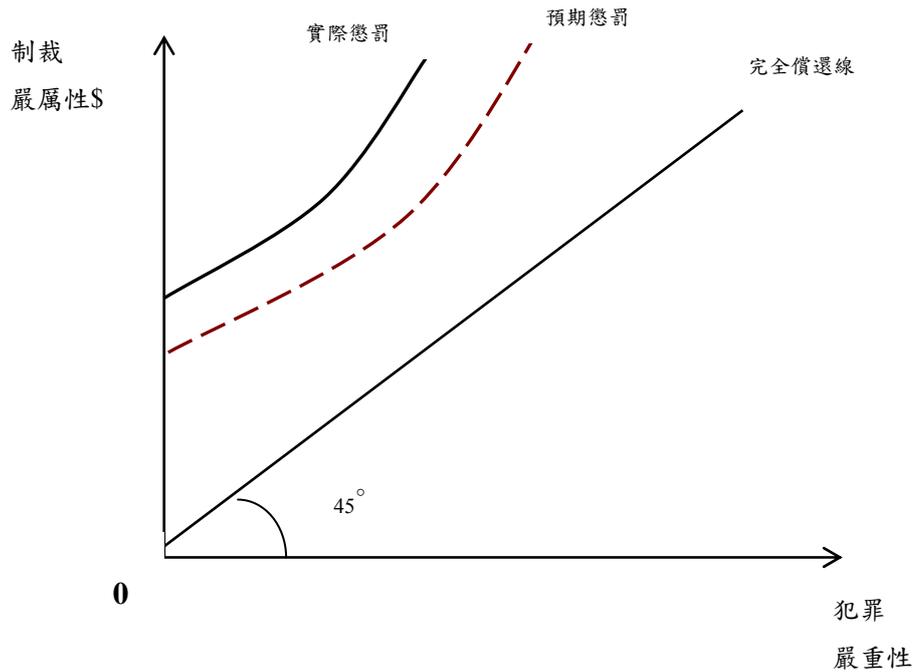


圖 19 理想的懲罰狀況圖

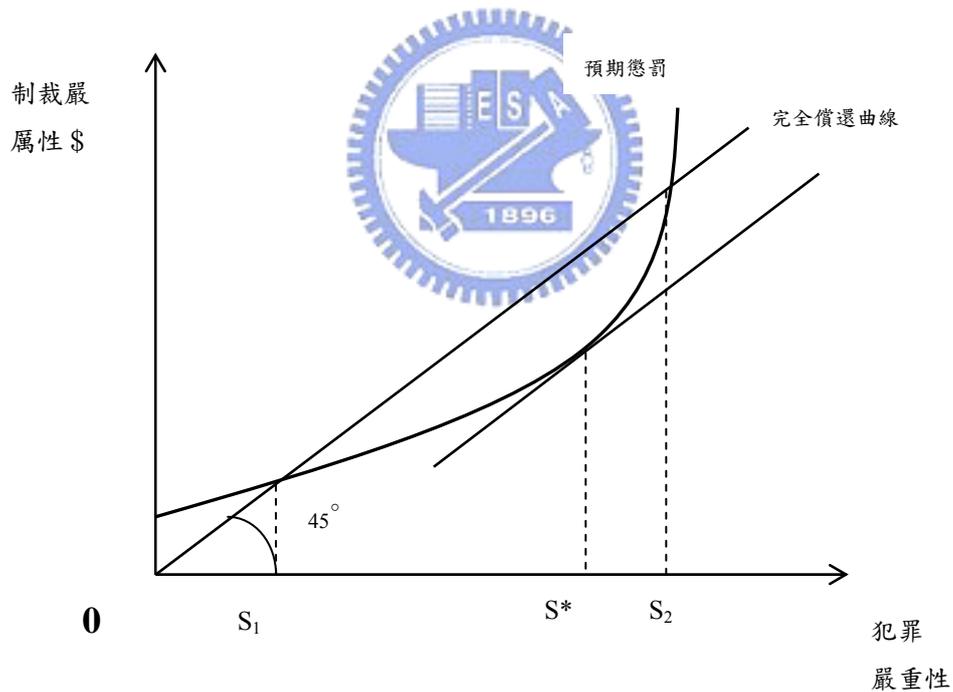


圖 20 預期制裁成本與犯罪決策圖

修法後販賣人頭帳戶之犯罪量遠較修法前多，則在販賣人頭帳戶之市場供給量大增的情況下，供給曲線會往右移，即人頭帳戶之市場價格自然會下降，此從前開實證之結果：修法前、後每本帳戶販賣報酬分別為 3188.02 元、2638.60 元，可為佐證。

而對一個理性的犯罪者而言，假設販賣人頭帳戶之「受制裁之機率」（被逮捕率×定罪率×執行率）在修法前後都一樣時，理論上，在修法後被告每賣一

本之平均犯罪利得降低 17.23%(修法前、後每本利得分別為 3188.02 元、2638.60 元)、平均刑度(修法前、後每本所處之平均刑度為 2.45、2.22 個月)僅下降 9.38%的情形下,潛在犯罪者在衡量犯罪利得與預期犯罪成本<sup>215</sup>後,應不會有誘因從事犯罪,而能有效降低販賣人頭帳戶案件之犯罪量。然而,從前開實證分析顯示,縱使修法後販賣每本帳戶之犯罪利得較原來降低 17.23%時,潛在犯罪者仍願意繼續從事販賣帳戶之犯罪行為,原因在於潛在犯罪者衡量犯罪利得與預期犯罪成本後認為,即使修法後之每本帳戶犯罪利得變少,但相對的法院量刑也變低,在其他條件不變之情況下,犯罪預期利益仍然超過犯罪行為人可能面對損失之時,即預期懲罰曲線仍然在完全賠償線以下,則犯罪對潛在犯罪者仍是有利可圖的,在此情況下,更多的潛在犯罪者願意投入販賣人頭帳戶之市場,加入販賣人頭帳戶之行列,這即是販賣人頭帳戶案件犯罪量上升之原因。

又若觀察一個更長期的時間,即修法前、後一年販賣人頭帳戶之逐月案件量曲線是呈現上升的趨勢,換言之,即此種販賣人頭帳戶之犯罪數在本事件之觀察期間是持續攀升的。由此可知,不論修法前或修法後,對於潛在犯罪者而言,「犯罪利得」必是高於「預期犯罪成本」,否則不會願意投入販賣人頭帳戶之市場。也許,我們可以說不論修法前後,法院量刑都偏低,即法院刑罰的程度並未與犯罪行為的不法內容與罪責程度相當,導致無法達到「罪得其罰」、「罰當其罪」之防止犯罪之理想目標。但是,對於此種販賣人頭帳戶之犯罪量刑,我國法院普遍之刑度是否偏低,似無客觀衡量之標準,故我們無法妄下斷語認為,法院量刑偏低,就是導致此種犯罪量居高不下的主因。而且,在刑事政策及比例原則之衡量上,亦不可能要求法官量刑無限提高,如此亦會導致侵害法益較輕之罪而判刑較法益侵害較大之罪為重的輕重失衡狀況。因此,我們再觀察另一影響「預期犯罪成本」之因素,即「受制裁之機率」。之前已經談到,我們假設販賣人頭帳戶之「受制裁之機率」在修法前後都一樣時,不論修法前或修法後,對於潛在犯罪者而言,「犯罪利得」應高於「預期犯罪成本」,則依據實證得到之數據,修法前每賣一本帳戶之利得為 3188.02 元,而每賣一本法院所處之平均刑度為 2.45 個月,則將平均刑度換算為易科罰金之代價換算(現行刑事訴訟制度之易科罰金制度,係以一日以新台幣 900 元計算,一月算 30 天)後可知,在修法前潛在犯罪者主觀之「受制裁之機率」應是低於 4.82%,這可能是因為潛在犯罪者低估或是不清楚真實的定罪率。從而,我們認為若能適度提高法院實際宣判刑度及受制裁機率,應可降低販賣人頭帳戶之犯罪發生數。

<sup>215</sup> 預期犯罪成本 = 法院量刑嚴厲性與受制裁機率之組合。

## 五、依理性犯罪模式架構提出建言

由以上實證及經濟分析結果可知，我國採取從「人頭帳戶」角度來防制詐欺之策略，對於降低網路詐欺之犯罪量並無成效。故本文嘗試依理性犯罪模式架構，從降低犯罪利得、提高定罪率及提高刑罰此三方面提出防制網路詐欺之建言，希望能供作刑事司法政策之參考：

### 5.1 降低被告犯罪利得方面

從前揭實證調查結果可知，我國網路詐欺之被害人 90.15%均是以 ATM 轉帳匯款方式交付金錢，若能移除犯罪者利用人頭帳戶取款之管道，應能有效降低該種類型案件之發生數。而此種犯罪對象之移除，可分成三部分說明

#### 一、交易付款機制

在網路交易中，若是 B2C 的交易行為，消費者在付款時無論是以信用卡刷卡或是以 ATM 轉帳，因為交易對象為企業或公司，若日後有交易糾紛，較不會發生求償無門的情形。反之，在 C2C 的交易模式，因交易者可隱匿自己之真實身分，則在此模式交易下，網路詐欺案件之發生層出不窮，且在我國發展 C2C 交易的市場障礙，主要在於 C2C 的付費機制尚不完善及網路交易者對交易安全之顧慮<sup>216</sup>，故如何選擇交易模式，藉以提高網路購物交易之安全性，實乃值得關心之課題。何況，從前開實證分析之網路詐欺案件，亦多屬 C2C 的交易模式下所產生之詐騙行為，故就網路交易付款面而言，若能在付款機制上面來防堵網路詐欺，即以移除犯罪者利用人頭帳戶取款之管道，定能有效降低該種類型案件之發生數。

國內上網人口使用之拍賣網站，以「eBay」及「Yahoo!奇摩」為大宗。而「eBay」及「Yahoo!奇摩」均致力於維護網路交易安全。在 eBay 的部份，從 2004 年 10 月 1 日起強制實行「賣家登記信用卡」的措施<sup>217</sup>，希望藉由提早在第一道關口做把關，先行過濾不肖賣家以降低買家碰到詐騙的機率，讓網路交易更安全。此外，2003 年 eBay 也宣布推薦從帳款線上代收代付起家的易付網 ezPay 成為其台灣區的拍賣服務合作夥伴，該家公司運用其原有金流機制，再加上履約保障服務，也被經濟部認定為履約保障機制的示範廠商<sup>218</sup>。同時，eBay 也在 2004 年 2 月底引進美國 PayPal 的線上付款機制<sup>219</sup>，作為跨國買賣使用美金進行交易時的金流安全平台。至於國內的另一家拍賣網站龍頭業者「Yahoo!奇摩」，目前所採取的措施和 eBay 亦為大同小異，同樣藉由信用卡認證<sup>220</sup>以及

<sup>216</sup>林豪鏘，電子商務，第 2 至 42 頁，旗標出版股份有限公司，2005 年 6 月版。

<sup>217</sup>見 <http://pages.tw.ebay.com/securitycenter/sv.html>，(2006/Jan/1)。

<sup>218</sup>參 <http://www.neweb.com.tw/partners.htm>，(2006/Jan/1)。

<sup>219</sup>參見如下網址：<http://www.ettoday.com/2004/02/26/10846-1592272.htm>，(2006/Jan/1)。

<sup>220</sup>參見如下網址，<http://tw.help.yahoo.com/auct/faq/ccd/index.html>，(2006/Jan/1)。

金、物流服務<sup>221</sup>及與履約保障<sup>222</sup>，來防堵可能遭遇到的網路拍賣詐欺問題。

而國外較普遍之網路交易安全之付款機制有 PayPal 及 Escrow（電子商務交易履約保證）二種方式。以下分別介紹之：

#### （一）PayPal 之線上付款機制：

美國 eBay 採用 PayPal 作為買賣方的購物安全保障，PayPal 是 eBay 提供線上付款和收款服務的子公司，在 PayPal 系統裡，支付款項的方式有兩種：使用信用卡和使用 PayPal 帳戶內的餘額。如果自己的 PayPal 帳戶沒有餘額，就只能持信用卡向 PayPal 刷卡，PayPal 在支付款項給賣方；如果 PayPal 帳戶有餘額（例如有國外買家付款到自己帳戶），就可以把餘額放在帳戶裡當購物基金，也可以把餘額提領出來。

使用 PayPal 對買家的好處如下：1.即時付款：線上即時付款，方便快捷。2.購物有保障：在美國 eBay 買東西，享有「PayPal 買家購物保障方案<sup>223</sup>」。3.速完成交易：因為付款快速，賣家很快地收到款項後，可盡早把物品寄出。

使用 PayPal 對賣家的好處：1.早收到款項：線上即時收款，方便快捷。2.完成交易：賣家更快收到款項後，就能提早把物品寄出，完成交易。3.式管理工具及服務，讓賣家更方便。

eBay 也在 2004 年 2 月底引進美國 PayPal 的線上付款機制<sup>224</sup>，作為跨國買賣使用美金進行交易時的金流安全平台。美國 eBay 拍賣網中消費者有 70% 以用 PayPal 來付款，然而，我國網路交易者並不習於使用 PayPal，有可能是消費者仍不習慣在網路上使用信用卡消費、購物，此與本文調查發現網路詐欺之被害人 90.15% 以 ATM 轉帳匯款之結果不謀而和。由此可見，礙於國人使用 ATM 轉帳匯款之消費習慣，及 ATM 櫃員機設立之普及，則我國引進美國 PayPal 之線上付款機，無法誘使網路交易者大量使用該機制，從而，亦無法藉此制度來防杜網路詐欺之發生。

#### （二）電子商務交易履約保證（Escrow）制度

美國另一付款機制為「電子商務交易履約保證」（Escrow），Escrow 係以第三者獨立客觀地位受交易雙方委任，收取消費者給付之價金後，需先將買方價金存入銀行之信託帳戶，之後，旋即通知賣方發出商品，惟需俟消費者收到商品且在鑑賞期間內無退貨之要求時，Escrow 業者始可將價金轉交付給賣家<sup>225</sup>。

使用 Escrow 對買家的好處如下：1.物有保障：網路 Escrow 經營者

<sup>221</sup> 見 <http://tw.bid.yahoo.com/phtml/auc/tw/ezPay/home.html>，(2006/Jan/1)。

<sup>222</sup> 見 [http://tw.bid.yahoo.com/phtml/auc/tw/tos\\_add/protection.html](http://tw.bid.yahoo.com/phtml/auc/tw/tos_add/protection.html)，(2006/Jan/1)。

<sup>223</sup> 見 [http://www.paypal.com/cgi-bin/webscr?cmd=\\_pbp-info-outside](http://www.paypal.com/cgi-bin/webscr?cmd=_pbp-info-outside)，(2006/Jan/1)。

<sup>224</sup> 參 <http://www.ettoday.com/2004/02/26/10846-1592272.htm>，(2006/Jan/1)。

<sup>225</sup> 翁靖珊，「交易履約保證機制法律面探討」，電子商務導航，第 6 卷，第 7 期，2004 年 6 月 16 日。可參 <http://www.ec.org.tw/Htmlupload/6-7.pdf>。

會確定買方收到貨品後，始會將價金交付賣方，不會有買家付錢後收不到貨的情形。2.付款安全性提高：因為買家是向網路 Escrow 經營者付款，不會有款項匯入人頭帳戶之風險。

使用 Escrow 對賣家的好處：1.高交易之信心：因此制度會使買家更有誘因在網路上購物，有促於網路交易更之達成。2.貨之處理：賣家在處理買方要求退貨時，亦可透過網路 Escrow 業者，確保價金可返還至買方。

台灣之藍新科技股份有限公司，在 2006 年 4 月 12 日推出之付款機制「ezPay 易付通」<sup>226</sup>，與上開美國之「電子商務交易履約保證」(Escrow) 制度極為類似。藍新公司「ezPay 易付通」之付款方式為：網路交易買賣之雙方約定使用「ezPay 易付通」後，買方可選擇網路 ATM、信用卡、ezPay 帳戶餘額等三種方式之一付款給 ezPay，ezPay 會通知賣方已收到款項，賣方可以放心出貨；待買方確認收到貨品無誤，即可提示 ezPay 將款項交付給賣方，完成交易。

然而，Escrow 制度對賣家最不利之處在於，會延遲收到貨款的時間，賣家比較沒有誘因想要使用此制度來保障雙方之交易安全。Escrow 交易方式雖在我國尚處於萌芽階段，然如前所述網路 Escrow 經營者需將買方價金存入銀行之信託帳戶，則買方將價金存入銀行之方式，則可選擇以 ATM 轉帳匯款方式為之，故此種交易制度而言，相較於 PayPal 的線上付款機，更能誘使我國網路交易者使用。只是相較於賣方而言，因此 Escrow 交易制度，會延緩買方收到款項之時間，則需要增加一些誘因誘使買方使用此交易制度。就以我國二大網路拍賣平台 eBay 及 Yahoo! 奇摩為例，eBay 提供交易平台之收費來源為收取 5%刊登費及 5%交易費，而 Yahoo! 奇摩目前收取每件 3 元之刊登費<sup>227</sup>及 5%交易費，則若 eBay 及 Yahoo! 奇摩二家網路公司可約定若採用 Escrow 交易制度的賣家可減免刊登費或交易費，則賣家會有極大之誘因想要使用此制度來從事交易，並可大大提升雙方之網路交易安全。

從法律經濟分析之觀點而言，有經濟學者認為能將社會成本極小化，亦是有效率的犯罪制裁手段。故對執司犯罪偵查與防制之司法、警政機關而言，選擇一個相對社會成本較小之防制手段，且能提高「犯罪成本」，方能達到遏止販賣人頭帳戶犯罪發生最大之效用。而如上所述，建議經營拍賣網站之業者使用 Escrow 交易制度並以減少甚至減免刊登費之方式來誘使賣方多多使用此制度，應能有效移除犯罪者利用人頭帳戶取款之管道，即確實能提高潛在犯罪者之「犯罪成本」，以達到預防網路詐欺發生之目的，而此種犯罪預防之成本，應是遠較執法機關在偵辦

<sup>226</sup> 藍新科技推出 ezPay 易付通保障網路交易安全，大紀元，2006 年 4 月 12 日，  
<http://www.epochtimes.com/b5/6/4/12/n1285340.htm> (2006/May/4)。

<sup>227</sup> YAHOO 奇摩拍賣網站於 2004 年 4 月 9 日起，開始向賣家收取刊登費，採取先刊登後付費之方式。

此種販賣人頭帳戶以從事詐欺之案件所耗費之成本（確定犯罪嫌疑人、調查相關證據、進行逮捕、偵查、審判及執行等等社會成本）來的低，故此種防制手段之採取，從經濟學的角度以觀，應可謂是有效率的。再者，對於經營拍賣網站之業者而言，經常發生網路拍賣詐欺，亦有損於拍賣網站之網路安全之信譽，而此信譽之高低，亦會直接影響現行或潛在網路使用者使用該拍賣網站交易平台從事網路交易之意願。從而，理論上，網路拍賣經營者應有誘因來選擇以低成本之方式來預防網路詐欺犯罪之發生，而前開 Escrow 交易制度之實施，應是拍賣網站經營者能有效降低網路詐欺之方法之一，只是，法律亦應提供一定之誘因，來促使拍賣網站經營者更有意願投入成本來預防犯罪之發生，而本文則建議執行機關得定期公開網路詐欺報案者在各拍賣網站發生之比例，並讓廣大之消費者知悉進而選擇網路詐欺發生率較低之拍賣網站從事交易，由此公開被害者被害之犯罪資訊，間接促使拍賣網站更有意願為維護該網站之交易安全而投入成本來預防犯罪之發生。

## 二、金融機構之開戶

不論是網路詐欺或是其他類型之詐欺集團，多係利用人頭帳戶來騙取被害人之金錢，顯見銀行業者在防堵人頭戶方面應有再加強之必要。而且從開戶階段來防止人頭戶之氾濫，實為移除犯罪者利用人頭帳戶取款之管道，亦為「提高犯罪成本」之降低犯罪量手段之一。

### （一）目前金融機構防制人頭戶之措施：

在討論如何從銀行開戶階段來防堵人頭帳戶前，應先來看看目前之金融帳戶做了哪些防制人頭帳戶之措施。金融機構目前有以下防制人頭戶之措施：

#### 1. 金融機構受理開戶採「雙卡認證」措施：

2004年5月10日起，金融機構受理開戶（包括個人戶及非個人戶），已實施雙重身分證明文件查核及留存該身分證明文件。個人戶部份，除身分證外，並應徵取其他可資證明身分之文件，如健保卡、護照、駕照或學生證等。非個人戶部份，除登記證照外，並應徵取董事會議紀錄、公司章程或財務報表等<sup>228</sup>。又2006年4月27日發布之「異常帳戶管理辦法」亦於第13條第1項明白規定此雙重認證機制。

#### 2. 金融機構受理開戶時，保留錄影機錄攝之影像檔，並採「建立新開戶影像檔案」措施：

金融機構於辦理客戶開戶時應注意防範歹徒以人頭或持偽變造身分證開立存款帳戶情事。另金融機構於辦理客戶開戶時，錄影機錄攝之影像檔，應保存至少六個月<sup>229</sup>。又金融機構對新存戶開戶時應建立影像檔案，而此之方式，不限於採拍照方式，亦可於現行機制下加強開戶櫃檯

<sup>228</sup> 財政部2004年4月28日台財融（一）字第093100318號函示。

<sup>229</sup> 財政部2001年4月3日台財融（一）第90733071號函。

監視錄影設備且錄影檔案獨立保存<sup>230</sup>。

### 3. 金融機構落實執行確認客戶原則：

2004年3月15日財政部函知各金融機構<sup>231</sup>：「為防範人頭帳戶及保障金融機構本身聲譽，金融機構應確實落實執行認識自己客戶原則，包括訂定一套認識客戶及審慎評估客戶之內部規範，如對於新開戶者，訂有標準流程來確認客戶身份並瞭解客戶；對於舊客戶，應明定相關措施，以持續注意其交易行為是否與其身份、收入或營業性質一致。此外，各金融機構如發現可疑帳戶時，應立即通報檢、警、調單位，以維護社會治安。」

#### (二) 金融機構應審慎把關開戶之申請

金融機構雖然有以上之防堵人頭帳戶之措施，然我國人頭帳戶之氾濫仍是普遍存在之現象，顯見金融機構在防堵人頭帳戶上仍有缺失，以致全民反詐騙的戰略防線，出現一個大缺口，肇致詐騙案件依舊氾濫，探究根本原因在於我國人頭戶開戶取得之氾濫，其實多肇因於金融機構業績掛帥，金融機構並不考慮申請開戶者之個人信用評等，只要來申請開戶，並攜帶相關之證件，即可取得開戶之資格，顯然過於浮濫且無過濾之機制。故除了司法、警政機關之防制人頭帳戶行動外，反制動作更應拉到銀行開戶階段，作為阻絕「詐欺集團利用人頭戶犯罪」之第一線，才能釜底抽薪。故本文認為金融機構應採取下列行為：

#### 1. 建立個人信用評等制度

應仿美、日等國將個人信用商品建立個人信用評等制度<sup>232</sup>，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，方有如此，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<sup>233</sup>。

目前我國有以下幾種管道可得知個人之信用狀況<sup>234</sup>：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動資料查詢；向票據交換所拒絕往來戶查詢；信用卡停卡紀錄查詢；支存照會查詢等。本文建議金融聯合徵信中心應比照信用卡等建立金融卡、存戶基本資料徵信檔，銀行等金融機構凡受理開戶申請應即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），銀行於

<sup>230</sup>財政部2003年12月10日台財融（二）字第0922001638號函釋。併依中華民國銀行商業同業公會全國聯合會研議之「國內金融機構受理存戶新開戶建立影像檔注意事項」辦理。

<sup>231</sup>2004年3月15日台財融（一）字第0938010347號函。

<sup>232</sup>李禮仲，開戶拍照消滅人頭戶財政部淪為採證部，聯合報，民意論壇，2003年11月1日。

<sup>233</sup>存款不見人心慌慌，藍天電子報，第61期，2003年10月16日，

<http://www.kmt.org.tw/epaper/Papers/921016/P4.html>，(2006/Mar/17)。

<sup>234</sup>消費者貸款審查要領及信用評等，<http://www.tabf.org.tw/tw/pub/preview/S0087.pdf>，(2006/Mar/17)。

准許個人開戶之申請時均應審慎調查，若開戶申請人無法提供合理解釋時，即應拒絕開戶之申請。另 2006 年 4 月 27 日發布之「異常帳戶管理辦法」固於第 13 條第 2 項規定銀行「應」拒絕客戶開戶申請之情形，惟此部分之辦法有逾越母法授權範圍之違法，故金融機構不宜逕以此辦法作為拒絕人民開戶之依據，充其量僅能作為參考標準。

又目前聯合徵信中心只供加入會員的金融機構查詢客戶及提供個人查詢，本文主張且應開放供大眾查詢，並改採使用者付費方式，使每個人都能取得個人信用評等，讓每個人的信用評等成為公共財。

## 2. 各銀行存款戶中涉嫌偽冒開戶、人頭帳戶數量與比率：

依據內政部警政署之人頭資料庫數據統計，自 2003 年 7 月 30 日至 2005 年 10 月 20 日止，人頭帳戶共 55,852 筆，其中郵局、銀行共 55,747 筆佔 99.81%、合作社、農漁會信用部 105 筆佔 0.19%<sup>235</sup>，金融機構之主管機關即行政院金管會銀行局應公布各金融機構存款戶中人頭帳戶數量與比率，並對於人頭帳戶較多的金融機構，積極深入查明該等金融機構人頭帳戶猖獗之真正原因，以瞭解其內部監督控制流程，且確實執行要求金融機構提出改善報告外，並約談其負責人，及責成金融機構稽核單位加強督導，如仍未改善，情節嚴重者，將依違反銀行法第 45 條之 1 核處罰鍰<sup>236</sup>或依銀行法第 61 條之 1 限制部分業務、解除負責人、經理人、或職員職務或其他必要處置等<sup>237</sup>。

## 三、可疑帳戶之凍結

「警示帳戶通報機制」之運作，縱使在銀行法第 45 條之 2 修正公布及「異常帳戶管理辦法」發布後，仍有違法行政處分之法律爭議，已如前述，即警示帳戶之合法性，迄今仍未取得合法之正當性。故在合法、合憲性要求之前提下，承辦詐欺個案之警調單位，應循合法途徑依照洗錢防制法報請檢察官或法官以命令方式將帳戶凍結，或是促請金融機構依照「異常帳戶管理辦法」第 4 條第 3 類之情形，自行暫停帳戶全部或部分交易功能。藉此移除犯罪者繼續利用人頭帳戶取款之管道，進而阻礙網路詐欺案件之發生。

## 5.2 提高受制裁機率方面

除加重刑罰外，提高查獲、定罪或執行率亦為提高理性犯罪者預期犯罪成本之方法。而目前警察機關多為查獲被告詐欺案件後，方清查被害人匯入款項之帳戶是否為人頭帳戶，此一方法，本文以為過於被動與消極，一方面因為網路詐欺等新興詐欺案件之查獲率本來就不高，從而就會影響人頭帳戶之查獲率，又網路詐欺等新興詐欺案件有許多是被害人雖然接獲詐欺訊息，但是實際上並未匯款，此種案件雖然在警方並不屬於「案件」，但是警方若是循線追查，

<sup>235</sup>內政部警政署刑事警察局提供，資料並未公開。

<sup>236</sup>依銀行法第 129 條第 7 款處新台幣 200 萬元以上 1000 萬元以下罰鍰。

<sup>237</sup>銀行櫃檯 反詐騙最前線，自由電子報，

<http://www.libertytimes.com.tw/2005/new/apr/22/today-so8.htm>，(2006/ Mar /17)。

應該也可以查獲人頭帳戶，甚至進而預防有更多的人受害，所以，警方如果能以更積極、主動的方式來查緝人頭帳戶，本文以為可以不在增加設備、人力、資源的情形下就可以增加人頭帳戶的查獲率，使出售人頭帳戶的犯罪者的預期懲罰升高，從而降低人頭犯罪。

而在 2006 年 4 月 27 日發布之「異常帳戶管理辦法」不僅利用將警示帳戶所產生之「衍生管制帳戶」暫停臨櫃提領以外功能，以防止有更多被害人繼續匯款受損外。更進一步在辦法第 5、7 條規定銀行應主動配合警調司法機關主動查緝犯罪之義務，包括：1. 存款帳戶經通報後，銀行如發現詐騙款項已匯至其他帳戶，應將該筆轉出之資料通報原通報機關。2. 銀行對有該辦法第 4 條第 3 類之疑似不法或顯屬異常之存款帳戶，並需進行查證及持續監控，如經查證有不法情事，即應通報司法員警機關。

### 5.3 提高刑罰方面

#### 5.2.1 提供人頭帳戶之刑責方面

我國洗錢防制法 2003 年之修法固然提高販賣人頭帳戶之法定刑，然而法院量刑並未因修法而加重，歸咎原因不外乎為地方法院適用法律見解之紊亂及修法僅提高處罰之上限等因素，導致修法後法院之平均刑度並未提高反而有略微降低的狀況。簡言之，提供人頭帳戶之犯罪，本可藉由洗錢防制法之修法提高刑罰之手段，來降低犯罪量，然而，因為執行面並未落實刑罰之提高，導致無法達到嚇阻潛在犯罪者之目的。

刑法於 2005 年 2 月 2 日修正公布刪除刑法第 340 條之常業詐欺罪，並訂於 2006 年 7 月 1 日施行；而洗錢防制法亦於 2006 年 5 月 30 日修正公布，擬於同年 11 月 30 日施行，同步將刑法第 340 條常業詐欺之罪，移除在洗錢防制法所屬之「重大犯罪」之列<sup>238</sup>。屆時提供人頭帳戶予他人從事詐欺之犯罪行為，不僅無從論以刑法常業詐欺幫助犯之罪責，亦無法適用洗錢防制法第 9 條第 2 項來加重其刑，從而，個案之法院於審理提供人頭帳戶之犯罪時，又回歸到僅能適用普通刑法之狀況，而依照我國實務普遍量刑之平均刑度，顯然是不足以嚇阻想要提供人頭帳戶以牟利之潛在犯罪者。

故在 2006 年 7 月 1 日以後，提供人頭帳戶之犯罪，即無法藉由洗錢防制法 2003 年修法提高刑罰之手段，來達到遏止犯罪之效果。因此，必須以強力宣導方式促請法官能同步加重個案之量刑，並能適度地運用併科罰金之手段，來提高犯罪者之預期犯罪制裁成本。

#### 5.2.2 使用人頭帳戶之刑罰部分

作者從事犯罪偵查實務工作發現，不論是一般詐欺或是網路詐欺，詐騙者多利用「人頭帳戶」來進行取款，並藉此逃避查緝。換言之，即詐騙行為通常

<sup>238</sup>洗錢防制法 2006 年 5 月 30 日修正公布，訂於同年 11 月 30 日施行，將原第 3 條第 1 項第 5 款明文刪除之，參 2006 年 5 月 30 日華總一義字第 09500075731 號函。

伴隨著使用人頭帳戶之行為態樣，從而，販賣人頭帳戶之犯罪型態，可謂是詐欺案件之「衍生犯罪」，或可稱為「前置犯罪」行為。而如前所述，販賣人頭帳戶是另一個供需市場，提供者之供給曲線，會因使用者之需求曲線產生變化。因此，根本解決詐欺集團利用人頭帳戶氾濫之問題，可從另一思考面向即「如何降低人頭帳戶之需求」來考慮。依照理性犯罪模型，從提高「詐欺集團利用人頭帳戶」之預期犯罪成本來看，若能提高「使用人頭帳戶從事詐欺者」之刑罰，則必將提高詐欺者利用人頭帳戶之成本，理論上，應能有效降低「使用人頭帳戶從事詐欺」之犯罪量，如此，不僅可正本清源解決詐欺日益猖獗的問題，亦可間接降低人頭帳戶市場之需求。

在現行制度下，使用人頭帳戶從事詐欺之犯罪行為，依實務之見解本應一同適用刑法常業詐欺罪及洗錢防制法第9條第1項之掩飾、隱匿因自己重大犯罪所得罪，惟法院在論罪科刑時，均認觸犯詐欺罪與洗錢防制法之罪係一行為觸犯數罪名，從一重即常業詐欺罪處斷即可。然而，審判上法院在個案上即使是利用人頭帳戶從事詐欺之犯罪，並不會均認定都是常業詐欺之行為，故不見得均會處以一年以上之有期徒刑，何況，刑法於2005年2月2日修正公布刪除刑法第340條之常業詐欺罪，而於2006年7月1日施行後，使用人頭帳戶從事詐欺之犯罪行為，不僅法院量處刑度時不受法定刑「有期徒刑一年以上」之限制，且在洗錢防制法第3條第1項第5款亦同步刪除之情況下，即無適用洗錢防制法之虞地，從而，個案之法院於審理時，是否會審酌利用人頭帳戶從事犯罪之情節而處以較高之刑度，則不得而知。

依此，本文建議提高刑罰之方式，或可參考竊盜罪之加重要件，將使用人頭帳戶列為詐欺之加重條件；又或是參考刑法業務侵占之規定，將「使用人頭帳戶從事詐欺」列為特殊之類型，同時提高法定刑之上限與下限，以收遏止之效<sup>239</sup>。

#### 5.4 從成本分析看防制手法之可行性

經濟學家認為犯罪行為是一種非自願性的交易，且形成負的外部性<sup>240</sup>。犯罪所產生之社會成本，包括事前預防犯罪之費用及事後制裁犯罪者之費用。而前開提出之各種防制建言中，其中採用「Escrow 交易機制」、「加強開立帳戶的查核機制」、「可疑帳戶之凍結」均屬事前犯罪之預防；「提高人頭帳戶查獲率」及「提高刑罰」部分，係均屬事後制裁之手段。而如何採取有效率之犯罪預防手段，則是經濟學家所重視的。若從「最低成本預防」之角度思考，在考量是否採取事前預防之「Escrow 交易機制」、「加強開立帳戶的查核機制」等手段前，

<sup>239</sup> 提高「使用人頭帳戶詐欺」之刑責，除從降低詐欺與人頭帳戶犯罪量之角度思考外，另外，如果考慮到「使用人頭帳戶詐欺」會造成之人與人彼此不信任之社會成本，與此種犯罪因查緝困難而增加之查緝成本，本文以為將此種使用人頭帳戶列為列為詐欺罪之加重要件，應屬合理。如或不然，則亦可考慮修正洗錢防制法，明確規定此種犯罪適用洗錢防制法第九條，並同時提高洗錢防制法之刑責，尤其是刑責之下限，則亦可達到提高刑責之目的。

<sup>240</sup> 同前揭註190。

我們應思考在市場交易結構下，由何人來負擔預防「販賣、使用人頭帳戶犯罪」之成本最有可能，而且承擔的成本最低？

就「Escrow 交易機制」而言，雖可有效移除犯罪者利用人頭帳戶取款之管道，惟此負擔防制成本者是在網路交易之雙方，即使用網路 Escrow 經營業者之手續費用必須由交易雙方負擔，此預防犯罪之成本，最後很有可能會轉嫁到購買物品之買家身上。而參照美國使用「Escrow 交易機制」之經驗，也許是因為網路 Escrow 經營業者收取之服務報償過高，導致「Escrow 交易機制」對小額交易來說並不划算<sup>241</sup>。而國內台灣之藍新科技股份有限公司，在 2006 年 4 月 12 日推出之類似電子商務交易履約保證（Escrow）制度之付款機制「ezPay 易付通」，其收費標準顯然低於美國之 Escrow.com 之經營業者<sup>242</sup>，理論上，對於具有小額性之網路交易買家而言，應是會有意願使用此制度。然而，目前僅有 Yahoo! 奇摩拍賣網站有提供網路交易者使用者「ezPay 易付通」之付款機制，且該付款機制尚未為網路交易者所普遍知悉或慣於使用，故仍待拍賣網站公司能提供誘因激勵網路交易雙方使用此付款機制。

另就金融機構「加強開立帳戶的查核機制」來看，若從金融機構方面來防制人頭帳戶之申請，在預防犯罪之發生上居於有利之地位。而就預防所可能產生之成本，包括：審查之成本及不准予開戶之可能經濟上之損失。至於前者，因我國已有警示帳戶通報機制，只要之前有販賣人頭帳戶之紀錄，在內政部警政署及金融聯合徵信中心都有紀錄可循，故並不需多花成本來建立審核之機制，何況，金融機構得參酌「異常帳戶管理辦法」第 13 條第 2 項拒絕客戶開立存款帳戶之情形，即可節省自行認定之不確定成本。至於後者，販賣之人頭帳戶於開戶後，多會將存摺、提款卡交付他人，並由詐欺集團之「車手」利用提款卡提領詐得款項，而在被列為警示帳戶之前，絕大多數金融機構並無機會再次提供服務並收取相關手續費用。再者，若人頭帳戶一旦被列為「警示帳戶」，則金融機構除必須終止該帳戶之全部交易功能外，尚必須進行以下之工作：1. 查證有無其他「衍生管制帳戶」，並應將暫停所有衍生管制帳戶臨櫃提領以外之功能；2. 需將「警示帳戶」、「衍生管制帳戶」匯入款項退回匯款行，若仍有餘額，則需依管理辦法第 11 條協助發還剩餘款項；3. 之後還要在符合一定條件下配合解除「警示帳戶」之手續。故就金融機構而言，不准可疑帳戶之申請不僅無何經濟損失，且可省卻列為「警示帳戶」後配合處理帳戶內款項及解除警示帳戶等繁複之程序，因此對金融機構來說不准開戶應比准予開戶更有利益。

而在提高查緝率、定罪率及執行率方面，勢必要增加警調、司法機關之費用及執行罰金刑、觀護人及監獄系統之費用，其耗費之勞力、時間、費用難以

<sup>241</sup> 如 Escrow.com 為例，就買方而言，每筆美金 5000 元以下交易收取每筆交易總額 3.25% 至 6.3% 不等之手續費；就賣方而言，則依照賣方支付款項方式之不同，而收取美金 10 到 20 不等之手續費。參 <https://www.escrow.com> 之網站。

<sup>242</sup> 易付通收費標準區分為個人會員及商務會員。個人會員每月交易限額為新台幣 2 萬元以下，則免註冊費、年費，加卡費每次 1 元，提錢每次每筆 15 元。商務會員每月交易限額為新台幣 40 萬元以下，則免註冊費、年費，加卡費每次 1 元，提錢每次每筆 15 元，另使用信用卡交易每筆收取 2.8%。

估算，而日前所發布之「異常帳戶管理辦法」，賦予金融機構在特定狀況下配合警方查緝之義務，而從最低成本預防者之角度思考，金融機構係基於直接管理帳戶交易之地位，相較於司法員警而言，顯係居於預防疑似不法或顯屬異常交易之有利地位，且由金融機構來負擔此成本，遠比司法員警所需付出之成本為低。至於在提高刑責方面，則主要增加之成本為執行之費用，然此犯制策略之採行，有一不確定因素，即是法院普遍在個案量刑上是否有欲藉提高刑罰之手段達到嚇阻潛在犯罪者之目的，而洗錢防制法第9條第2項之修正法院在販賣人頭帳戶個案上並未有提高刑責之情形，則是最好之例證。

因此，在目前現行法律制度及政策運作下，我們希望提供更多經濟或是法律上之誘因，來促使在市場交易結構中之當事人都有意願來採取預防措施。首先，我們認為，金融機構對於預防利用人頭帳戶從事詐欺之犯罪行為發生居於有利之地位，且承擔之成本相較於其他警調、司法機關來得低，故在法律、命令上明文要求金融機構於開戶前應過濾、審核可疑帳戶，且於帳戶開立後並應持續性監控帳戶之不法交易情形<sup>243</sup>，並課予申報之義務，若有違反申報之義務即需擔負洗錢防制法第7條第3項、第8條第4項之罰鍰處罰。換言之，課予金融機構相當之行政罰責任，使得金融機構內生化預防成本與利益，促使金融機構更有誘因採取預防措施。其次，如前所述，本文建議執行機關應定期公布網路詐欺報案者在各拍賣網站發生之比例，無非即是希望經營拍賣網站之業者，能夠愛惜自己之信譽，為了維護網路交易平台之交易安全，居於一個詐欺觀察者之角色，來積極投入並採取預防之措施，甚至主動提供誘因刺激網路交易雙方使用「Escrow」付款機制來降低網路詐欺之發生率。最後，我們亦期許預防犯罪最後一道防線之司法審判機關，能夠肩負刑罰預防犯罪之社會責任，在個案量刑上適度加重提供人頭帳戶及利用人頭帳戶從事詐欺之刑罰，藉此降低人頭帳戶之市場需求，亦可正本清源來解決實務上降低詐欺犯罪量之困境。如此方能在目前運行之制度下，利用較低預防成本之犯罪策略而能達到較高效率之防制效果。

---

<sup>243</sup>銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法第16條，規範金融機構應對於帳戶有交易額超過一定門檻、交易額與帳戶平均餘額顯不相當、短時間內密集使用電子交易功能等三種具體狀況持續監控，並輔以資訊系統進行補助。

## 六、結論

隨著網際網路的普及，網路技術之成熟與上網人口、時數之激增，網路使用的活動內容也日趨多樣化，伴隨而來的負面效應，即是增加了新型態的犯罪機會，其中網路詐欺犯罪之層出不窮，直接對於電子商務的發展造成嚴重威脅，加之，網路犯罪之隱匿性、即時性，導致查緝之困難性，故對於網路詐欺犯罪之防制，已成為刻不容緩之議題。依照本文實證統計之觀察發現，網路詐欺案件中有 90.15% 之被害人是以轉帳匯款方式付款，換言之，即在網路之虛擬世界中，利用人頭帳戶從事詐騙行為之比例甚高。因此，在我國防制網路詐欺，應該與其他國家採用不同的做法，而不應一味地沿襲其他國家。而從防制人頭帳戶的角度，即是一個方向。本文認為從查緝人頭帳戶之角度來防制網路詐欺之發生，應能有效降低犯罪之發生數。

依照經濟學家 Becker 提出之「理性犯罪模型」，實務上採行「警示帳戶通報機制」、「非約定轉帳限制」及「提高刑罰」之防制策略，分別為降低犯罪利得及提高刑罰之降低犯罪量手段，本文則為檢驗政策及法律之制定，是否在實際運作上達成預防「網路詐欺」犯罪之目的，試從實證統計數據檢視預防犯罪之目的是否達成，繼之，利用「法律之經濟分析」來解釋「警示帳戶通報機制」、「非約定轉帳限制」、「提高刑罰」之實際運作狀況。但經過實證分析以後發現，利用查緝人頭帳戶犯罪或從人頭帳戶角度來遏止詐欺犯罪之防制策略，對於特定之詐欺類型即「網路詐欺」，並無明顯成果。其中依照「警示帳戶通報機制」被列為「警示帳戶」之數量雖然逐年增加，但是並未同步地遏止人頭帳戶案件及網路詐欺之發生數。在「非約定轉帳限制」之政策，從實證結果發現我國網路詐欺被騙金額每筆不超過 3 萬元者高達 79.44%，故非約定帳戶之 3 萬元轉帳限制，對於大部分之小額網路詐欺案件並無限制之效果。另在「提高刑罰」方面，首先，本文研究後發現洗錢防制法之修正，並未使法院因此提高刑罰，另外，法院目前對出售人頭帳戶犯罪者的刑罰，可能還無法足夠遏止人頭帳戶犯罪。

因此，本文依照「理性犯罪模型」之模式，從網路詐欺大多利用人頭帳戶取款之特殊性著眼，並考量最低成本預防之觀念，提出用以降低網路詐欺行為發生之防制策略。在目前未變動現行法律、政策制度下，本文建議要求居於預防犯罪有利地位之金融機構應審慎開戶、監控可疑帳戶以及配合警方主動查緝之同時，亦應利用公布被害人在交易網站受害之資訊，使經營網路拍賣之業者更有誘因來善盡維護網路交易安全之責任。此外，促請地方法院在個案上適度加重刑罰，希望能在變動最小的情況下達到有效率之降低犯罪量的成效。

# 參考文獻

## 中文資料

### 書籍

4. Cooter 及 Ulen 著，法律經濟學，溫麗琪編譯，華泰文化事業公司，第 2、3 頁，2003 年 6 月初版。
5. Richard A. Posner 著，法律的經濟分析，蔣兆康譯，第 292 頁，中國大百科全球出版社，1997 年。
6. 甘添貴，體系刑法各論第一卷侵害個人專屬法益之犯罪，第 10 頁，自版，1999 年 9 月初版。
7. 吳庚，行政法之理論與實務，增訂 4 版，第 77、83、88、92 頁，自版，1998 年。
8. 吳照琰，「網路入侵型犯罪法治議題分析」，財團法人資訊工業策進會科技法律中心戴豪君等合著，數位科技法律大未來，第 137 頁，2004 年 12 月。
9. 林豪鏘，電子商務，第 2 至 42 頁，旗標出版股份有限公司，2005 年 6 月版。
10. 國立交通大學科技法律研究所，調查研究方法手冊，第 21 頁，2004 年 1 月。
11. 許春金，犯罪學，修訂 3 版，第 174 至 185 頁，自版，2000 年 8 月。
12. 馮震宇，「我國網路犯罪類型及案例探討」，網路法基本問題研究（一），第 337 頁，學林出版社，1997 年 7 月 1 日。
13. 黃茂榮，法學方法與現代民法，第 308 頁，自版，1993 年。
14. 黃榮堅，「電腦犯罪的刑法問題」，刑罰的極限，元照出版社，第 202 頁，1999 年。
15. 楊仁壽，法學方法論，第 123、130、154 頁，三民書局，1994 年。
16. 葉奇鑫，刑法有關電腦（網路）犯罪研修資料彙編，法務部印製，2002 年 12 月。
17. 熊秉元，熊秉元漫步法律，第 20 至 37 頁，時報文化出版，2003 年。
18. 蘇南桓，洗錢防制理論與實務，第 200 頁，自版，1997 年 10 月初版。

### 期刊

1. 「國內經濟金融日誌」，中央銀行季刊，第 27 期卷第 2 期，2005 年 4 月份。
2. 王藏偉，「公開收購有價證券之制度及運作淺析」，證券暨期貨月刊，第 23 卷，第 7 期，2005 年 7 月 16 日出版。
3. 李傑清，「洗錢罪保護法益及處罰」，月旦法學，第 115 期，第 23 頁，2004 年 11 月。
4. 林宜隆，「網路犯罪之案件分析」，中央警察大學學報，第 37 期，第 224 頁，2000 年。
5. 翁瑋珊，「交易履約保證機制法律面探討」，電子商務導航，第 6 卷，第 7 期。
6. 高大宇、王旭正，「網路病毒傳播與偵防機制策略研究」，資訊學會季刊，第 2 卷第 3 期，第 57 到 62 頁，1999 年。
7. 陳彥希，「效率、正義與契約」，日新警察半年刊，第 5 期，第 10 頁，內政

部警政署印製，2005年9月。

## 學位、研討會論文

1. 王麗芳，「洗錢暨防制洗錢相關法律責任之省思—兼論美國九一一事件後防治洗錢之新發展」，中國文化大學法律系，碩士論文，第94頁，2002年6月。
2. 江志慶，「ATM轉帳詐欺犯罪之實證研究」，中央警察大學犯罪防治系，碩士論文，第30頁，2005年。
3. 洪志忠，「我國網路犯罪案例及發展趨勢之探討」，2003年網際空間：科技、犯罪與法律社會學術研究暨實務研討會，第443頁，2003年。
4. 郭士傑，「詐欺及其類似犯罪區辨之研究」，東吳大學法律學系，專業碩士班碩士論文，第65頁，2003年。
5. 賴添貴，「台灣地區經濟詐欺狀況處理與防制之實證研究」，大業大學事業經營系，碩士論文，第54、127頁，2005年2月。
6. 謝開平，「電腦詐欺在比較刑法上之研究」，國立台北大學法律系，博士論文，第19頁，2003年7月。

## 研究報告

1. 內政部警政署刑事警察局委託研究報告（申請機構：中央警察大學，研究主持人：范國勇，共同主持人：張平君），ATM轉帳詐欺犯罪之實證研究，第42頁，2004年12月。
2. 台灣證券交易所股份有限公司委託研究報告，（研究人蓋華英、楊佳政、吳淑惠），如何消弭證券市場人頭戶氾濫問題，第2-1頁，1994年9月30日。
3. 吳天雲，「日本反洗錢制度與我國利法之比較」，九十年洗錢防制工作年報，第66頁以下，法務部調查局，2002年4月。
4. 李傑清，「我國洗錢防制法『確認身份』規定之研究—與日本『本人確認法』比較之觀點」，九十二年洗錢防制工作年報，第54頁以下，法務部調查局，2004年4月。
5. 陳茂益，「金融交易『人頭戶』洗錢犯罪問題探討與建議」，中華民國九十一年洗錢防制工作年報，第74頁，法務部調查局，2003年4月出版。
6. 謝宏滿，「警示帳戶」相關問題之處理機制，未公開發表之內部報告。
7. 鐘慧珍，「防制犯罪集團利用銀行存款帳戶進行詐騙之執行成果報告」，法務部調查局「經濟犯罪防制執行會議」第101次會議專題報告，第3頁，2004年12月29日。

## 報紙資料

1. 李禮仲，開戶拍照消滅人頭戶財政部淪為採證部，聯合報，民意論壇，2003年11月1日。
2. 卓榮泰，經濟日報，A4版金融新聞，2005年4月15日。
3. 易明秋，聯合報，A15版/民意論壇，2005年4月15日。
4. 陳一雄，聯合報，A5版話題，2005年4月13日。
5. 陳亮諭，「仿冒賣家帳號詐財 網拍陷阱」，聯合報，C4版，2006年3月22日。

6. 陳素玲、黃國樑，聯合晚報，1版要聞，2005年4月14日。
7. 陸倩瑤，聯合報，A3版焦點，2005年4月15日。
8. 楊文琪、邱金蘭，經濟日報，A4版金融新聞，2005年4月14日。
9. 楊惠鈞，”網路犯罪日益嚴重消費者如何自保？”，電子商務時報，2002年9月20日。
10. 聯合報，2005年4月16日。
11. 聯合報，A1版要聞，2005年4月15日。
12. 聯合報，社會版A8，2005年11月1日。
13. 蘇位榮，凍結警示帳戶法官認違法，聯合報，A9社會話題版，2006年3月8日。

## 網路資料

1. 2004年4月份新聞彙集，參 <http://gptaiwan.org.tw/~ayo/2Info/2004Apr.html>，(2005/12/4)
2. E騙術宣導，司法院政風處第一科，[http://w2.judicial.gov.tw/ged/workSystem/3\\_workshow.asp?work\\_id=46](http://w2.judicial.gov.tw/ged/workSystem/3_workshow.asp?work_id=46) (2006/3/1)。
3. Hinet新聞網，<http://times.hinet.net/SpecialTopic/940525-cheat/1425463.htm>，(2005/7/22)
4. <http://pages.tw.ebay.com/securitycenter/sv.html>，(2006/1/1)。
5. <http://tw.bid.yahoo.com/phtml/auc/tw/ezPay/home.html>，(2006/1/1)。
6. [http://tw.bid.yahoo.com/phtml/auc/tw/tos\\_add/protection.html](http://tw.bid.yahoo.com/phtml/auc/tw/tos_add/protection.html)，(2006/1/1)。
7. <http://www.neweb.com.tw/partners.htm>，(2006/1/1)。
8. <http://www.ettoday.com/2004/02/26/10846-1592272.htm> (2006/May/4)。
9. <http://www.ettoday.com/2004/02/26/10846-1592272.htm>，(2006/1/1)。
10. [http://www.paypal.com/cgi-bin/webscr?cmd=\\_pbp-info-outside](http://www.paypal.com/cgi-bin/webscr?cmd=_pbp-info-outside)，(2006/1/1)。
11. PC home on line 新聞，2005年7月22日，<http://news.pchome.com.tw/society/chinatimes/20040731/index-20040731023624240700.html> (2005/Oct/11)
12. 人頭戶之風險以及法律責任簡介，中華民國證券商業同業公會，<http://www.csa.org.tw/csa10/%E4%BA%BA%E9%A0%AD%E6%88%B6%E4%B9%8B%E9%A2%A8%E9%9A%AA%E4%BB%A5%E5%8F%8A%E6%B3%95%E5%BE%8B%E8%B2%AC%E4%BB%BB%E7%B0%A1%E4%BB%8B.doc>，(2006/3/4)。
13. 人頭帳戶犯罪，警署強力打擊，台中地檢署電子公佈欄，2003年7月4日，[http://www.tcc.moj.gov.tw/html/6/bulletin\\_detail.asp?news\\_id=131&kind\\_id=0](http://www.tcc.moj.gov.tw/html/6/bulletin_detail.asp?news_id=131&kind_id=0)，(2005/5/6)。
14. 小心網路騙局，公平會新聞稿，<http://www.ftc.gov.tw/news0918.htm>，(2006/3/1)。
15. 中華郵政網路郵局服務約定書，[http://download.post.gov.tw/post/intranet/DL\\_SERVER/P98044092.doc](http://download.post.gov.tw/post/intranet/DL_SERVER/P98044092.doc)，(2006/Mar/5)。
16. 內政部警政署網站，統計資料之警政統計年報，網址：[http://www.npa.gov.tw/stats.php?page=content06\\_1&id=70&tr\\_id=&pages=1](http://www.npa.gov.tw/stats.php?page=content06_1&id=70&tr_id=&pages=1)，(2006/3/4)。

17. 王文君、賴文智,線上遊戲防騙-線上遊戲常見詐騙手法與因應之道(一),  
<http://www.is-law.com/OurDocuments/GM0011WA.pdf>, (2006/3/1); 王文君、  
賴文智,“線上遊戲防騙-線上遊戲常見詐騙手法與因應之道(二),  
<http://www.is-law.com/OurDocuments/GM0012WA.pdf>, (2006/3/1)。
18. 台北市警察局犯罪預防宣導團,常見詐騙犯住類型及防制之道,  
[http://www.tcpd.gov.tw/all-tcpd.php?topage=1&id=243&t\\_type=d&tcpdlink=防制詐騙專區#網路交易詐騙](http://www.tcpd.gov.tw/all-tcpd.php?topage=1&id=243&t_type=d&tcpdlink=防制詐騙專區#網路交易詐騙) (2006/3/1)。
19. 民調大陸女口音十之八九詐騙, WEBS-TV 新聞,  
<http://news.web-tv.net/index.php>, (2006/Jan/5)。
20. 申辦貸款未查證,小心成為人頭戶,刑事警察局網站資料,  
[http://www.cib.gov.tw/crime/crime02\\_2.aspx?no=136](http://www.cib.gov.tw/crime/crime02_2.aspx?no=136), (2005/12/4)。
21. 存款不見人心慌慌,藍天電子報,第61期,2003年10月16日,  
<http://www.kmt.org.tw/epaper/Papers/921016/P4.html>, (2006/3/17)。
22. 行政院金融監督管理委員會銀行局之行政資訊目錄(9404),  
[http://www.fscey.gov.tw/lp\\_search.asp](http://www.fscey.gov.tw/lp_search.asp), (2006/Mar/5)。
23. 行政院監督管理委員網站,  
<http://www.fscey.gov.tw/ct.asp?xItem=28503&ctNode=17&mp=2>,  
(2006/Mar/5)
24. 消費者貸款審查要領及信用評等,  
<http://www.tabf.org.tw/tw/pub/preview/S0087.pdf>, (2006/3/17)。
25. 財政部對處理中興銀行案之說明,中央存款保險股份有限公司網址:  
<http://www.cdic.gov.tw/ct.asp?xItem=65&ctNode=192> (2006/May/1)。
26. 財團法人台灣資訊中心網站, TWNIC 2006年1月「台灣寬頻使用調查」摘要分析  
<http://www.twnic.net.tw/index4.php>, (2006/Feb/26)。
27. 張維平,我國網路犯罪現況分析,  
<http://www.ccpb.gov.tw/internet-fraud-01.htm>, (2006/3/4)
28. 張維平,我國網路犯罪現況分析,  
<http://www.ccpb.gov.tw/internet-fraud-01.htm>, (2005/7/22)。
29. 第三章存款存摺實務,  
<http://www.boaf.gov.tw/site/boaf/public/Attachment/52210233371.doc>,  
(2006/Mar/5)。
30. 莊哲維,刑事法規解釋之問題研究—兼論刑法秘密罪之解釋,  
<http://www.ntpu.edu.tw/law/paper/01/2001a/8971502a.PDF>, (2006/3/13)。
31. 郭尚義,防制電話詐欺與簡訊詐欺之治標與治本對策,ET today .com 東森  
新聞報,2005年4月20日,  
<http://www.ettoday.com/2005/04/20/320-1779631.htm>, (2006/3/3)。
32. 陳聰富,定型化契約的管制,台大校友雙月刊,  
<http://www.alum.ntu.edu.tw/read.php?num=25&sn=438>, (2006/5/26)。
33. 章光明,第11章台灣人權,莫讓網路成為天堂路,2005年台灣年鑑,  
[http://www.gov.tw/EBOOKS/TWANNUAL/show\\_book.php?path=3\\_011\\_001](http://www.gov.tw/EBOOKS/TWANNUAL/show_book.php?path=3_011_001),  
(2006/Mar/15)。
34. 郵政儲金匯兌法於2002年6月11日立法通過,見  
<http://lis.ly.gov.tw/npl/fast/02077/910611.htm>, (2006/3/10)。
35. 廉政電子報, <http://www.tcmvd.gov.tw/d9k/main/>, (2006/Feb/27)。

36. 電腦鑑識科學的現在與未來(一),台灣電腦網路危機處理暨協調中心網頁, <http://www.cert.org.tw/document/column/show.php?key=68> (2006/Feb/27)。
37. 廖德琦,法務部:勁永案 11/7 前水落石出,Taiwan New 新台灣雜誌,第 500 期,2005 年 10 月 20 日, <http://www.newtaiwan.com.tw/bulletinview.jsp?period=500&bulletinid=23029>,(2006/3/4)。
38. 網址:<http://www.ettoday.com/2004/02/26/10846-1592272.htm>,(2006/1/1)。
39. 網址:<http://tw.help.yahoo.com/auct/faq/ccd/index.html>,(2006/1/1)。
40. 網路安全新聞總覽,<http://www.acc.ncku.edu.tw/>(2005/5/7)
41. 銀行櫃檯 反詐騙最前線,自由電子報, <http://www.libertytimes.com.tw/2005/new/apr/22/today-so8.htm>,(2006/3/17)。
42. 劉克正,行政指導(一)、(二)、(三),內政部消防署消防影音新聞台, <http://enews.nfa.gov.tw/one-news.asp?NewsNo=5352>,(2006/Mar/5)。
43. 鄭琪芳,利用人頭戶逃漏稅財政部追查,自由新聞網, <http://www.libertytimes.com.tw/2004/new/sep/23/today-e4.htm>(2006/3/4)
44. 謝中凡,網路蒐購人頭戶轉賣 年轉千萬,中華日報,2004 年 12 月 22 日, <http://www.cdnnews.com.tw/20041223/news/shwx/733720002004122219204025.htm>,(2006/3/4)。
45. 藍新科技推出 ezPay 易付通保障網路交易安全,大紀元,2006 年 4 月 12 日, <http://www.epochtimes.com/b5/6/4/12/n1285340.htm>(2006/May/4)。
46. 驚悚回顧國內 2004 資安事件, <http://www.acc.ncku.edu.tw/>(2005/5/5)

## 其他

1. 1996 年 10 月 23 日總統(85)華總(一)義字第 08500251110 號令制定公布全文 15 條。
2. 2003 年 2 月 6 日總統(92)華總(一)義字第 09200019300 號令制定公布全文 15 條。
3. 2004 年 3 月 15 日台財融(一)字第 0938010347 號函。
4. 2006 年 4 月 27 日行政院監督管理委員會以金管銀(一)字第 09510001640 號令。
5. 台財融(一)字第 0931000318 號函及所附之「研商防制利用自動櫃員機詐財案件」會議紀錄。
6. 台財融字第 0931000331 號函及「研商遲延自動櫃員機轉帳入帳時間防制利用自動櫃員機轉帳功能進行詐騙事宜」會議紀錄。參見行政院金融監督管理委員會銀行局 94 年 4 月份大事紀要及行政資訊目錄。
7. 立法院議案關係文書,院總第 1692 號政府提案第 8848 號,案由:行政院函請審議「洗錢防制法修正草案」,2002 年 10 月 30 日印發。
8. 行政院回覆曾華德立法委員之書面質詢,見立法院公報,94 卷,第 40 期,第 97 頁。
9. 財政部 2001 年 4 月 3 日台財融(一)第 90733071 號函。
10. 財政部 2003 年 12 月 10 日台財融(二)字第 0922001638 號函釋。併依中華民國銀行商業同業公會全國聯合會研議之「國內金融機構受理存戶新開戶建立影像檔注意事項」辦理。
11. 財政部 2004 年 4 月 28 日台財融(一)字第 093100318 號函示。

## 外文資料

### 日文

#### 書籍

1. 佐藤英善，「經濟行政法」，第 943 頁，1990 年 6 月。

#### 期刊文章

1. 「いわゆる振り込め詐欺の被害者が振込先口座の預金者に対する不當利得返還請求権を被保全債権として同預金者の銀行に対する預金返還請求権を代位元行使することが認められた事例（東京地判 17. 3. 30）」，判例特報，1895 期，第 44 頁，2005 年 8 月 11 日。
2. 「ロー・フォーラム—立法の話題—『振り込め詐欺』の防止に向けて—攜帶電話本人確認・不正利用防止法の成立」，法學セミナー，第 606 期，第 127 頁，2005 年 6 月。
3. 伊藤涉，「振り込め詐欺」，法學教室月刊，296 期，第 13 頁，2005 年 5 月 1 日。

#### 網路資料

1. 日本金融廳網站：[www.fsa.go.jp/policy/honninkakunin/00.pdf](http://www.fsa.go.jp/policy/honninkakunin/00.pdf)。
2. 日本警視廳之網站：[http://www.npa.go.jp/safetylife/seianki31/1\\_hurikome.htm](http://www.npa.go.jp/safetylife/seianki31/1_hurikome.htm)，(2006/May/1)。

## 英文

#### 書籍

1. Clarke, R.V and R.Home(1997).A Revised Classification of Situational Crime Prevention Techiques. In S.P.Lab (ed): Crime Prevention at a Crossroads. Anderson.

#### 期刊文章

1. Becker, Gary,” Crime and punishment: An economic approach” , Journal of Political Economy 76 , page169 , 1968 。
2. Ehrlich,Isaac,”Participation in Illegitimate Activity : A Theoretical and Empirical Investigation” , Journal of Political Economy, Vol. 81, No. 3 (May - Jun., 1973), page 521-565 。
3. Posner,Richard A,Economic Analsis od law(5th ed,1998) ; The New Palgrave Dictinonary of Economics and the Law (1998).

#### 網路資料

1. “IC3 2005 Internet Fraud –Crime report ” ,  
[http://www.ic3.gov/media/annualreport/2005\\_ic3report.pdf](http://www.ic3.gov/media/annualreport/2005_ic3report.pdf), ( 2006/May/1 ) ◦
2. “Internet Scams Fraud Trends January-December  
2005”,[http://www.fraud.org/2005\\_Internet\\_Fraud\\_Report.pdf](http://www.fraud.org/2005_Internet_Fraud_Report.pdf) , ( 2006/Feb/26 ) ◦
3. Consumer Fraud and Indentity Theft Complaint Data January-December 2005 ,  
page3 , <http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf>  
( 2006/Feb/26 ) ◦
4. <https://www.escrow.com> ◦
5. Mann-Whitney U Test:<http://eatworms.swmed.edu/~leon/stats/utest.cgi> ◦
6. The term "Internet fraud" refers generally to any type of fraud scheme that uses  
one or more components of the Internet - such as chat rooms, e-mail, message  
boards, or Web sites - to present fraudulent solicitations to prospective victims,  
to conduct fraudulent transactions, or to transmit the proceeds of fraud to  
financial institutions or to other connected with the scheme ,  
<http://www.internetfraud.usdoj.gov/#What%20Is%20Internet%20Fraud> ,  
( 2006/Feb/26 ) ◦



# 附 錄 一

## 銀行對疑似不法或顯屬異常交易之存款帳戶

### 管理辦法總說明

隨社會經濟迅速發展及科技日益昌明，高科技資訊產品如手機、網路及自動櫃員機（ATM）等工具，誠然為國人生活提供諸多便利，惟亦為不法之徒予以扭曲濫用，犯罪集團憑藉其綿密之組織結構、精細之技巧訓練及科技化資訊產品，假藉各種名義並運用人性弱點，肆行詐財等不法勾當，除侵害民眾財產，已衍生為社會問題。此外，自 90 年美國 911 事件後，國際間為防制洗錢及打擊資助恐怖主義，對疑似不法或顯屬異常交易之帳戶均投以特別關注，我國身為國際社會一員，亦不能自外於此。

為維護金融體系運作之完整及消費者權益，銀行法第四十八條第一項明訂「銀行非依法院之裁判或其他法律之規定，不得接受第三人有關停止給付存款或匯款、扣留擔保物或保管物或其他類似之請求」，惟對於歹徒利用各式便捷之金融管道進行不法利得移轉以遂行其不法目的之行為，尚無一立即有效之防制規範。

鑑於前述之不法犯罪行為，已嚴重斷傷金融秩序及民眾信心，為遏止不法行為並期身處第一道防線之金融機構，得以貫徹政府打擊犯罪及國際間反洗錢與反恐政策，特於銀行法第四十五條之二增訂第二項「銀行對存款帳戶應負善良管理人責任。對疑似不法或顯屬異常交易之存款帳戶，得予暫停存入或提領、匯出款項。」及第三項「前項疑似不法或顯屬異常交易帳戶之認定標準，及暫停帳戶之作業程序及辦法，由主管機關定之。」本項修正案係於 94 年 5 月 18 日總統令公布施行。

依據前開法律授權，行政院金融監督管理委員會特訂定「銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法」（以下稱本辦法），並於 94 年 11 月 9 日、94 年 12 月 7 日及 95 年 1 月 10 日邀集司法院、法務部、內政部、中央銀行、中華民國銀行商業同業公會全國聯合會、中華民國信用合作社聯合社、金融聯合徵信中心、財金資訊股份有限公司、及金融業者等相關單位舉行 3 次公聽會，聽取各界意見，取得共識。本辦法共計 20 條，主要規範重點如下：

- 一、法令授權依據（第一條）。
- 二、存款帳戶之範圍。（第二條）
- 三、本辦法用詞之定義。（第三條）
- 四、疑似不法或顯屬異常交易存款帳戶之認定標準及分類（第四條）。
- 五、銀行對疑似不法或顯屬異常交易帳戶之處理措施（第五至七條）。
- 六、扣押命令及警示帳戶之優先適用順序（第八條）。
- 七、相關帳戶限制措施之解除標準（第九、十條）。
- 八、警示帳戶內剩餘款項之處理機制（第十一條）。
- 九、銀行應建立明確之「認識客戶」原則（第十二條）。
- 十、銀行應拒絕存款開戶申請之情形（第十三條）。
- 十一、銀行應以資訊系統整合其全行存款客戶之基本資料及交易資料（第十四條）。
- 十二、對於具較高風險之存款客戶，銀行除為一般性之客戶審查措施外，

應有適當之風險管理措施（第十五條）。

十三、銀行應以資訊系統輔助清查存款帳戶之異常交易，對於交易額超過一定門檻等狀況，應設立預警指標，每日至少查核追蹤乙次（第十六條）。

十四、銀行之國外分行及子銀行之適用標準（第十七條）。

十五、銀行應依本辦法訂定其內部作業準則（第十八條）。

十六、銀行應將其訂定準則之相關規範納入內部控制及內部稽核項目（第十九條）。



## 銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法

條文	說明
<p>第一條 本辦法依銀行法第四十五條之二第三項規定訂定之。</p>	<p>依據銀行法第四十五條之二第三項授權規定，訂定本辦法。</p>
<p>第二條 本辦法所稱存款帳戶，指銀行法第六條至第八條所稱之支票存款、活期存款及定期存款帳戶。</p>	<p>明定存款帳戶之範圍，包括支票存款、活期存款及定期存款帳戶。</p>
<p>第三條 本辦法用詞定義如下：</p> <p>一、警示帳戶：指法院、檢察署或司法警察機關為偵辦刑事案件需要，通報銀行將存款帳戶列為警示者。</p> <p>二、衍生管制帳戶：指警示帳戶之開戶人所開立之其他存款帳戶。</p> <p>三、通報：指法院、檢察署或司法警察機關以公文書通知銀行將存款帳戶列為警示或解除警示，惟如屬重大緊急案件，得以電話、傳真或其他可行方式先行通知，並應即補辦公文書資料。</p>	<p>訂定本辦法之用詞定義：</p> <p>一、警示帳戶機制係為配合警調機關查緝電話詐欺恐嚇案件需要，暨維護民眾權益，於 91 年 10 月建立之通報、支付方式變更及協助還款機制，明訂於本辦法以提升其法律位階；另為強化該機制功能，將其適用範圍擴大至偵辦刑事案件需要。</p> <p>二、衍生管制帳戶係參酌銀行公會 94 年 8 月「一人持有多个金融機構存款帳戶，其中一帳戶經通報為警示帳戶，其餘帳戶之通報及控管作業程序」訂定之。</p>
<p>第四條 本辦法所稱疑似不法或顯屬異常交易存款帳戶之認定標準及分類如下：</p> <p>一、第一類：</p> <p>（一）法院、檢察署因偵辦刑事案件需要，依法扣押或禁止處分之存款帳戶。</p> <p>（二）存款帳戶屬偽冒開戶者。</p> <p>二、第二類：</p> <p>（一）屬警示帳戶者。</p> <p>（二）屬衍生管制帳戶者。</p> <p>三、第三類：</p> <p>（一）短期間內頻繁申請開立存款帳戶，且無法提出合理說明者。</p> <p>（二）客戶申請之交易功能與其年齡或背景顯不相當者。</p> <p>（三）客戶提供之聯絡資料均無法以合理之方式查證者。</p> <p>（四）存款帳戶經金融機構或民眾通知，疑為犯罪行為人使用者。</p>	<p>一、本條之認定標準係參考銀行公會意見、銀行防制洗錢注意事項範本及彙整相關行政函令後訂定。</p> <p>二、認定標準依不法行為之嚴重程度概分為三類，第一類包括依法扣押、禁止處分之存款帳戶及偽冒開戶者；第二類包括警示帳戶及衍生管制帳戶；第三類包括其他疑似不法或顯屬異常交易之情事者。</p>

條文	說明
<p>(五) 存款帳戶內常有多筆小額轉出入交易，近似測試行為者。</p> <p>(六) 短期間內密集使用銀行之電子服務或設備，與客戶日常交易習慣明顯不符者。</p> <p>(七) 靜止戶恢復往來，且交易有異常情況者。</p> <p>(八) 符合銀行防制洗錢注意事項範本所列疑似洗錢表徵之交易者。</p> <p>(九) 其他經主管機關或銀行認定為疑似不法或顯屬異常交易之存款帳戶。</p>	
<p><b>第五條</b> 存款帳戶依前條之分類標準認定為疑似不法或顯屬異常交易者，銀行應採取下列處理措施：</p> <p>一、第一類：</p> <p>(一) 存款帳戶依法扣押或禁止處分者，應即依相關法令規定辦理。</p> <p>(二) 存款帳戶如屬偽冒開戶者，應即通知司法警察機關、法務部調查局洗錢防制中心及金融聯合徵信中心，銀行並應即結清該帳戶，其剩餘款項則俟依法可領取者申請給付時處理。</p> <p>(三) 依其他法令規定之處理措施。</p> <p>二、第二類：</p> <p>(一) 存款帳戶經通報為警示帳戶者，應即通知金融聯合徵信中心，並暫停該帳戶全部交易功能，匯入款項逕以退匯方式退回匯款行。</p> <p>(二) 存款帳戶屬衍生管制帳戶者，應即暫停該帳戶使用提款卡、語音轉帳、網路轉帳及其他電子支付功能，匯入款項逕以退匯方式退回匯款行。</p> <p>(三) 依其他法令規定之處理措施。</p> <p>三、第三類：</p> <p>(一) 對該等帳戶進行查證及持續進行監控，如經查證有不法情事者，除通知司法警察機關外，並得採行前二款之部分或全部措施。</p>	<p>一、處理措施依第四條之分類標準亦概分為三類，第一類包括依法扣押、禁止處分之帳戶及偽冒開戶之處置措施；第二類包括警示帳戶及衍生管制帳戶之處置措施；第三類包括其他疑似不法或顯屬異常交易情事者之處置措施。</p> <p>二、考量警示帳戶已明定警示期限及救濟途徑，為免帳戶開戶人臨櫃交易及委託代扣繳等實務執行上迭生爭議，爰將警示帳戶之限制措施擴大為「暫停該帳戶全部交易功能」。</p> <p>三、衍生管制帳戶因尚無明顯犯罪之事實及依據，限制措施限於「暫停該帳戶使用提款卡、語音轉帳、網路轉帳及其他電子支付等功能」恐用以快速移轉不法資金之管道，臨櫃交易及委託扣繳稅費等功能則不受限制。</p>

條文	說明
(二) 依洗錢防制法等相關法令規定之處理措施。	
<p>第六條 銀行除依前條所列措施辦理外，並應於內部採取下列措施：</p> <p>一、循內部程序通報所屬總行或總管理機構之專責單位。</p> <p>二、將已採行及擬採行之處理措施一併陳報總行或總管理機構之專責單位。</p> <p>三、於銀行內部資訊系統中加以註記，提醒各分支機構加強防範。</p>	<p>明訂銀行除依第五條所列措施辦理外，並應於其內部採取之措施。</p>
<p>第七條 存款帳戶經法院、檢察署或司法警察機關通報為警示帳戶者，銀行應即查詢帳戶相關交易，如發現通報之詐騙款項已轉出至其他帳戶，應將該筆款項轉出之資料及原通報機關名稱，通知該筆款項之受款行，並通知原通報機關。</p> <p>警示帳戶之原通報機關依前項資料進行查證後，如認為該等受款帳戶亦須列為警示帳戶者，由該原通報機關再進一步通報相關銀行列為警示。</p> <p>詐騙款項之相關受款行，應依第一項規定辦理交易查詢及通知作業，如查證受款帳戶有犯罪事實者，應即採行第五條第三款所列處理措施。</p> <p>本條之通知方式、通知範圍及所需文件等作業程序，由中華民國銀行商業同業公會全國聯合會訂定，並報主管機關備查。</p>	<p>為有效阻斷犯罪集團之資金流向，以降低民眾損失，特依據 93 年 11 月 22 日「反詐騙聯防平臺」第 1 次會議決議事項建立聯防機制。</p>
<p>第八條 存款帳戶之款項若已遭扣押或禁止處分，復接獲法院、檢察署或司法警察機關通報為警示帳戶，該帳戶仍應列為警示帳戶，但該等款項優先依扣押或禁止處分命令規定辦理。</p>	<p>明訂扣押命令及警示帳戶之優先適用順序。</p>
<p>第九條 警示帳戶之警示期限自每次通報時起算，逾 5 年自動失其效力，但有繼續警示之必要者，原通報機關應於期限屆滿前再行通報之。</p> <p>警示帳戶之開戶人對其存款帳戶被列為警示如有疑義，由開戶人洽原通報機關處理，銀行於必要時並應提供協助。</p>	<p>為保障消費者權益，特訂定警示帳戶之警示期限不得逾 5 年，且開戶人如有疑義，原通報機關應負責處理，銀行於必要時並應提供協助。</p>

條文	說明
<p>第十條 依法扣押或禁止處分之存款帳戶及警示帳戶，嗣後應依原扣押或通報機關之通報，或警示期限屆滿，銀行方得解除該等帳戶之限制。</p> <p>屬衍生管制帳戶及依第四條第三款所列標準認定為疑似不法或顯屬異常交易之存款帳戶者，經銀行查證該等疑似不法或顯屬異常情形消滅時，應即解除相關限制措施。</p> <p>警示帳戶依原通報機關之通報解除，或原通報機關依前條第一項再行通報銀行繼續警示者，銀行應即通知金融聯合徵信中心。</p>	<p>訂定疑似不法或顯屬異常交易存款帳戶之解除標準：</p> <p>一、依法扣押或禁止處分之存款帳戶及警示帳戶，嗣後應依原查扣或通報單位之通報，或警示期限屆滿，銀行方得解除該等帳戶之限制。</p> <p>二、其餘則於該等疑似不法或顯屬異常情形消滅時，辦理限制措施之解除。</p>
<p>第十一條 存款帳戶經通報為警示帳戶，銀行經確認通報原因屬詐財案件，且該帳戶中尚有被害人匯（轉）入之款項未被提領者，應依開戶資料聯絡開戶人，與其協商發還警示帳戶內剩餘款項事宜。</p> <p>銀行依前項辦理，仍無法聯絡開戶人者，應透過匯（轉）出行通知被害人，由被害人檢具下列文件，經銀行依匯（轉）入時間順序逐筆認定其尚未被提領部分，由最後一筆金額往前推算至帳戶餘額為零止，發還警示帳戶內剩餘款項：</p> <p>一、刑事案件報案三聯單。</p> <p>二、申請不實致銀行受有損失，由該被害人負一切法律責任之切結書。</p> <p>銀行依本條規定辦理警示帳戶剩餘款項之發還，如有下列情事之一者，得逕行結清該帳戶，並將剩餘款項轉列其他應付款，俟依法可領取者申請給付時處理；但銀行須經通報解除警示或警示期限屆滿後，方得解除對該帳戶開戶人之警示效力。</p> <p>一、剩餘款項在一定金額以下，不符作業成本者。</p> <p>二、自警示通報時起超過 6 個月，仍無法</p>	<p>一、訂定警示帳戶內剩餘款項之處理機制。</p> <p>二、參酌 94 年 2 月 4 日「研商金融機構發還滯留於警示帳戶內剩餘款項之處理機制」會議結論事項、銀行公會之「金融機構返還滯留於警示帳戶內剩餘款項作業程序」、及本會銀行局 94 年 5 月 16 日銀局（一）字第 0941000352 號函有關警示帳戶餘額在新台幣 1,000 元以下之處理方式訂定。</p>

條文	說明
<p>聯絡開戶人或被害人者。</p> <p>三、被害人不願報案或不願出面領取款項者。</p> <p>銀行應指定一位副總經理或相當層級之主管專責督導警示帳戶內剩餘款項之處理事宜。</p> <p>疑似交易糾紛或案情複雜等案件，不適用本條所定剩餘款項發還之規定，應循司法程序辦理。</p>	
<p>第十二條 銀行應建立明確之認識客戶政策及作業程序，包括接受客戶開立存款帳戶之標準、對客戶之辨識、存款帳戶及交易之監控及必要教育訓練等重要事項。</p> <p>前項有關接受客戶開立存款帳戶之作業審核程序，由中華民國銀行商業同業公會全國聯合會訂定範本，並報主管機關備查。</p>	<p>參酌2004年10月巴塞爾銀行監理委員會發布之「整合客戶風險管理」 「Consolidated KYC Risk Management」相關規範訂定。</p>
<p>第十三條 銀行受理客戶開立存款帳戶，應實施雙重身分證明文件查核，身分證及登記證照以外之第二身分證明文件，應具辨識力。</p> <p>銀行應確認客戶身分，始得受理客戶開立存款帳戶，如有下列情形，應拒絕客戶之開戶申請：</p> <p>一、疑似使用假名、人頭、虛設行號或虛設法人團體開立存款帳戶者。</p> <p>二、持用偽、變造身分證明文件或出示之身分證明文件均為影本者。</p> <p>三、提供之文件資料可疑、模糊不清、不願提供其他佐證資料、或提供之文件資料無法進行查證者。</p> <p>四、客戶不尋常拖延應提供之身分證明文件者。</p> <p>五、客戶開立之其他存款帳戶經通報為警示帳戶尚未解除者，但為就業需要開立薪資轉帳戶，並經銀行查證屬實者，不在此限，且不列為衍生管制帳戶。</p> <p>六、受理開戶時有其他異常情形，且客戶無法提</p>	<p>一、為期自源頭阻斷不法帳戶之開立，參酌銀行公會訂定之「銀行防制洗錢注意事項範本」規範，及本會93年8月4日金管銀(一)字第0938011385號函等規定，明訂開戶應實施雙重身分證明文件查核，及銀行得拒絕客戶開立存款帳戶之情形，以收先行防杜之效。</p> <p>二、為保障客戶之工作權，特於本條第二項第五款訂定但書，並於第十五條訂定配套管理措施。</p>

條文	說明
出合理說明者。	
<p>第十四條 銀行應以資訊系統整合其全行存款客戶之基本資料及交易資料，供其總分支機構查詢，對於各單位調取及查詢客戶之資料，應建立內部控制程序，並注意資料之保密性。</p>	<p>為加強對客戶之辨識，以有效控管全行之作業風險及聲譽風險，明訂銀行應整合其存款客戶基本資料及交易資料，供其總分支機構查詢。</p>
<p>第十五條 由專業中介機構代為處理之交易、曾經通報為警示帳戶而已解除者、依第十三條第二項第五款但書申請開戶者、或其他經研判具高風險之存款客戶或交易，銀行除為一般性之客戶審查措施外，另應有適當之風險管理措施，包括：</p> <p>一、帳戶之開立應經較高層級主管之核准。</p> <p>二、確認其財產及資金來源、去處之合理性。</p> <p>三、對其存款交易實施持續監控。</p>	<p>一、對於由專業中介機構代為處理之交易、曾經通報為警示帳戶而已解除者、依第十三條第二項第五款但書開戶者、及其他經研判具高風險之存款客戶或交易，訂定配套管理措施。</p> <p>二、參酌「打擊清洗黑錢財務行動特別組織」(FATF)發布之「40項建議及9項特別建議評鑑方法論」(Methodology for Assessing Compliance with the FATF 40 Recommendations and 9 Special Recommendations)第6項建議，及巴塞爾銀行監理委員會2001年10月發布之「銀行客戶審查準則」(Customer Due Diligence for banks; CDD)相關規範訂定。</p> <p>三、依據FATF發布之「40項建議及9項特別建議評鑑方法論」，專業中介機構包括金融機構、律師、公證人及會計師等專業第三人。</p>
<p>第十六條 銀行應建立以資訊系統輔助清查存款帳戶異常交易之機制，對於交易金額超過一定門檻、交易金額與帳戶平均餘額顯不相當、或短期間內密集使用電子交易功能等狀況，應設立預警指標，每日由專人至少查核及追蹤乙次並作成紀錄，依內部程序送交權責主管核閱。</p> <p>前項所稱紀錄及其相關資訊，至少應保存5年，並得提供主管機關、有關單位及內部稽核單位調閱。</p>	<p>一、銀行業務繁重且通路廣泛，難以僅賴櫃員判斷疑似不法或顯屬異常交易之存款帳戶，爰規範銀行應以資訊系統進行輔助偵測及監控，對於交易額超過一定門檻、交易額與帳戶平均餘額顯不相當、或短期間內密集使用電子交易功能等三類較具體之狀況，尤應設立預警指標，每日至少追蹤乙次，俾及時發現異常帳戶。</p> <p>二、參酌亞太洗錢防制組織「評鑑遵循反洗錢與打擊資助恐怖主義標準方法</p>

條文	說明
	論」(Methodology for Assessing Compliance with Anti-Money Laundering and Combating the Financing of Terrorism Standards)中有關持續性監控帳戶與交易(On-going monitoring of accounts and transactions)及紀錄保存(Record keeping)相關規範訂定。
第十七條 銀行之國外分行及子銀行在其所在國法令許可範圍內，應遵守本辦法之規定，但所在國之法令與本辦法牴觸時，銀行應將相關事實陳報主管機關備查。	參酌「打擊清洗黑錢財務行動特別組織」(FATF)發佈之「40項建議及9項特別建議評鑑方法論」第22項建議中有關銀行國外分行及子銀行之必要準則訂定。
第十八條 銀行應依本辦法訂定其內部作業準則，其內容應至少包括疑似不法或顯屬異常交易帳戶之認定標準及應採取之措施、第六條第一款所稱專責單位之指定、第十一條第三項第一款所稱一定金額、第十六條第一項所稱預警指標之建立、紛爭處理、員工教育訓練及稽核功能等。	銀行應考量自身規模、組織架構、風險承擔能力及資訊系統之複雜性後，將其對疑似不法或顯屬異常交易存款帳戶之認定標準、應採取之措施、專責單位、警示帳戶逕予結清之金額門檻、預警指標、紛爭處理、員工教育訓練及稽核功能等，訂定於其內部準則俾供依循。
第十九條 銀行應將前條所稱內部作業準則之規範納入內部控制及內部稽核項目，並依據銀行內部控制及稽核制度實施辦法之規定，辦理內部稽核及自行查核。	為落實本辦法所列規定，銀行應依相關規範辦理內部稽核及自行查核作業。
第二十條 本辦法除第十四條、第十六條、第十八條及第十九條自九十六年一月一日施行外，自發布日施行。	本辦法第十四、十六、十八及第十九條因涉銀行資訊系統及作業準則之建置，應予緩衝期因應外，餘自發布日施行。

## 銀行對疑似不法或顯屬異常交易之存款帳戶管理辦法

- 第一條 本辦法依銀行法第四十五條之二第三項規定訂定之。
- 第二條 本辦法所稱存款帳戶，指銀行法第六條至第八條所稱之支票存款、活期存款及定期存款帳戶。
- 第三條 本辦法用詞定義如下：
- 一、警示帳戶：指法院、檢察署或司法警察機關為偵辦刑事案件需要，通報銀行將存款帳戶列為警示者。
  - 二、衍生管制帳戶：指警示帳戶之開戶人所開立之其他存款帳戶。
  - 三、通報：指法院、檢察署或司法警察機關以公文書通知銀行將存款帳戶列為警示或解除警示，惟如屬重大緊急案件，得以電話、傳真或其他可行方式先行通知，並應即補辦公文書資料。
- 第四條 本辦法所稱疑似不法或顯屬異常交易存款帳戶之認定標準及分類如下：
- 一、第一類：
    - (一) 法院、檢察署因偵辦刑事案件需要，依法扣押或禁止處分之存款帳戶。
    - (二) 存款帳戶屬偽冒開戶者。
  - 二、第二類：
    - (一) 屬警示帳戶者。
    - (二) 屬衍生管制帳戶者。
  - 三、第三類：
    - (一) 短期間內頻繁申請開立存款帳戶，且無法提出合理說明者。
    - (二) 客戶申請之交易功能與其年齡或背景顯不相當者。
    - (三) 客戶提供之聯絡資料均無法以合理之方式查證者。
    - (四) 存款帳戶經金融機構或民眾通知，疑為犯罪行為人使用者。
    - (五) 存款帳戶內常有多筆小額轉出入交易，近似測試行為者。
    - (六) 短期間內密集使用銀行之電子服務或設備，與客戶日常交易習慣明顯不符者。
    - (七) 靜止戶恢復往來，且交易有異常情況者。
    - (八) 符合銀行防制洗錢注意事項範本所列疑似洗錢表徵之交易者。
    - (九) 其他經主管機關或銀行認定為疑似不法或顯屬異常交易之存款帳戶。
- 第五條 存款帳戶依前條之分類標準認定為疑似不法或顯屬異常交易者，銀行應採取下列處理措施：
- 一、第一類：
    - (一) 存款帳戶依法扣押或禁止處分者，應即依相關法令規定辦理。
    - (二) 存款帳戶如屬偽冒開戶者，應即通知司法警察機關、法務部調查局洗錢防制中心及金融聯合徵信中心，銀行並應即結清該

帳戶，其剩餘款項則俟依法可領取者申請給付時處理。

(三) 依其他法令規定之處理措施。

## 二、第二類：

(一) 存款帳戶經通報為警示帳戶者，應即通知金融聯合徵信中心，並暫停該帳戶全部交易功能，匯入款項逕以退匯方式退回匯款行。

(二) 存款帳戶屬衍生管制帳戶者，應即暫停該帳戶使用提款卡、語音轉帳、網路轉帳及其他電子支付功能，匯入款項逕以退匯方式退回匯款行。

(三) 依其他法令規定之處理措施。

## 三、第三類：

(一) 對該等帳戶進行查證及持續進行監控，如經查證有不法情事者，除通知司法警察機關外，並得採行前二款之部分或全部措施。

(二) 依洗錢防制法等相關法令規定之處理措施。

第六條 銀行除依前條所列措施辦理外，並應於內部採取下列措施：

一、循內部程序通報所屬總行或總管理機構之專責單位。

二、將已採行及擬採行之處理措施一併陳報總行或總管理機構之專責單位。

三、於銀行內部資訊系統中加以註記，提醒各分支機構加強防範。

第七條 存款帳戶經法院、檢察署或司法警察機關通報為警示帳戶者，銀行應即查詢帳戶相關交易，如發現通報之詐騙款項已轉出至其他帳戶，應將該筆款項轉出之資料及原通報機關名稱，通知該筆款項之受款行，並通知原通報機關。

警示帳戶之原通報機關依前項資料進行查證後，如認為該等受款帳戶亦須列為警示帳戶者，由該原通報機關再進一步通報相關銀行列為警示。

詐騙款項之相關受款行，應依第一項規定辦理交易查詢及通知作業，如查證受款帳戶有犯罪事實者，應即採行第五條第三款所列處理措施。

本條之通知方式、通知範圍及所需文件等作業程序，由中華民國銀行商業同業公會全國聯合會訂定，並報主管機關備查。

第八條 存款帳戶之款項若已遭扣押或禁止處分，復接獲法院、檢察署或司法警察機關通報為警示帳戶，該帳戶仍應列為警示帳戶，但該等款項優先依扣押或禁止處分命令規定辦理。

第九條 警示帳戶之警示期限自每次通報時起算，逾5年自動失其效力，但有繼續警示之必要者，原通報機關應於期限屆滿前再行通報之。

警示帳戶之開戶人對其存款帳戶被列為警示如有疑義，由開戶人洽原通報機關處理，銀行於必要時並應提供協助。

第十條 依法扣押或禁止處分之存款帳戶及警示帳戶，嗣後應依原扣押或通報機關之通報，或警示期限屆滿，銀行方得解除該等帳戶之限制。

屬衍生管制帳戶及依第四條第三款所列標準認定為疑似不法或顯屬異常交易之存款帳戶者，經銀行查證該等疑似不法或顯屬異常情形消滅時，應即解除相關限制措施。

警示帳戶依原通報機關之通報解除，或原通報機關依前條第一項再行通報銀行繼續警示者，銀行應即通知金融聯合徵信中心。

第十一條 存款帳戶經通報為警示帳戶，銀行經確認通報原因屬詐財案件，且該帳戶中尚有被害人匯（轉）入之款項未被提領者，應依開戶資料聯絡開戶人，與其協商發還警示帳戶內剩餘款項事宜。

銀行依前項辦理，仍無法聯絡開戶人者，應透過匯（轉）出行通知被害人，由被害人檢具下列文件，經銀行依匯（轉）入時間順序逐筆認定其尚未被提領部分，由最後一筆金額往前推算至帳戶餘額為零止，發還警示帳戶內剩餘款項：

- 一、刑事案件報案三聯單。
- 二、申請不實致銀行受有損失，由該被害人負一切法律責任之切結書。

銀行依本條規定辦理警示帳戶剩餘款項之發還，如有下列情事之一者，得逕行結清該帳戶，並將剩餘款項轉列其他應付款，俟依法可領取者申請給付時處理；但銀行須經通報解除警示或警示期限屆滿後，方得解除對該帳戶開戶人之警示效力。

- 一、剩餘款項在一定金額以下，不符作業成本者。
- 二、自警示通報時起超過6個月，仍無法聯絡開戶人或被害人者。
- 三、被害人不願報案或不願出面領取款項者。

銀行應指定一位副總經理或相當層級之主管專責督導警示帳戶內剩餘款項之處理事宜。

疑似交易糾紛或案情複雜等案件，不適用本條所定剩餘款項發還之規定，應循司法程序辦理。

第十二條 銀行應建立明確之認識客戶政策及作業程序，包括接受客戶開立存款帳戶之標準、對客戶之辨識、存款帳戶及交易之監控及必要教育訓練等重要事項。

前項有關接受客戶開立存款帳戶之作業審核程序，由中華民國銀行商業同業公會全國聯合會訂定範本，並報主管機關備查。

第十三條 銀行受理客戶開立存款帳戶，應實施雙重身分證明文件查核，身分證及登記證照以外之第二身分證明文件，應具辨識力。

銀行應確認客戶身分，始得受理客戶開立存款帳戶，如有下列情形，應拒絕客戶之開戶申請：

- 一、疑似使用假名、人頭、虛設行號或虛設法人團體開立存款帳戶者。
- 二、持用偽、變造身分證明文件或出示之身分證明文件均為影本者。
- 三、提供之文件資料可疑、模糊不清、不願提供其他佐證資料、或提供之文件資料無法進行查證者。
- 四、客戶不尋常拖延應提供之身分證明文件者。
- 五、客戶開立之其他存款帳戶經通報為警示帳戶尚未解除者，但為就業需要開立薪資轉帳戶，並經銀行查證屬實者，不在此限，且不列為衍生管制帳戶。
- 六、受理開戶時有其他異常情形，且客戶無法提出合理說明者。

第十四條 銀行應以資訊系統整合其全行存款客戶之基本資料及交易資料，供其總分支機構查詢，對於各單位調取及查詢客戶之資料，應建立內

部控制程序，並注意資料之保密性。

- 第十五條 由專業中介機構代為處理之交易、曾經通報為警示帳戶而已解除者、依第十三條第二項第五款但書申請開戶者、或其他經研判具高風險之存款客戶或交易，銀行除為一般性之客戶審查措施外，另應有適當之風險管理措施，包括：
- 一、帳戶之開立應經較高層級主管之核准。
  - 二、確認其財產及資金來源、去處之合理性。
  - 三、對其存款交易實施持續監控。
- 第十六條 銀行應建立以資訊系統輔助清查存款帳戶異常交易之機制，對於交易金額超過一定門檻、交易金額與帳戶平均餘額顯不相當、或短期間內密集使用電子交易功能等狀況，應設立預警指標，每日由專人至少查核及追蹤乙次並作成紀錄，依內部程序送交權責主管核閱。前項所稱紀錄及其相關資訊，至少應保存 5 年，並得提供主管機關、有關單位及內部稽核單位調閱。
- 第十七條 銀行之國外分行及子銀行在其所在國法令許可範圍內，應遵守本辦法之規定，但所在國之法令與本辦法抵觸時，銀行應將相關事實陳報主管機關備查。
- 第十八條 銀行應依本辦法訂定其內部作業準則，其內容應至少包括疑似不法或顯屬異常交易帳戶之認定標準及應採取之措施、第六條第一款所稱專責單位之指定、第十一條第三項第一款所稱一定金額、第十六條第一項所稱預警指標之建立、紛爭處理、員工教育訓練及稽核功能等。
- 第十九條 銀行應將前條所稱內部作業準則之規範納入內部控制及內部稽核項目，並依據銀行內部控制及稽核制度實施辦法之規定，辦理內部稽核及自行查核。
- 第二十條 本辦法除第十四條、第十六條、第十八條及第十九條自九十六年一月一日施行外，自發布日施行。

## 附 錄 二

### 金融電信人頭帳戶及電話犯罪案件處理執行規定

#### 壹、依據

92年7月7日行政院強化社會治安第19次專案會議 院長裁示事項辦理。

#### 貳、目的

律定利用金融電信人頭帳戶及電話犯罪案件處理流程，統一偵查權責、建檔管制人頭資料庫，以有效遏制利用金融電信科技犯罪，確保民眾財產安全。

#### 參、作法

本署刑事警察局偵七隊暨各市、縣（市）警察局刑警（大）隊於92年7月4日起成立「人頭帳戶、電話犯罪案件專責處理、偵辦窗口」（簡稱專責組），各警察分局亦自93年1月5日起成立專責窗口，並分別於92年7月16日及93年1月1日正式啟用「人頭資料庫」第一、二階段功能，提供各警察機關、民眾查詢及整合各種詐騙人頭資訊，以有效斷絕詐騙集團所使用之犯罪及吸金工具。

#### 肆、金融電信人頭帳戶及電話犯罪案件態樣及範圍

##### 一、犯罪態樣：

- （一）詐欺案件：電話恐嚇、刮刮樂、退稅或退費、防疫補助款、手機簡訊及家庭代工、仲介、貸款、...網路詐欺等。
- （二）恐嚇取財案件：竊車恐嚇取財、網鴿恐嚇取財等。

二、案件範圍：有被害人報案或民眾檢舉告發，且涉有利用金融帳戶、電信電話犯前項詐欺、恐嚇取財案件，查證屬實後屬本執行規定案件處理範圍。

#### 伍、責任區分

##### 一、詐欺案件：（涉及帳戶匯款案件）

以人頭帳戶（涉及多個帳戶者，以第一次匯入帳戶）開戶金融機構所在地之警察機關主辦，其他警察機關協同辦理。如受款地在境外，則由第一次匯款地之警察機關主辦。

##### 二、網路詐欺：

（一）依一般網路犯罪案件管轄責任區分（非以第一次匯款地之警察機關主辦）。

- 1、以網路犯罪被害人現住所或戶籍所在地之警察機關為管轄機關。
- 2、以網路犯罪被害人上網發生權益受損之上網所在地之警察機關為管轄機關。
- 3、以犯罪嫌疑人現住所或戶籍地或上網從事犯罪行為之所在地之警察機關為管轄機關（如被害人可提供懷疑對象）。

4、以被害人發生權益受損之網頁、電子郵件、新聞群組、BBS 站等各項網路服務及網路位址伺服器所在地之警察機關為管轄機關。

（二）有關網路購物、拍賣疑有交易糾紛之案件，應先行查證釐清，確屬以人頭帳戶作為詐財工具，以隱瞞真實身份，防止司法機關追查之情形，方可列為警示帳戶；如係交易糾紛案件，不得列為警示帳戶，

可請被害人循民事求償程序辦理，以維雙方權益。

三、恐嚇取財案件：(涉及人頭帳戶案件)

(一) 竊車恐嚇取財：由車輛失竊地之警察機關負責偵辦。

(二) 網鴿恐嚇取財：由被害人居住地或飼養鴿子之所在地之警察機關負責偵辦。

(三) 其他恐嚇取財案件：以發生地之警察機關負責偵辦。

四、各市、縣(市)警察局專責組任務：

(一) 管制各所屬分局、分駐(派出)所受理利用人頭帳戶詐欺、恐嚇取財案件(含確認金融機構列警示通報帳戶、財金公司監看跨行提領狀況、電信公司斷線斷話事宜及所屬各受理管轄分局「人頭資料庫」建檔作業)。

(二) 統籌調度所屬各單位利用人頭帳戶、電話詐欺案件偵處作為；恐嚇取財案件偵辦部分仍由前述原管轄警察機關負責。

五、各專業警察機關處理流程比照本處理執行規定陸、處理流程二、受理他轄案件應辦事項辦理。

陸、處理流程

一、人頭帳戶(流程圖如附件一)

(一) 受理本轄案件：

1、分駐(派出)所應辦理事項：

(1) 單純檢舉案件：

檢具相關檢舉資料(或製作筆錄)陳報分局刑事組列管偵處。

(2) 被害案件：

甲、受理報案並依相關規定填製各項表報。

乙、填報「詐欺帳戶通報警示、詐騙電話斷話簡便格式表」及「報案三聯單」傳真至人頭帳戶開戶金融機構通報警示。

丙、將前項簡便格式表及相關報案(筆錄、三聯單、匯款明細表等)、檢舉告發資料陳送分局辦理。

2、分局刑事組應辦理事項：

(1) 審核分駐(派出)所陳報資料。

(2) 三日內製作正式公文函發金融機構(後補)將帳戶列為警示帳戶(終止人頭帳號使用提款卡、語音轉帳、網路轉帳、其他電子支付轉帳)、提供開戶人基本資料，並副知警察局專責組追蹤、列管。

(3) 將被害(檢舉)人基本資料、轉帳明細及金融機構回復之開戶基本資料依規定輸入人頭資料庫及相關刑案系統。

(4) 調閱交易明細、通聯紀錄、錄影帶等資料積極偵辦。

(5) 查明人頭帳戶是否屬遭偽(變)造或冒名開立，函復金融機構。

(6) 屬重大刑案者依通報程序通報。

(7) 分局依轄區責任負責偵辦全案，並報由警察局專責組列管及請求協助警力支援、調度。

(8) 逕行受理民眾報案者，應依前述1、2各項辦理。

(9) 接獲由他轄依單一窗口受理移轉之案件，仍應依前列(4)、(5)、(6)、(7)點辦理。

(10) 相關資料陳報(副知)警察局專責組辦理。

3、警察局專責組應辦理事項：

(1) 管制分局函文金融機構協助將帳戶列為警示帳戶(終止人頭帳號使用提款卡、語音轉帳、網路轉帳、其他電子支付轉帳)及提供開戶人基本資料。

(2) 管制分局輸入人頭資料庫及相關刑案系統。

(3) 分析監控轄區受理人頭資料庫，或接受分局對具時效性之詐欺案件，製作函文傳真財金資訊公司監看跨行提領狀況，正式公文後補。

※ 注意事項：目前財金公司係以人工方式協助各單位監看通報警示帳戶，僅可同時監看 20 線帳戶，故各單位應先查證過濾後再請財金公司監看，以免過度氾濫，反而無法產生實效。

(4) 管制、督促分局調閱交易明細、通聯紀錄、錄影帶等資料積極偵辦及查明人頭帳戶是否屬遭偽(變)造或冒名開立，函復金融機構。

(5) 管制由他轄(或本轄)依單一窗口受理移轉之案件。

(6) 逕行受理民眾報案者，依前列 1、2、3 各點辦理並偵辦。

(7) 管理人頭資料庫。

(二) 受理他轄案件：

1、分駐(派出)所應辦理事項：

(1) 單純檢舉案件：

檢具相關檢舉資料(或製作筆錄)陳報分局刑事組列管偵處。

(2) 被害案件：

甲、受理報案並依相關規定填製各項表報。

乙、填報「詐欺帳戶通報警示、詐騙電話斷話簡便格式表」及「報案三聯單」傳真至人頭帳戶開戶金融機構通報警示。

丙、將前項簡便格式表及相關報案(筆錄、三聯單、匯款明細表等)、檢舉告發資料陳送分局辦理。

2、分局刑事組應辦理事項：

(1) 審核分駐(派出)所陳報資料，確認管轄歸屬。

(2) 三日內製作正式公文函發金融機構(後補)將帳戶列為警示帳戶(終止人頭帳號使用提款卡、語音轉帳、網路轉帳、其他電子支付轉帳)、提供開戶人基本資料，並副知警察局專責組追蹤、列管。

(3) 將被害(檢舉)人基本資料、轉帳明細等輸入人頭資料庫及相關刑案系統。

(4) 將金融機構回復之開戶基本資料輸入人頭資料庫，並將資料函轉管轄分局及副知所屬警察局專責組管制。

(5) 將報案資料依受理單一窗口報案流程，先行傳真管轄單位分局勤務指揮中心，正式公文後補並副知警察局專責組。

(6) 逕行受理民眾報案，而案屬他轄者，依前列 1、2 各點辦理。

3、警察局專責組應辦事項：

(1) 管制分局函文金融機構協助將帳戶列為警示帳戶(終止人頭帳號使用提款卡、語音轉帳、網路轉帳、其他電子支付轉帳)

等相關資料。

(2) 查證過濾後確實緊急需代管轄單位製作函文傳真財金資訊公司監看跨行提領狀況，正式公文後補並副知管轄單位。

(3) 管制分局輸入人頭資料庫及相關刑案系統。

(4) 管理人頭資料庫。

(三) 警示帳戶臨櫃提領之處置：

警示帳戶遇嫌疑人臨櫃提領，警察機關接獲金融機構通報，應立即派員前往協助查證，並深入調查有無不法，以求迅速偵破，減輕民眾損失。其處理流程如下：

- 1、調閱開戶人基本資料及資金交往明細資料與涉嫌人資料相互查核其身分及交易明細是否為開戶人本人。
- 2、如為詐欺集團之成員立即移送法辦。
- 3、如為志願性人頭戶（販賣帳戶者）應移送法辦。
- 4、若遭歹徒冒用開立帳戶之無辜第三人則函請金融機構准予重新開戶（惟該偽冒開立之帳戶仍應列警示）。

(四) 協助民眾遭冒名申請金融帳戶撤銷警示

各警察機關受理民眾遭冒名申請金融帳戶案件，經查證屬實後，應函請設置警示帳戶之金融機構准許其重新開戶，惟該遭冒名之帳戶仍應持續列管警示，並副知本署刑事警察局更正註記人頭資料庫資料（無須副知財團法人聯合徵信中心）。

(五) 協助金融機構處理滯留於『警示帳戶』內剩餘款項發還事宜

- 1、各警察機關於金融機構依「返還滯留於『警示帳戶』內剩餘款項作業程序」第三點，請求查明「警示帳戶」內有幾個被害人報案時，應依該作業程序所定格式於文到七日內查明函覆。
- 2、有關作業程序四之（二）協尋帳戶開戶人部分，由本署刑事警察局彙整函發各警察機關協尋一個月（協尋期間含警方已通緝期間），協尋有無結果各警察機關均應以各銀行總行為分類，於文到一個月內報由本署刑事警察局彙整函覆。

二、人頭電話（流程圖如附件二）

(一) 受理本轄案件：

1、分駐（派出）所應辦理事項：

(1) 單純檢舉案件：

檢具相關檢舉資料(或製作筆錄)陳報分局刑事組。

(2) 被害案件：

甲、受理報案並依相關規定填製各項表報。

乙、填報「詐欺帳戶通報警示、詐騙電話斷話簡便格式表」傳真至電信公司協助斷話。

丙、將前項簡便格式表及相關報案（筆錄、三聯單等）、檢舉告發資料陳送分局辦理。

2、分局刑事組應辦理事項：

(1) 審核分駐（派出）所陳報資料。

(2) 三日內製作正式公文函發電信公司（後補）協助斷話、提供申請人基本資料，並副知警察局專責組追蹤、列管。

- (3) 將被害(檢舉)人基本資料、人頭電話及電信公司回復之申請人基本資料依規定輸入人頭資料庫及相關刑案系統。
- (4) 調閱交易明細、通聯紀錄、錄影帶等資料積極偵辦。
- (5) 若查明誤斷電話，應函文電信公司復話。
- (6) 屬重大刑案者依通報程序通報。
- (7) 分局依轄區責任負責偵辦全案，並報由警察局專責組列管及請求協助警力支援、調度。
- (8) 逕行受理民眾報案者，應依前述1、2各項辦理。
- (9) 接獲由他轄依單一窗口受理移轉之案件，仍應依前列(4)、(5)、(6)、(7)點辦理。
- (10) 相關資料陳報(副知)警察局專責組辦理。

3、警察局專責組應辦理事項：

- (1) 管制分局函文電信公司協助斷話及提供申請人基本資料。
- (2) 管制分局輸入人頭資料庫及相關刑案系統。
- (3) 管制、督促分局調閱交易明細、通聯紀錄、錄影帶等資料積極偵辦。
- (4) 管制由他轄(或本轄)依單一窗口受理移轉之案件。
- (5) 逕行受理民眾報案者，依前列1、2、3各點辦理並偵辦。
- (6) 管理人頭資料庫。

(二) 受理他轄案件：

1、分駐(派出)所應辦理事項：

- (1) 單純檢舉案件：  
檢具相關檢舉資料(或製作筆錄)陳報分局刑事組。
- (2) 被害案件：
  - 甲、受理報案並依相關規定填製各項表報。
  - 乙、填報「詐欺帳戶通報警示、詐騙電話斷話簡便格式表」傳真至電信公司協助斷話。
  - 丙、將前項簡便格式表及相關報案(筆錄、三聯單等)、檢舉告發資料陳送分局辦理。

2、分局刑事組應辦理事項：

- (1) 審核分駐(派出)所陳報資料，確認管轄歸屬。
- (2) 三日內製作正式公文函發電信公司(後補)協助斷話、提供申請人基本資料，並副知警察局專責組追蹤、列管。
- (3) 將被害(檢舉)人基本資料、人頭電話等輸入人頭資料庫及相關刑案系統。
- (4) 將電信公司回復之申請人基本資料輸入人頭資料庫，並將資料函轉管轄分局及副知所屬警察局專責組管制。
- (5) 將報案資料依受理單一窗口報案流程，先行傳真管轄單位分局勤務指揮中心，正式公文後補並副知警察局專責組。
- (6) 逕行受理民眾報案，而案屬他轄者，依前列1、2各點辦理。

3、警察局專責組應辦理事項：

- (1) 管制分局函文電信公司協助斷話及提供申請人基本資料。
- (2) 管制分局輸入人頭資料庫及相關刑案系統。
- (3) 管理人頭資料庫。

## 柒、人頭資料庫管考

### 一、管制：

- (一) 每一涉有金融帳戶資料、電信電話之詐欺及恐嚇取財案件，一經受理即應陳報分局、警察局專責組輸入，以便即時斷話、監控帳號，進而偵破案件。
- (二) 帳號經監看 14 天仍未偵破者，第 15 天起自動取消監看，如需延長應另行傳真及函文續監管，偵破案件時應依規定輸入偵破狀況，並通知財金公司取消監看。
- (三) 人頭資料庫操作使用，應遵循電腦處理個人資料保護法、本署電子計算機作業保密安全實施規定、刑案資料查詢作業及人頭資料庫系統操作手冊相關規定。
- (四) 警察局專責組應管制、督考所屬有無將案件資料（含偵辦情形及進度）依規定輸入人頭資料庫，保持資料常新與完整。

### 二、督導考核：

- (一) 受理報案單位應確實依處理流程於受理報案查證屬實後，立即傳真金融機構、電信公司通報警示、斷話，分局刑事組於收到分駐（派出）所陳報資料後應於三日內製作正式公文函發電信公司或金融機構（後補公文），且應立即輸入人頭資料庫。
- (二) 受理報案及審核單位應確實依處理流程於受理報案起 48 小時內，將全案相關資料函發上級或管轄單位。
- (三) 本署每月將抽查稽核人頭資料庫，凡經受理而未依前二項規定通報、陳報、審核、輸入或傳真協助斷話、列為警示帳戶者，列入獎懲考核。
- (四) 案件偵破符合報領刑事類獎勵金者，應檢附輸入人頭資料庫資料影本，未檢附者，不予核發獎勵金。

### 三、獎懲規定：

#### (一) 獎勵：

項目	件數	承辦人獎勵額度 (不含協辦人員)	期間	備註
輸入人頭資料庫且資料完整者(含他轄轉本轄續建檔人頭帳戶及人頭電話等)	50(含)筆以下 ~21筆	嘉獎壹次	各警察機關每半年累計依權責自行辦理獎勵。	經稽核發現達最高敘獎額度(獎獎貳次)後，即不輸入或懈怠輸入者，除撤銷原獎勵外，並從嚴議處。
	100(含)筆以下 ~51筆	嘉獎貳次		

(二) 懲處：審核發現未依規定程序完成輸入人頭資料庫者，依「警察人員獎懲標準表」規定辦理懲處。

(三) 本署辦理人頭資料庫系統管理、稽核、管制分析不法詐欺集團之業務承辦人員、組長及正(副)主管，每半年於嘉獎範圍內簽報獎勵。

### 捌、訓練講習

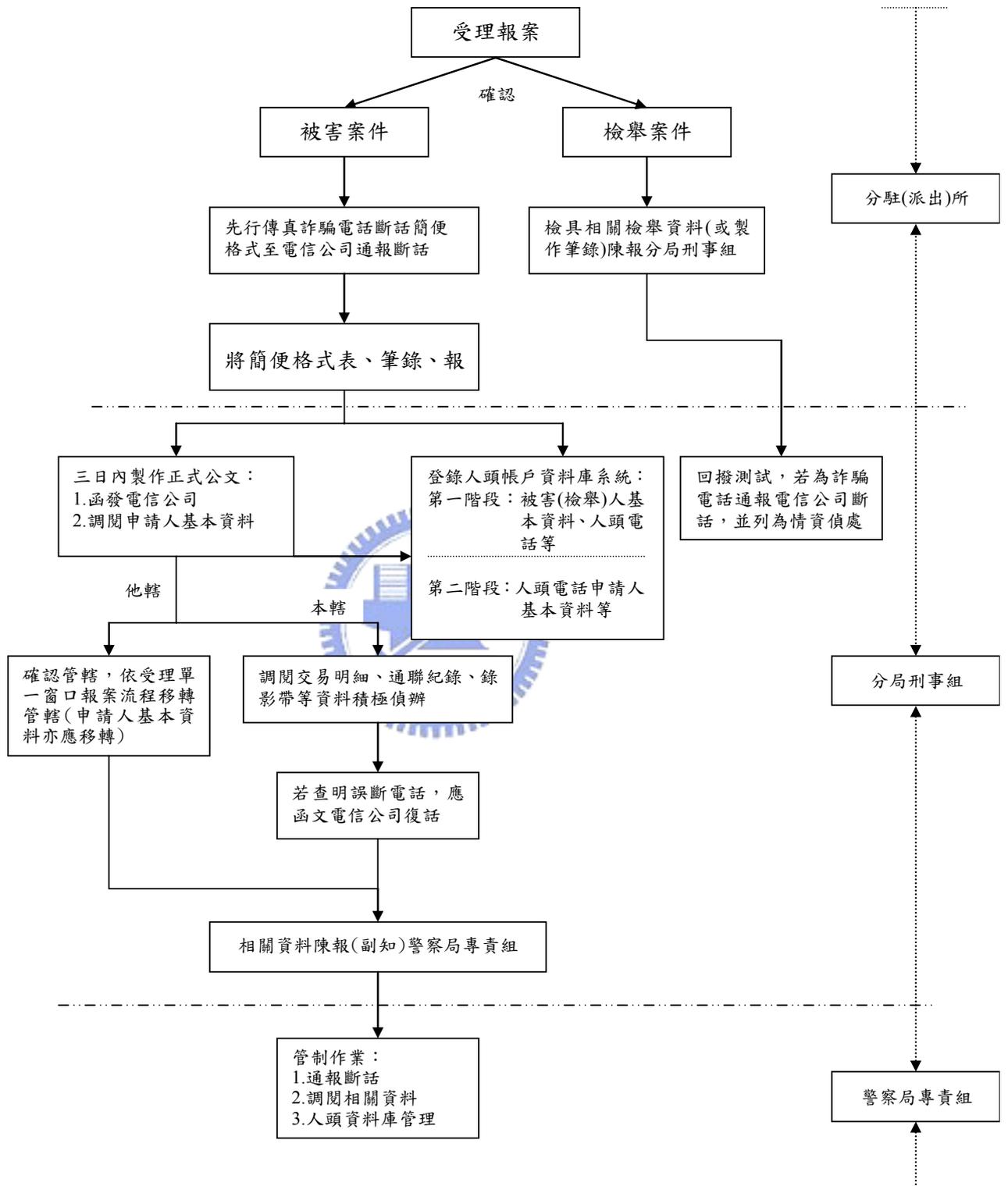
各市、縣(市)警察局專責組應依本處理執行規定，擔任種子教官，配合各種訓練、勤教場合對員警實施訓練講習並紀錄備查。

### 玖、相關函示資料(如附件三)

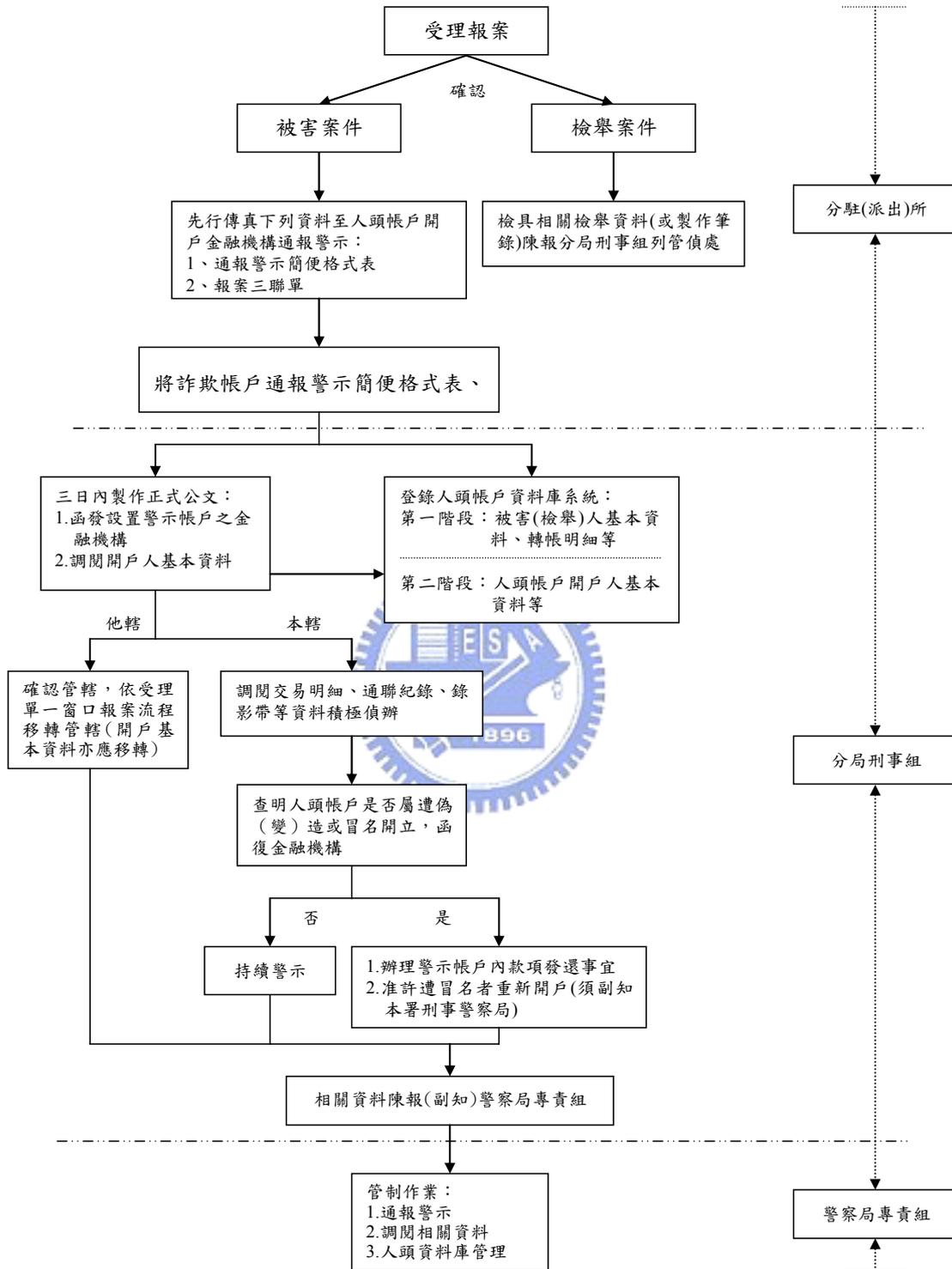
- 一、93年9月15日警署刑偵字第0930136441-A號函。
  - 二、93年10月12日警署刑偵字第0930153110號函。
  - 三、93年11月16日警署刑偵字第0930173445號函。
  - 四、93年12月30日警署刑偵字第0930194563號函。
  - 五、94年1月27日警署刑偵字第0940006418號函。
  - 六、94年3月4日警署刑偵字第0940019783號函。
- 拾、本處理執行規定如有未盡事宜，得隨時以函文補充之。



# 警察機關受理詐欺案件通報電話斷話(復話)流程圖



# 警察機關受理詐欺案件通報(解除)警示帳戶流程圖



### 附 錄 三

#### 受理詐騙帳戶通報警示、詐騙電路段話簡便格式

0 0 0 警 察 局 0 0 分 局 0 0 派 出 所  
受理詐騙帳戶通報警示、詐騙電話斷話簡便格式表

發生日期時間	年 月 日 時 分	承辦單位 電話	警用：_____ 自動：_____	
人 頭 帳 戶	人頭帳戶銀行名稱 <small>(匯款結果地之銀行或郵局)</small>		____銀行(郵局)____分行(支局) 銀行代碼_____	
	人頭帳戶帳號		帳號：_____；_____	
	匯款結果地之 銀行或郵局	郵遞區號：____地址：_____		
	匯款地點		損失金額 _____ 元	
人頭電話 <small>(此欄填寫人頭帳戶 聯繫電話，如有數支聯 絡電話，請依序填寫)</small>				
被 害 人	姓 名	聯絡電話	學 歷	
	地 址	被害人 帳 號	銀行代碼_____ 帳 號_____	
	出 生 年 月 日	年 月 日	身分證字號	
受理單位 <small>(指受理報案之單 位，如他轄轉本轄時請 填寫何分局轉本轄)</small>	____分局____派出所		受 理 時 間  年 月 日 時 分	
管轄單位 <small>(第一次匯款結果地 警察機關)</small>	____警察局____分局			
報案三聯單 碼	NO：_____	<input type="checkbox"/> 本轄受理本轄案件。 <input type="checkbox"/> 本轄受理轉他轄案件，應轉至____警察局____分局案件。 ____年__月__日 字____號移轉他轄辦理(分局刑事 組轉他轄時請填註本欄)。 <input type="checkbox"/> 他轄已受理轉本轄案件，____警察局____分局轉至本轄案件。		
收 受 傳 真 單 位	金 融 機 構	電 信 公 司	警 察 分 局	警 察 局
	行(局)	公 司	分 局	
	年 月 日 時 分	年 月 日 時 分	年 月 日 時 分	年 月 日 時 分
	受話人	受話人	受話人	受話人
	電 話	電 話	電 話	電 話
備 註 <small>(案類：請勾選)</small>	<input type="checkbox"/> 刮刮樂詐欺 <input type="checkbox"/> 虛設行號詐欺 <input type="checkbox"/> 假退稅真詐財 <input type="checkbox"/> 信用貸款詐欺 <input type="checkbox"/> 簡訊詐財 <input type="checkbox"/> 色情廣告詐財 <input type="checkbox"/> 求職詐欺 <input type="checkbox"/> 恐嚇詐欺 <input type="checkbox"/> 通知假消費真詐財 <input type="checkbox"/> 網路詐欺 <input type="checkbox"/> 其他 <small>(簡述犯案手法)</small> ：			

受理單位戳章：

填表人：

主管：

## 簡 歷

古慧珍，1975 年生，已婚，一女

東吳大學法律系畢業（民國83年-87年）

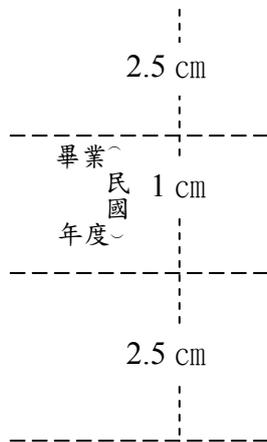
司法官特考及格（民國88年）

彰化地方法院檢察署檢察官（民國90年1月10月）

交通大學科技法律研究所（民國 91 年-95 年）

桃園地方法院檢察署檢察官（民國91年10月迄今）

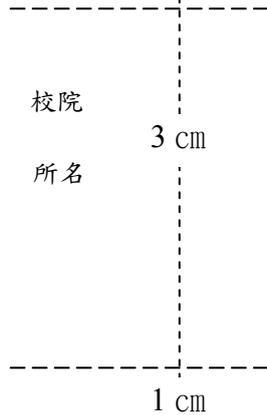




畢業  
民國  
年度

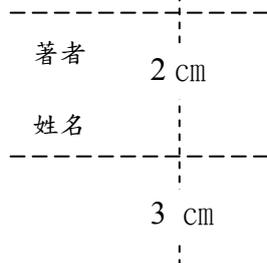
94 碩士論文

論文  
題目



校院  
所名

交通大學  
管理學院  
科技法律研究所



著者  
姓名

古慧珍



94 碩士論文

我國網路詐欺  
防範之研究  
——以使用人頭帳戶為中心

交通大學  
管理學院  
科技法律研究所

古慧珍