簡訊犯罪資料探勘與防範措施之研究

A Study on Data Mining and Precaution for the Crimes of Mobile Phone Short Message Services

賴森堂
屏東商業技術學院資訊科技系
屏東市 900 民生東路 51 號
stlai@npic.edu.tw

林宜隆
中央警察大學資訊管理學系
桃園縣龜山鄉 333 大崗村樹人路 56 號
illin@www.im.cpu.edu.tw

摘要

高普及率的行動電話儼然已成爲無線通訊 E 世代不可或缺的通訊工具，各種加諸在行動電話的服務項目更是不斷被推出，手機簡訊（Short Message Service，SMS）就是透過文字以行動電話即時傳遞訊息的一項服務。行動電話具備高度機動性且使用人數眾多，使得簡訊傳輸服務不僅廣受歡迎且造成非常熱烈的迴響，不過，卻也成爲詐騙集團的犯罪工具。利用行動電話簡訊進行犯罪的行爲有愈來愈多的趨勢，如何有效嚇阻且打擊簡訊犯罪以維護社會秩序是刻不容緩的工作。本文針對行動電話簡訊犯罪的行爲進行瞭解與剖析，且深入探討簡訊犯罪過程中所留下的犯罪資料，進而整合犯罪資料的搜尋、擷取、解譯、推導、篩選、分類、統計與分析等功能，提出一套行動電話簡訊犯罪資料探勘模式，以具體提昇行動電話簡訊犯罪偵查作業的執行效率與品質。有計畫的簡訊犯罪，歹徒會事先規劃犯罪行爲與資料的掩飾工作，造成犯罪偵查的一大阻礙，爲此，本文從行動電話的門號申請、簡訊傳送監控及銀行匯款監控等作業提出一套簡訊犯罪的防範措施，以具體且有效的打擊行動電話簡訊犯罪的行爲。

關鍵詞：簡訊犯罪、資料探勘、防範措施、行動電話、通聯紀錄。

Abstract

Short Message Service (SMS) is a service of mobile phone which can transmit the text message in real time. High mobility and high universality are two major features of mobile phone that make SMS become a very popular transmission service. However, the evil fellows use SMS to cheat for money. The crime behavior of SMS is more and more serious. How to terminate or prevent the crime of SMS, become an important issue for improving public security. In this paper, the crime behavior of SMS will be surveyed and analyzed. Characteristics and procedure of SMS crime will be discussed and studied. And, a data mining model for the SMS crime which integrates searching, retrieval, interpretation, deduction, selection, classification, statistic and analysis functions will be proposed. Applying

the crime detective data which produce by the data mining model, the efficiency and quality of SMS crime detective operations can be improved. On the other hand, SMS crime with perfect plan, the evil fellows will be beforehand with covering their crime data and behavior. For this, the precaution of SMS crime that includes mobile phone application, SMS transmission monitoring and bank account remittance monitoring will be proposed in this paper. Based on the precaution of SMS crime, the SMS crime can be prevented and reduced.

Keywords: SMS, data mining, precaution, mobile phone, call records

一、緒論

E 世代網路通訊積極努力的重要目標就是具體且有效的提昇人與人之間溝通與互動的效率，爲了達成此項目標，各種通訊研究成果與相關的設備紛紛出籠，其中又以無線通訊爲最具潛力、最熱門且最受歡迎的通訊方式之一。無線通訊於電信業務開放民營後，在業者間良性的相互競爭下，積極進行各項基礎建設且裝置配備新穎的通訊設施，以有效吸引不同層級的客戶群，其中又以行動電話業務最爲顯著。每年的行動電話用戶數都在持續成長中，依據電信總局於民國 90 年 12 月公布的統計數字顯示，全國六家行動電話業者的用戶數已超過 2,160 萬，普及率高達 96.6% 僅次於盧森堡的 96.7%，高居世界第二，以 2,300 萬的台灣人口數來計算，幾乎已經接近人手一機的階段。爲了服務廣大的用戶數以提高業績，各種推陳出新的行動電話服務項目，在業者積極且有心的促銷下，不僅迅速的捕獲年輕用戶的心且爲一般用戶所接受，行動電話簡訊便是其中一項促銷成功且廣受歡迎的服務項目。根據中華電信的統計，民國 91 年農曆過年期間，一天的簡訊發送量就高達四百多萬通，有此可見行動電話簡訊已逐漸取代特殊節日寄送卡片的功能。

行動電話開放民營後，業者間相互競爭的熱度逐漸升高，各種優惠措施與促銷方案相繼推出，目的就是要積極拉攏新的客戶群以提昇其業績，對於應該嚴格把關且仔細確認的客戶申請資料反而不加重視，使得行動電話門號的取得不僅太過容易甚至有些浮濫，歹徒不費力氣就可以輕易取得足以掩飾身份的犯罪工具。行動電話簡訊成爲廣受歡迎的通訊方式後，也成爲詐騙集團騙取錢財的工具，詐騙集團利用人性貪婪的弱點，將「中獎通知」或「低價商品」等不實簡訊透過行動電話傳送給特定的民眾，儘管大部份的民眾不易受此類型簡訊的誘騙，不過，仍舊有少數財迷心竅的民眾受不了高額獎金或低價商品的誘惑，會以簡訊中所提供的查詢電話主動與歹徒聯絡，受害民眾一旦落入詐騙集團設下的圈套，就很難全身而退，小者部份錢財，大者所有積蓄將匯入或轉進歹徒所預設的銀行帳戶。行動電話簡訊的詐騙過程中，歹徒也留下了許多具偵查效用的犯罪資料：(1) 依據發送簡訊的發話號碼可以追查出發送者與發送區域[5][8][17]； (2) 歹徒簡訊中留下的查詢電號，可以追查出電話用戶及電話互聯的相關資料[8][16]；(3) 歹徒要求被害人匯入或轉進的銀行帳戶，可以追查出開戶及戶頭往來的相關資料。建立一套簡訊犯罪資料的探勘模式[4]，可以有效提昇偵查作業的品質與效率，但是，在歹徒有計畫的犯罪行爲下，犯罪資料不僅難以追查出歹徒，更可能誤導偵查的方向。從「預防重於治療」的角度思考，如何有效的降低或嚇阻簡訊犯罪，具體的防範措施是值得深入探究的話題[2]。

經濟不景氣，失業率居高不下，歹徒透過各種詐騙方式取得不當錢財的犯罪行爲，有愈來愈多的趨勢。其中又以行動電話的簡訊犯罪最值的重視，歹徒利用新的通訊技術「行動電話簡訊」當做犯罪工具，以騙取被害人的錢財，如何有效嚇阻且打擊行動電話簡訊犯罪以維護社會秩序是刻不容緩的工作。本文針對行動電話簡訊犯罪的行爲進行深入的剖析，以瞭解簡訊犯罪型態，且以立意抽樣方式，將最近的簡訊詐財案中較爲引起輿論注意的案例，以框架表示式分析其行爲，進而整合犯罪資料的搜尋、擷取、解譯、推導、篩選、分類、統計與分析等功能，提出一套行動電話簡訊犯罪資料探勘模式，以具體的提昇行動電話簡訊犯罪偵查作業的執行效率與品質。此外，本文從簡訊犯罪行爲的掩飾及犯罪偵查的角度進行探討，彙集三方面的簡訊犯罪防範方式包括:行動電話門號的申請作業、簡訊資料傳送的監控作業及銀行帳戶匯款的監控作業等，建立一套簡訊犯罪的防範措施，在歹徒的犯罪行爲未得逞前，立即終結其犯行，以有效嚇阻簡訊犯罪行爲。行動電話通聯紀錄與銀行的交易紀錄都涉及商業機密及個人隱私，資料取得相當困難，爲此本文並未針對所提之模式與措施進行實際的驗證。本文第二節將詳細探討行動電話簡訊犯罪型態，且舉出最近發生的四個簡訊詐騙案例，以深入分析行動電話簡訊詐騙流程與特徵。第三節將從行動電話簡訊犯罪所留下的原始犯罪資料包括：發送簡訊的發話號碼、供查詢或確認的電話號碼及要求匯款或轉帳的帳戶號碼等，進行資料源頭的探討與說明。第四節將分別討論犯罪資料的搜尋、擷取、解譯、推導、篩選、分類、統計與分析等功能，且結合這些功能提出一套行動電話簡訊犯罪資料探勘模式。第五節將探討歹徒掩飾犯罪行爲與犯罪偵查的方式，進而從行動電話門號的申請、簡訊資料傳送的監控及銀行帳戶及匯款的監控等作業提出簡訊犯罪的防範措施，以有效嚇阻簡訊的犯罪行爲。最後，於第六節將再次說明簡訊犯罪資料探勘模式的特性及防範措施的優勢，且針對本文所探討的主題作結論。

二、行動電話簡訊犯罪型態探討

詐騙集團以行動電話簡訊做爲詐財的工具，有日益嚴重的趨勢，瞭解且剖析行動電話簡訊的犯罪行爲與流程是蒐集與精鍊行動電話簡訊犯罪資料[4]及規劃犯罪防範措施的依據。

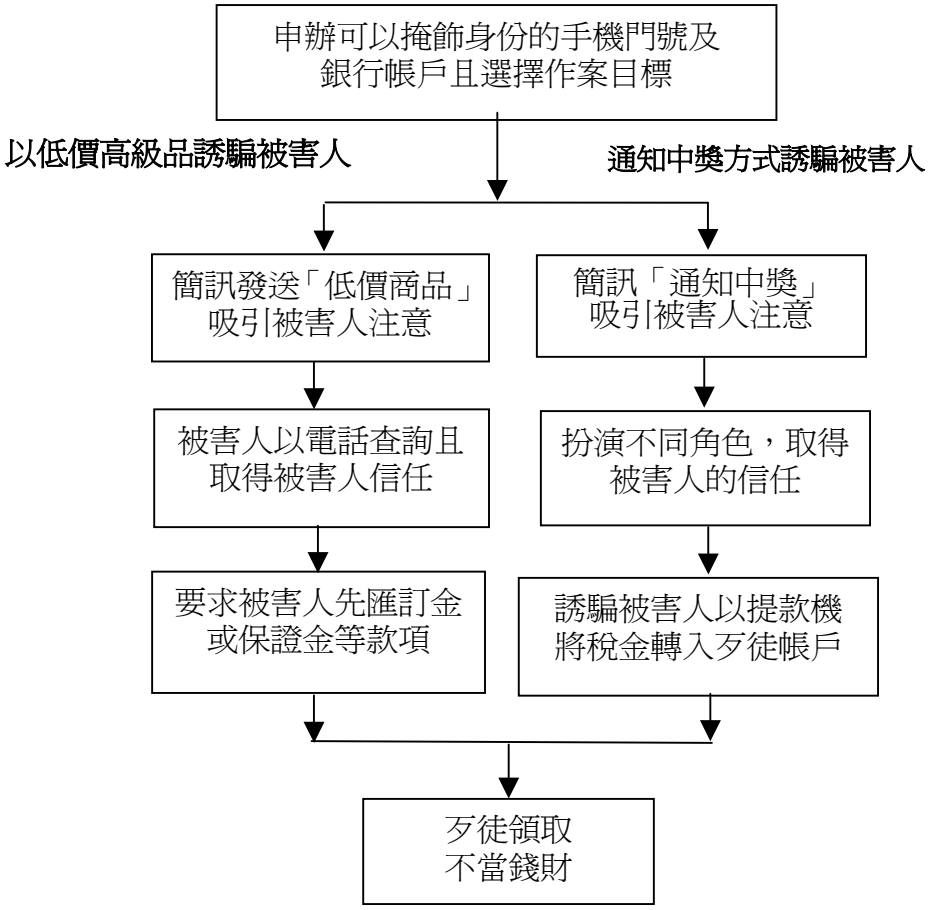
1. 行動電話簡訊詐騙流程剖析

蒐集最近發生的一些重要行動電話簡訊犯罪的案例，可以歸納出簡訊犯罪的一些特徵與犯罪過程，這些案例的犯罪方式與過程，將可協助我們進行行動電話簡訊犯罪資料蒐集與探勘的作業。利用人性貪婪的弱點，騙取不當的錢財是簡訊犯罪的最終目的，歹徒爲了使一般民眾上當，順利騙得不當的錢財，一般都必須經過精心的策劃，甚至由多人扮演不同角色一起參與犯案以取得被害人的信任，被害人一旦喪失防範的戒心，便會將款項自動匯入或或轉入歹徒帳號，歹徒便可輕鬆領取騙來的錢財。整個簡訊詐騙的作案流程如圖一所示，可以分成下面五個步驟：

步驟 1：申辦可以掩飾身份的手機門號及銀行帳戶作爲犯罪工具，同時選定作案目標。
步驟 2：發送「低價高級商品」或「中獎通知」等簡訊，引起被害人的注意。
步驟 3：透過各種方式取得被害人的信任，使被害人喪失防範的戒心。
步驟 4：要求被害人匯款或誘騙被害人以提款機轉帳等方式，將錢存入歹徒帳戶。

步驟 5：歹徒提領被害人匯入或轉入的所有款項。

歹徒發送「低價高級商品」或「中獎通知」等誘騙簡訊時，也會提供相關的聯絡電話，以便接受被害人的查詢且取得被害人的信任。此外，歹徒爲了要求被害人事先匯款或誘騙被害人轉出存款，都會提供預先開設好的銀行帳號，以便接收匯款及轉入的款項，這些騙取被害人錢財的犯罪過程中所留下的原始犯罪資料，也正是偵查與蒐集行動電話簡訊犯罪資料的重心。



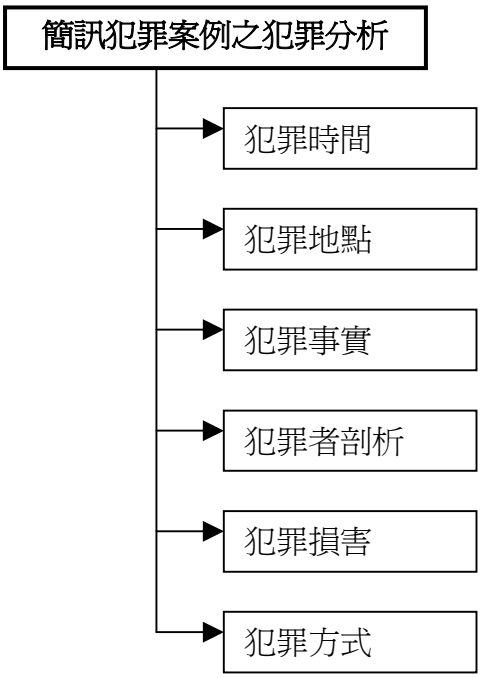
圖一：一般行動電話簡訊犯罪流程圖

2. 簡訊的詐騙案例之犯罪分析

爲瞭解最近行動電話簡訊犯罪的現況，以有效協助犯罪資料的蒐集探勘作業，就必須廣泛蒐集及選取行動電話簡訊犯罪案例加以分析，本文以立意抽樣(Purposive Sampling)方式，將最近發生的簡訊詐財案中，較具代表性且引起輿論注意的案例，以框架(Frame)結構(如圖二所示)表示犯罪的分析方式[1]：

案例 1：三嫌僞造證件辦門號，傳簡訊詐財

(1) **犯罪時間**：民國九十一年十月
(2) **犯罪地點**：高雄市
(3) **犯罪事實**：高雄市警方破獲一個專門以假身分證辦理手機門號，再販售門號圖利，並以簡訊詐財的集團，起出近兩百張身分證，逮捕三名嫌犯。

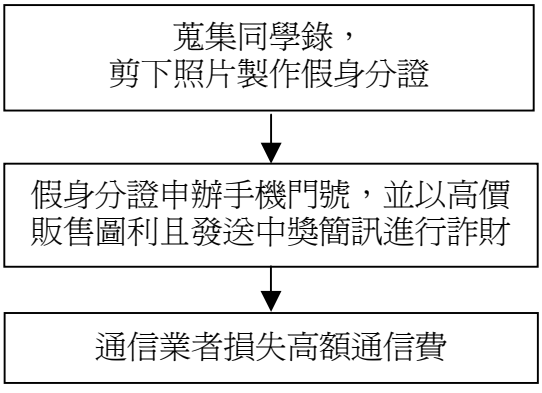


圖二：犯罪分析框架結構示意圖

(4) **犯罪者剖析：**警局桌上滿滿的近兩百張僞造身分證正本和影印本，就是嫌犯拿來申請手機門號圖利的工具。嫌犯是先拿到學校的同學錄將照片剪下來後，製作假身分證，到電信公司申辦門號，並以一個門號八千到一萬元的價格，販售圖利。不只販售圖利。嫌犯還用假身分證申請來的門號四處發送中獎簡訊，騙取稅金，電信業者競爭激烈，申辦門號簡便，假人頭假身分證就可以輕申請到到門號，業者防不勝防。業者表示，每個月至少會發生十多起類似案件最多一個門號被盜打十多萬元，由於帳單地址多是不法集團的假地址，在追討無門的情況下，只好自己承擔損失，並在追蹤申辦人通話狀況，查出異常緊急斷話，不過業者感嘆，面對這樣的損失現在實在無計可施。

(5) **犯罪損害：**民眾遭詐騙集團騙取稅金，通信業者損失高額通信費。

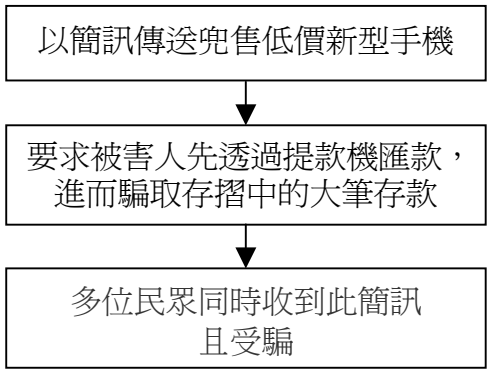
(6) **犯罪方式：**參閱圖三所示。



圖三：案例 1 的犯罪方式流程

案例 2：轉帳購手機錢被提光光

(1) 犯罪時間：民國九十一年十月
(2) 犯罪地點：台中縣沙鹿鎮
(3) 犯罪事實：林姓女子從手機簡訊中，向坊間詐騙集團，以三千元購買市價兩萬餘元的手機，不僅手機未見蹤影，歹徒十分鐘內利用跨行轉帳方式，將林姓女子及母親三本存摺內二十餘萬元，利用提款卡詐騙一空。
(4) 犯罪者剖析：歹徒利用手機傳遞簡訊方式，以三千元兜售目前坊間一支兩萬餘元，具有衛星追蹤功能的新型手機，且要求被害人依手機號碼與對方連絡。歹徒宣稱首次購物不受理現金，要求她到台中市自由路的土地銀行，利用提款卡轉帳三千元到指定帳戶，等收到匯款後，立即派員將手機送到她手上。歹徒的用意並非只是區區的三千元，而是存摺中的高額存款，因此，歹徒宣稱因電腦當機未收到轉帳，且提供假冒全國中央金控中心銀行女性行員之電話號碼，要求受害人與該行員聯絡，最後在假冒銀行女性行員的指示操作下，將不同存摺內共二十餘萬元的存款匯入歹徒的銀行帳戶。
(5) 犯罪損害：多位民眾損失存摺存款。
(6) 犯罪方式：參閱圖四所示。



圖四：案例 2 的犯罪方式流程

案例 3：手機簡訊詐財，大學女生受騙

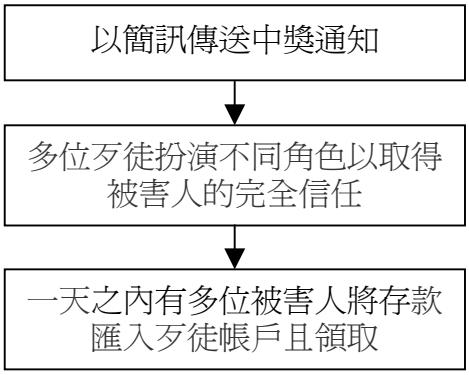
(1) **犯罪時間**：民國九十年十二月二十九日
(2) **犯罪地點**：高雄市
(3) **犯罪事實**：就讀大學的被害人陳女是收到歹徒手機簡訊，指某科技公司週年酬賓，恭喜抽中三獎現金廿八萬元，並留下免付費電話供連絡，陳女回電後，歹徒即表示應先向贈獎見證律師連絡，手續完備才可領獎，陳女見領獎過程如此嚴謹不疑有他，乃與律師連繫。 歹徒假扮的律師則佯稱尚要準備兩個以上的帳戶供會計部門轉帳匯款，並由會計部門確認內碼後，扣除稅捐及手續費後再匯款。不久，陳女陳女就接獲會計部門的電話通知，謊稱爲便查證款項是否匯入，請陳女到自動提款機，先以金融卡查詢餘額後並以電話告知帳戶餘額後，依指示輸入第一組內碼確定是否中獎，然後再要求

輸入第二組內碼，隨後一再謊稱內碼錯誤再重新輸入，直至帳戶內金額完全被領光爲止，然後再聲稱帳戶有問題無法領獎要求更換另個帳戶，待陳女查覺有異時，帳戶早被提領一空。

(4) **犯罪者剖析：**歹徒以手機簡訊傳送中獎通知，且利用被害人一時貪念且不熟悉提款機的操作方式，指示被害人以提款卡查詢是否完成匯款動作，而騙走被害人卅餘萬元積蓄，警方特別公佈此種翻新的手機簡訊詐財手法，呼籲民眾不要自恃未輸入金額而讓歹徒得逞。

(5) 犯罪損害：一天之內匯入歹徒帳戶且被領取款項有數百萬元之多。

(6) 犯罪方式：參閱圖五所示。



圖五：案例 3 的犯罪方式流程

案例 4：帳戶被鎖定，騙徒提款中伏

(1) **犯罪時間：**民國九十一年十月

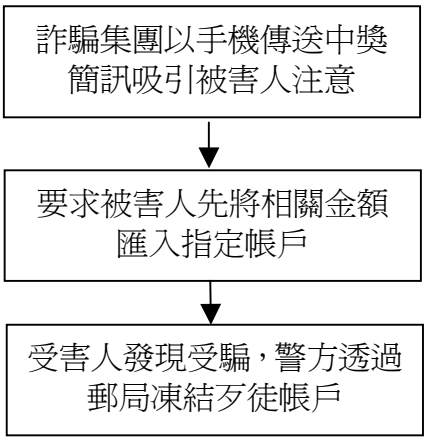
(2) **犯罪地點：**台東縣

(3) **犯罪事實：**台東縣關山警分局接獲線報，指稱二十三歲陳姓女子正辦理恢復使用一個已遭鎖定的詐騙帳戶。員警帶回陳姓女子及其男友，查閱存簿資料後才發現，該帳戶在月初短短三天內共有三十一人匯入一百零七萬，這些匯款者中已有人發覺被騙報警處理。

(4) **犯罪者剖析：**警方調查，陳姓女子的郵局帳戶，因九月初被台中市民報案指稱爲詐騙集團帳戶，台中警方行文郵政總局鎖定帳戶存款。詐騙集團渾然不知，持續在本月五至七日持續以手機簡訊詐財，三天內共有三十一人匯入金額三到九萬元的詐騙金、總額約一百零七萬元。因一百零七萬元詐騙金遭郵局鎖定、無法領取，陳姓女子昨日上午返回原開戶的關山郵局欲解除限制，被警方聞訊查獲。陳女到案後否認提供郵局帳戶遭詐騙集團使用，辯稱存簿及提款卡六月份便遺失，根本不知道已被詐騙集團使用。但存簿相關文件，遺失三個月後才報失，遺失期間內存簿持續有大批金額流通，而陳女及其男友手邊各有五支行動電話，警方根據這些疑點，懷疑他們是近來盛行的手機簡訊詐騙集團。

(5) **犯罪損害：**歹徒的帳戶共有三十一位受害者匯入一百零七萬的匯款。

(6) 犯罪方式：參閱圖六所示。



圖六：案例 4 的犯罪方式流程

綜合這些簡訊的犯罪案例，可以得到以下幾項結論：

- 歹徒以假身份申請行動電話門號，再傳送誘騙被害人上當之簡訊。
- 歹徒會要求被害人以轉帳方式或查詢帳號方式匯出存款。
- 當被害人查覺有異常時，歹徒已迅速將匯入或轉進的款項盜領一空。
- 一再出現的行動電話簡訊犯罪詐財行爲，破案不易，讓歹徒可以逍遙法外。

三、偵查行動電話簡訊犯罪的資料來源

剖析行動電話簡訊犯罪行爲，可以歸納出行動電話簡訊犯罪資料的來源，包括歹徒發送的簡訊資料、歹徒留下的聯絡電話號碼及歹徒要求匯款或轉帳的帳戶等資料。

1. 行動電話發送簡訊的資料

歹徒發送誘騙被害人上當的簡訊一般可以採取兩種方式進行：(1) 以行動電話直接將不實簡訊傳送給被害人；(2) 透過網路電信業者將不實簡訊傳送給被害人。利用行動電話發送簡訊較爲麻煩，使用者必須以手機所提供的中文輸入法編寫中文簡訊，爲此有網路業者與電信業者合作成立的網路電信公司，可提供使用者直接在網站上鍵入簡訊內容或利用網站寫好的罐頭訊息，再輸入對方的行動電話號碼，簡訊就可以順利傳送到對方的手機。最近業者所提供的簡訊傳輸服務功能越來越強，透過業者所提供的網站，無論任何時間或地點都可以傳送簡訊，而且可以廣播的方式大量的傳送同一份簡訊。歹徒若利用此簡訊傳輸服務功能進行簡訊的詐財犯罪行爲，將造成社會治安的一大隱憂。

不過，無論歹徒利用何種方式發送簡訊，所進行的犯罪行爲都會留下一些足以協助犯罪偵查的資料。以下依據簡訊發送的方式，分成兩方面來探討犯罪資料蒐集：(1) 歹徒以行動電話直接傳送的簡訊，則此通簡訊勢必會留下通聯紀錄(Call Records)[8][16]，從行動電話的通聯紀錄可以查出歹徒所使用行動電話號碼、手機的廠牌、型號以及發話的區域等[4][17]，深入的分析所蒐集到通聯紀錄資料，更可探勘出許多協助犯罪偵查的資料[5][6]。(2) 歹徒透過網路電信業者傳送簡訊，則可以由網路電信業者取得歹徒申請簡訊傳輸服務所填寫的用戶相關資料，以及發送簡訊時所輸入的相關資料，甚至可以取得歹徒使用電腦上網的 IP address 及住所[1]。

2. 聯絡電話號碼的用戶資料

歹徒發送誘騙被害人上當的簡訊後，爲了取得被害人的信任，一般都會附上相關的聯絡電話號碼以供被害人進行查詢及確認，進而取得被害人的信任而消除其戒心，以便騙取不當的錢財。歹徒留下聯絡的電話號碼也是偵查行動電話簡訊犯罪的另一項重要資料來源，因爲一般用戶在申請安裝電話時，必須提供姓名、身份證號、裝機地址、帳寄地址、住宅/非住宅等用戶的相關資料，而電信公司依電話號碼更可以查出此設備的相關資料包括：申請日期、安裝日期、每個月的通話費用以及最近幾個月的通聯紀錄等重要資訊[5][6]。從歹徒留下供聯絡的電號碼還可推導出下面的重要資訊：

- 歹徒所提供的聯絡電話是否最近才完成申裝作業？
- 歹徒是否利用不實資料或人頭來進行聯絡電話的申裝作業？
- 歹徒發送簡訊後，是否會造成聯絡電話號碼的通話量大幅增加？
- 歹徒是否利用此電話與其他詐騙集團的成員聯絡？

3. 匯款或轉帳的帳戶資料

網際網路熱潮下的 E 世代，促使各種追求高效率與高品質的服務都必須與網際網路適當的結合，如此才能在網路熱潮下提昇其競爭力以延續其的生存空間，商業的各項行爲與活動一直都是追求高時效性與高利潤的先驅，因此，配合網際網路而改變的各種商業行爲與活動，更是積極且快速的被開發與推動。銀行匯款、轉帳及提款作業也都可以透過網路來進行交易，大幅的提昇了一般存取款民眾的方便性，網路帶來的便利性卻也成爲心存不軌歹徒的犯罪工具。銀行開放民營後，民眾的開戶作業更是方便，只要民眾準備身分證及印章，任何人在幾分鐘就可以順利開設一個新的銀行戶頭，有了銀行戶頭，歹徒便可進行簡訊詐財的犯罪行爲。歹徒爲了騙取被害人的錢財，一般都會主動提供銀行帳號供被害人將各種款項匯入或轉入此帳戶，而且歹徒會在極短的時間將得手的款項全部提領一空，或是透過一連串的轉帳方式，將騙得的款項轉到不易追查的帳戶下，當被害人發覺有異狀時，已無法追回匯出或轉出的款項。詐騙集團所開設的銀行帳戶很可能是利用人頭或假資料所申辦的，開設帳戶的相關資料對於犯罪偵查作業或許缺乏直接的協助，不過，對於防止詐騙集團再度危害社會卻有正面且直接的效用。

四、行動電話簡訊犯罪資料的探勘模式

歹徒進行簡訊犯罪所留下的資料是犯罪偵查作業的重要依據，這些犯罪資料若能完整、正確且快速的取得，將可大幅的提昇偵查作業執行效率[5]。爲此，本節將結合犯罪基本資料蒐集作業及進階資料的精鍊作業，提出一套行動電話簡訊犯罪資料探勘模式[9][10][15]。

1. 簡訊犯罪基本資料的蒐集作業

犯罪資料的取得是經過一層層的步驟搭配相關的功能所完成的，簡訊犯罪的基本資料蒐集作業結合了搜尋(Searching)、擷取(Retrieval)、解譯(Interpretation)及推導(Deduction)等四項功能(如圖七所示)，以下將說明這四項功能所屬的步驟與目的：

(1) 搜尋功能：犯罪資料蒐集作業的第一個步驟，主要目的是從犯罪行爲所留下的原始犯罪資料進行追查，以便搜尋出該筆犯罪資料的起源處是來那家公司的那個單位。

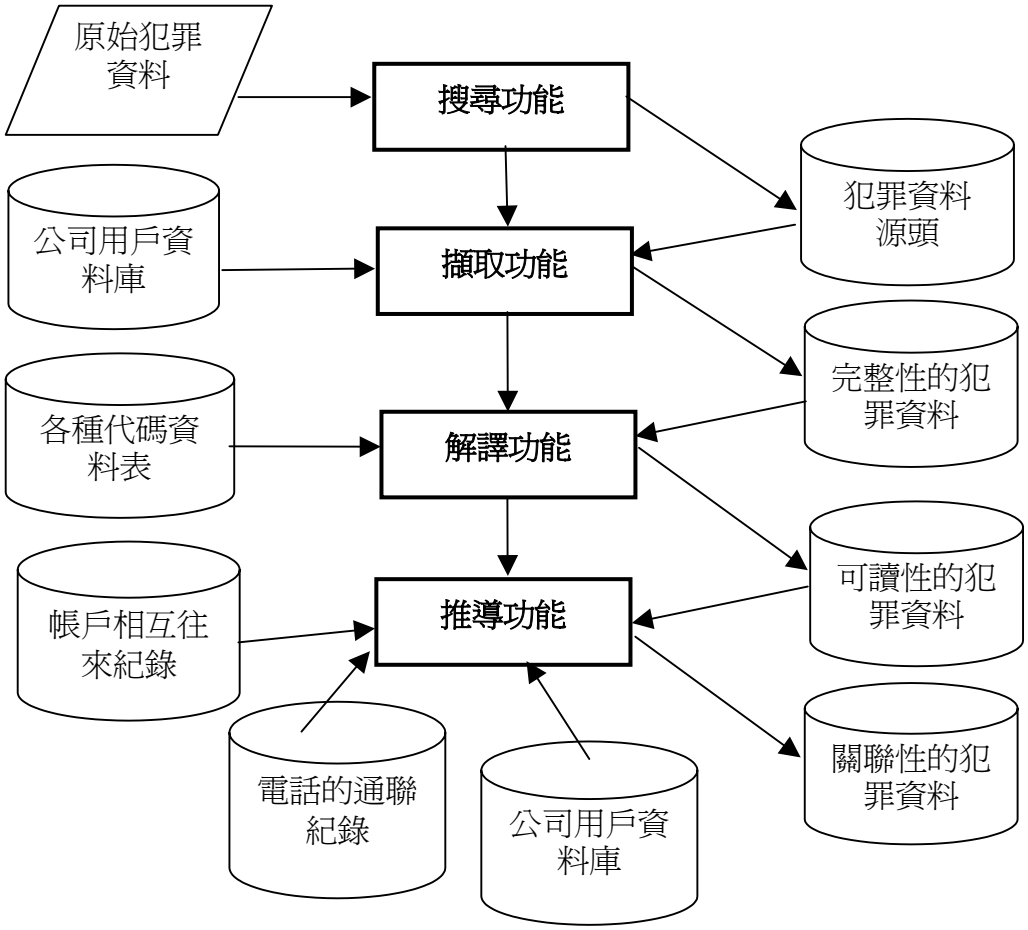
透過搜尋功能找出發話號碼、聯絡電話及銀行帳戶等資料的起源處：

- 不論歹徒傳送的簡訊是透過行動電話或是網路電信業者發送，可以從「發話號碼」的前面四個數字，配合電信公司的號碼字頭確認出所屬的行動電話公司[5][6]。
- 歹徒所留下的「聯絡電話」不論是行動電話或是固網電話，同樣可以透過電信公司的電話號碼字頭確認出所屬的則電信公司。
- 歹徒要求匯款或轉帳的「銀行帳戶」帳號，可以透過銀行與分行代號追查出該帳號是屬於那一家銀行及那個分行所有[4]。

(2) 擷取功能：犯罪資料蒐集作業的第二個步驟，利用搜尋功能追查出的犯罪資料的起源處後，便可以利用擷取功能從該單位的資料庫中，擷取出用戶的詳細資料以及與該用戶相互往來的資料[7][9]。

(3) 解譯功能：犯罪資料蒐集作業的第三個步驟，利用擷取功能所取得的大量資料中，有部份資料項目是以代碼的方式存放，這些代碼將不利犯罪偵查作業的進行，運用解釋功能可以將隱含在資料中的代碼轉成有意義且易於瞭解的訊息。例如，通聯紀錄的 IMEI 代碼可以解釋成發話的手機廠牌及型號[17]。

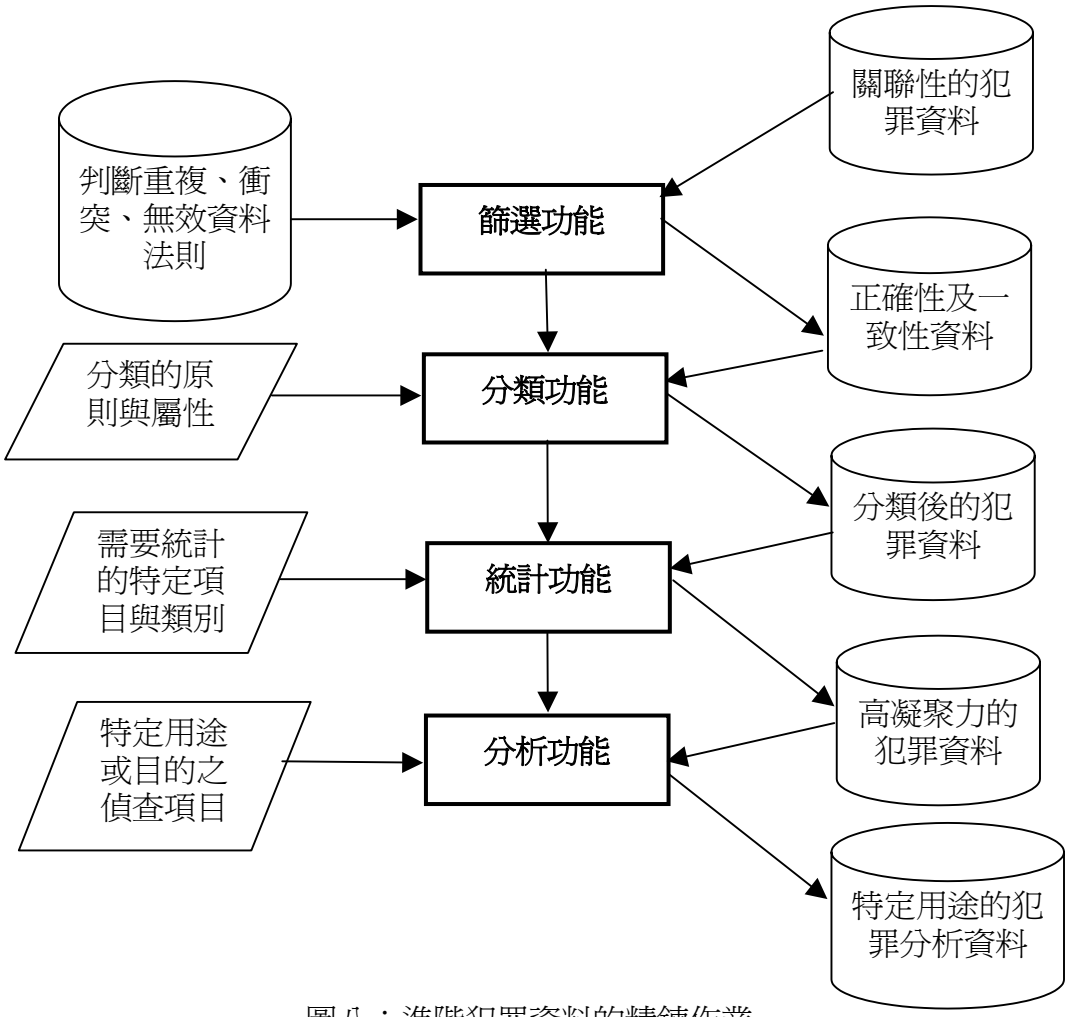
(4) 推導功能：犯罪資料蒐集作業的第四個步驟，經過搜尋、擷取及解譯等功能的運作，大部份與簡訊犯罪有關的直接資料都已被蒐集完成，不過，還有許多間接的犯罪資料必須透過推導過程才能取得，推導功能的目的就是將一些與犯罪主體資料有相互引用關係的間接資料透過推導的方式一一取得。



圖七：基本犯罪資料的蒐集作業

2. 簡訊犯罪進階資料的精鍊作業

經過四個步驟的犯罪基本資料蒐集作業，涵蓋直接與間接的大量犯罪資料都已被徹底的蒐集完成，蒐集到的龐大犯罪資料中，事實上，並非所有資料都具有協助犯罪偵查的效用。爲此，這些龐大的犯罪資料必須經過適當的精鍊作業，以便將重複出現的、互相矛盾的、與犯罪無關的等不適用的犯罪資料有效刪減或剔除，進而提昇後續作業的效率與品質。簡訊犯罪進階資料的精鍊作業是由篩選(Selection)、分類(Classification)、統計(Static)與分析(Analysis)等四項功能結合而成(如圖八所示)，以下將針對這四項功能的步驟與目的分別說明之：



圖八：進階犯罪資料的精鍊作業

(1) 篩選功能：犯罪資料精鍊作業的第一個步驟，主要目的是將蒐集作業所取得的大量資料進行適當且有效的過濾及刪減，因爲經過蒐集作業所取得的大量資料，並非都具有高度偵查的價值，對於重複、相互衝突、相互矛盾及缺乏偵查價值等資料，必須進行適切的刪減或剔除，以有效提昇犯罪偵查作業的效率與成果。

(2) 分類功能：犯罪資料精鍊作業的第二個步驟，經過篩選過後的資料已經具備了高度的正確性與一致性，但是仍舊缺乏具體的結構性與組織性，分類功能的主要目的就是將資料依據不同的屬性進行層次分明的劃分，以大幅提昇資料的凝聚力，對於後續處理及偵查作業更能夠快速且有效的取得所要引用的資料[12][13[15]。

(3) 統計功能：犯罪資料精鍊作業的第三個步驟，主要目的是將分類過後的資料依據事

先劃分好的特定項目與類別進行統計的作業，經過統計彙集處理後的資料更具整合效益，對於特定資料項目與類別將有助於偵查作業的進行[11][15]。

(4) 分析功能：犯罪資料精鍊作業的第四個步驟，主要目的是依據統計後的相關資料且配合特定目的或用途的偵查作業進行有系統的分析[14][15]。例如，(1)歹徒發送不實簡訊後，聯絡電話的通話量是否也隨之大幅增加？ (2) 歹徒發送不實簡訊後，歹徒設立的銀行帳戶交易次數是否也隨之大幅增加？

3. 整合蒐集與精鍊作業的犯罪資料探勘模式

歹徒透過行動電話簡訊所進行的詐騙行爲，將留下幾項具有偵查價值的原始犯罪資料，犯罪基本資料的蒐集作業利用搜尋、擷取、解譯及推導等四項功能，可以從幾項原始犯罪資料中取得具高完整性、高可讀性與高關聯性的大量犯罪資料。這些大量的資料中，有些是重複出現的，有些是互相矛盾的，有些與犯罪無關的，必須加以刪減或剔除，否則將造成資料缺乏一致性、正確性與凝聚力，不僅對犯罪偵查作業的幫助有限，反而會妨礙偵查作業的運作而降低偵查的效率與品質，爲此，必須對蒐集作業所取得的大量犯罪資料進行進一步的萃取及整合。犯罪進階資料的精鍊作業是透過篩選、分類、統計與分析等四項功能，精簡了資料的數量且提昇資料的效用，使資料具備一致性、正確性、有效性及高度凝聚力。行動電話簡訊犯罪資料探勘模式就是結合犯罪基本資料的蒐集作業與進階資料的精鍊作業，同時融合兩階段作業的八項功能，如圖 8 所示。此犯罪資料探勘模式發揮這八項功能以達成下面六項特質：

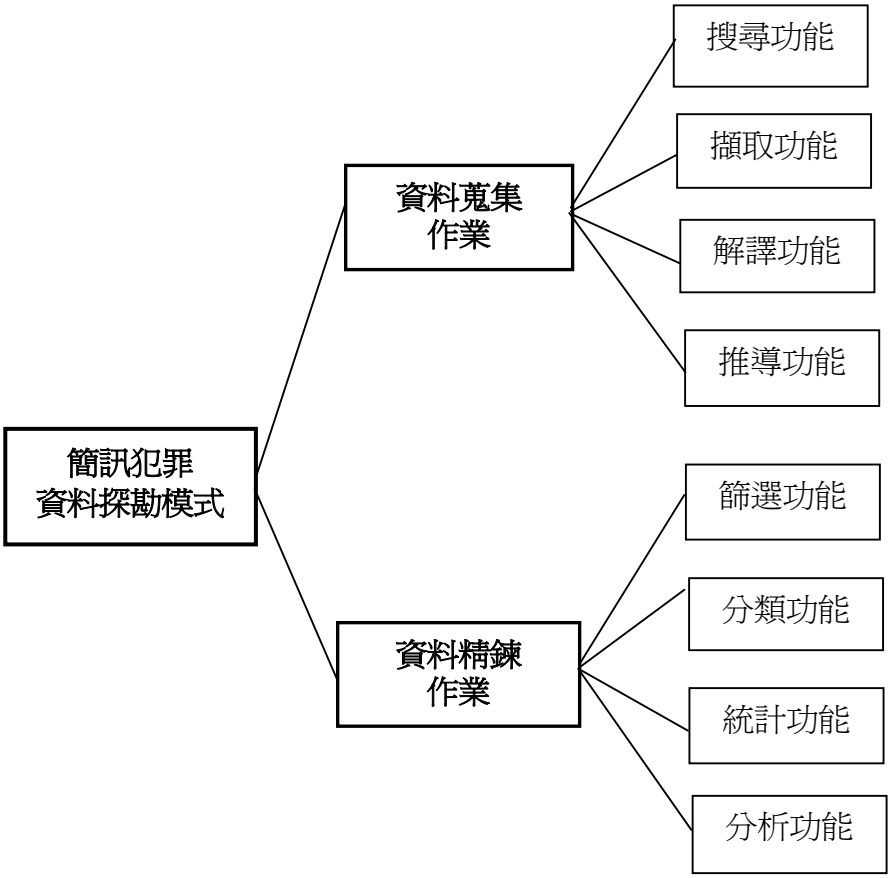
(1) 以循序性的方式一層層的取得各層級的犯罪資料以達資料的完整性。
(2) 利用解譯功能將資料中不易瞭解的代碼轉成有意義的資料以達資料的可讀性。
(3) 透過推導功能可以快速的建立且取得與其他資料間的關係以達資料的關聯性。
(4) 利用篩選功能可以刪減或剔除重複、矛盾及無關的資料以達資料的一致性與正確性。
(5) 利用分類及統計功能可以對資料進行有系統整編與彙集以建立資料的凝聚力。
(6) 依據偵查的需要與用途對犯罪資料進行有系統的分析以達資料的有效性。

五、行動電話簡訊犯罪的防範措施

歹徒進行有計畫的簡訊犯罪，勢必會想盡各種辦法掩飾犯罪行爲所留下的犯罪資料與證據。事實上，歹徒掩飾犯罪行爲的動作，大部份是可以事先加以預防的。爲此，本節將從掩飾犯罪行爲與犯罪偵查的角度進行探討，且提供一套簡訊犯罪的防範措施以有效遏止簡訊犯罪的行爲。

1. 行動電話門號的申請作業

歹徒透過行動電話發送簡訊，以行詐騙錢財的犯罪行爲之前，必須先取得行動電話的門號做爲犯罪的工具。不過，無論歹徒透過何種方式發送簡訊，終究可以透過一些偵查管道查出發送簡訊的行動電話門號。因此，歹徒一般都會先蹧漏洞，以不正當的方式取得行動電話的門號以掩飾其身份，如此，當偵查作業好不容易從數量龐大的通聯紀錄中查出發送簡訊的門號，再由門號追查出行動電話的用戶資料後，才赫然發現用戶的申請資料是假的，或是用戶也是被歹徒冒用的受害者。這樣的結果不僅將延誤犯罪的偵查



圖九：結合八項功能的簡訊犯罪資料探勘模式架構

作業，更使得歹徒能夠逍遙法外且繼續爲害社會。爲了避免歹徒以不正當的方式取得可以掩飾其身份的行動電話門號，電信業者對於行動電話門號的申請作業就必須規劃一套較嚴謹的防範措施：

(1) 用戶身份的確認：行動電話開放民營後，業者間推出各種新的促銷方案與優惠措施相互競爭，爲了就是拉攏新的客戶，新門號的申請作業也因此大幅的簡化。簡化後的門號申請作業成爲用戶身份確認的一大隱憂，用戶透過影印的身份證就可以輕鬆取得手機門號，從好的方面看，業者爭取到一位可以增加公司利潤的新客戶，從壞的方面看，業者可能要冒著無法收回大筆通話費用的呆帳風險，更遭的是，門號可能成爲歹徒用來詐騙錢財的犯罪工具。因此，爲了避免手機門號成爲歹徒犯罪的工具，同時也爲了減少業者無法收回通話費用的呆帳風險，應該建立一套較嚴格的用戶身份確認措施，例如以正本身份證或由本人親自到服務櫃檯申辦，以降低歹徒以不正當的方式取得可以掩飾其身份的手機門號。

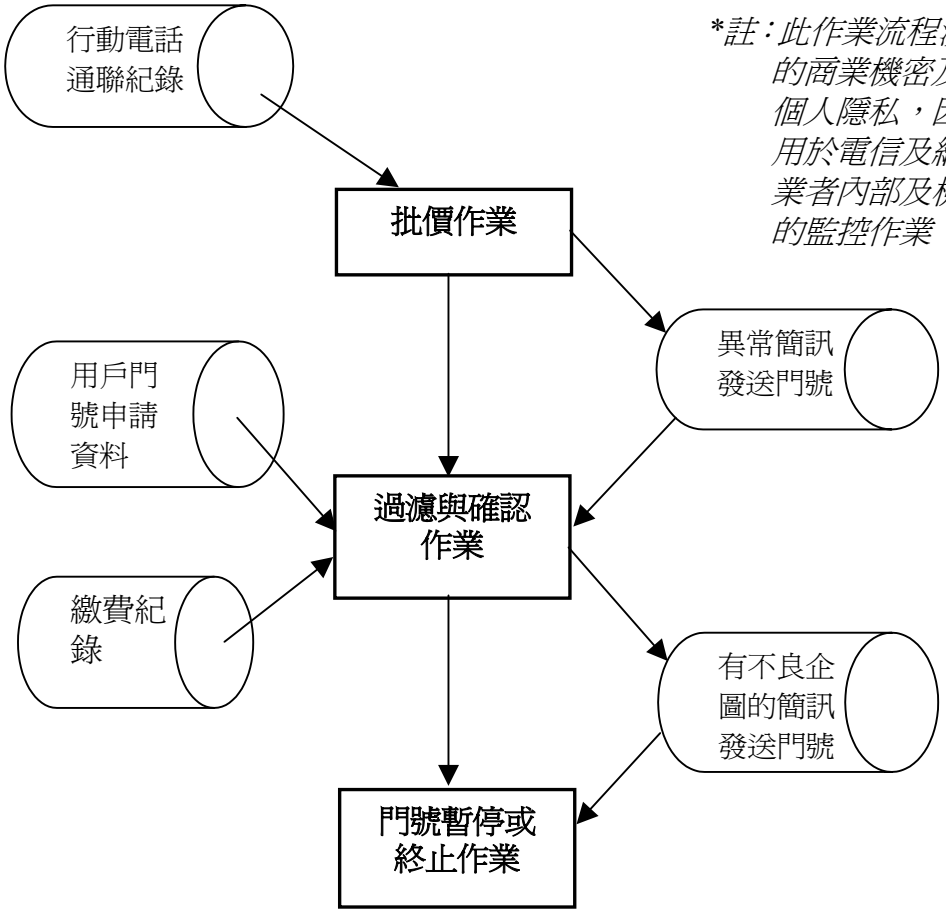
(2) 事後確認或查證：電信公司打著快速的申裝作業來吸引客戶，號稱在接受門號申請後極短時間內即可通話，使得門號申請後的查證幾乎被省略，也間接造成

歹徒有可乘之機。爲了避免此漏洞產生，對於非親自辦理門號申請或身份未經確認的客戶，應該對其資料進行深一層的確認與查證作業，經查證無誤後才可對該門號提供通話的服務。

(3) 處罰或終止代理商合約：行動電信業者爲了方便客戶的門號申請作業，將門號的申請手續交給手機經銷商代理收件，手機經銷商素質良莠不齊，對於客戶身份證明文件的辨識能力值得商榷，業者對於手機經銷商的門號申請代理權應該有所規範，一旦經銷商所代理的申請案件發現是因假的證明文件，而造成業者的呆帳損失或成爲歹徒的犯罪工具，就應該對該經銷商有所處分甚至終止其代理權，以促使經銷商加強客戶身份證明文件的辨識能力，進而減少不當的門號申請案件。

2. 簡訊資料傳送的監控作業

歹徒以不正當的手段取得行動電話門號，且以這些門號當作犯罪的工具，大量發送各種誘騙被害人上當的簡訊，大量犯罪簡訊的發送費用，將造成行動電話業者或是網路服務業者一大損失，高額的簡訊發送費用勢必成爲難以彌補的呆帳。業者爲了避免高額簡訊發送費用的損失，應該可以從簡訊發送的數量來監控發送簡訊的門號，在歹徒的犯罪行爲未完全得逞之前，就終止其犯罪工具的使用，不僅可以大幅減少簡訊犯罪受害者的人數，且可以嚇阻簡訊犯罪行爲的發生。爲此，電信及網路服務業者從簡訊資料傳送的監控作業流程(如圖十所示)，可以規劃一些具體的防範措施：



註：此作業流程涉及業者的商業機密及用戶的個人隱私，因此只適用於電信及網路服務業者內部及檢調單位的監控作業。

圖十：簡訊資料傳送的監控作業流程圖

(1) 蒐集異常傳送簡訊門號：從簡訊犯罪行爲的相關案例研判，歹徒發送簡訊誘騙被害人上當的方式，一般都是在同一時間大量發送的，電信業者或是網路服務業者在進行通信費用批價作業時，可以同時統計出手機門號的簡訊發送量，若手機門號在某一段特定時間有大量的簡訊發送行爲，就應該將其視爲異常傳送簡訊門號，透過此防範措施所蒐集到異常傳送簡訊門號可以過濾出有犯罪傾向的手機門號，進而降低簡訊犯罪的比率。

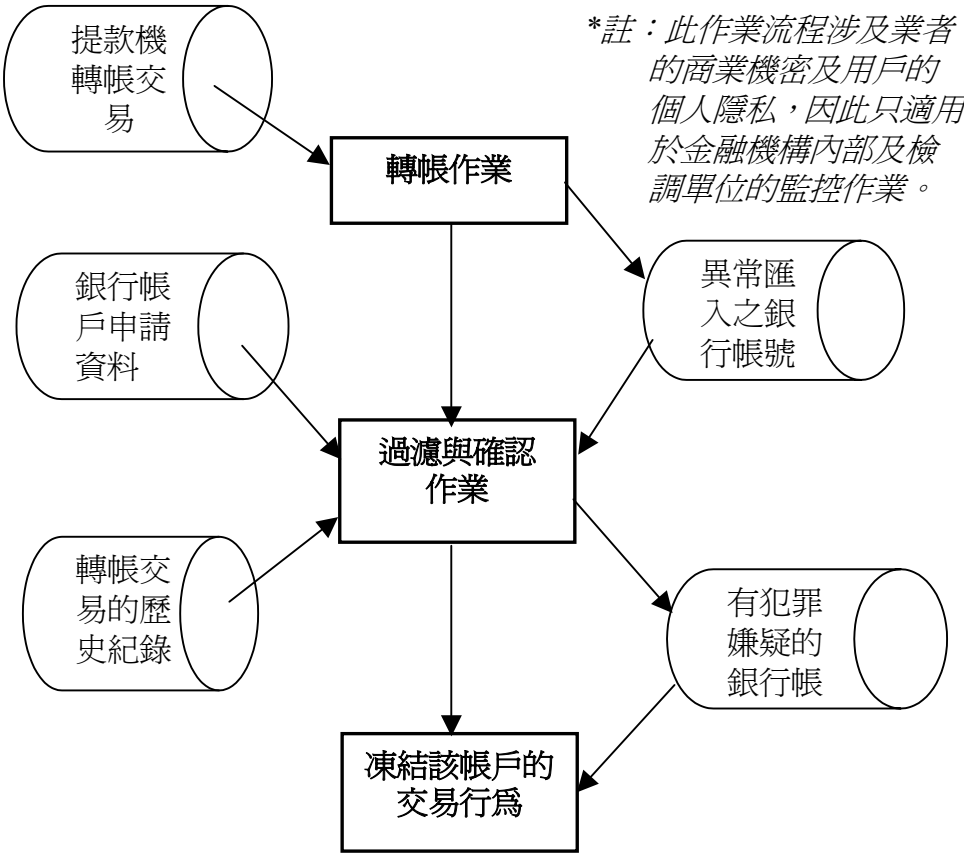
(2) 過濾且確認有疑慮的門號：蒐集到異常傳送簡訊的門號中，大部份是屬於正常管道申裝的合法門號且無犯罪傾向，例如發送大量簡訊可能是某個團體組織透過簡訊傳送的方式，將訊息通知所有成員，也有可能是某家服務業者透過簡訊傳送的方式，將新的優惠措施或促銷方案等告知客戶等等。不過，從過去的通聯紀錄、繳費資料及客戶的申裝日期，很快就可以將這些合法的門號用戶從異常的門號中排除，剩餘的門號就成爲值得進一步確認的有疑慮門號，再透過簡訊傳送的訊息內容來進行分析與判斷，應該可以找出具高度犯罪傾向的手機門號。

(3) 暫停或立即終止該門號的使用：爲了避免有犯罪傾向的手機門號成爲歹徒的犯罪工具，危害社會治安、破壞社會秩序，對於經過蒐集、分析與確認作業所篩選出具犯罪傾向的手機門號，應該規劃一套迅速的因應策略，暫停或立即終止該門號的使用是行動電信業者可以使用的最有效方式，同時也須積極配合檢調單位進一步的調查與確認工作，此防範措施粉碎了歹徒以手機門號當作犯罪工具的企圖，進而降低或減少簡訊犯罪受害者的損失。

3. 銀行帳戶及匯款的監控作業

歹徒透過行動電話簡訊進行的詐騙行爲，有許不同引誘受害者上當的花樣，不過，最終的目的只有一個，就是騙取受害者銀行存摺內的存款。因此，歹徒騙取錢財的手段，幾乎都是要求被害人透過提款機將存款匯入指定帳戶，或是誘騙不熟悉提款機操作方式的受害者，在不知情的情形下，將存摺內的大筆存款匯入歹徒的帳戶。當受害者發覺情況不對，進一步查看存摺的存款時，爲時已晚，大部份的存款已經在不知情的情形下匯出，且轉入歹徒預設的帳戶。此外，計畫周全的簡訊犯罪行爲，歹徒還會經過好幾次的轉帳作業，將騙得的錢財轉入難以追查的帳戶中，再從容的將存款提領一空。爲了避免銀行的帳戶及提款機成爲歹徒簡訊犯罪的工具，金融機構應該從銀行的開戶、匯款過程的監控及可疑帳戶的凍結等作業流程(如圖十一所示)規劃出相關的防範措施，以減少或是杜絕簡訊犯罪的行爲所造成的傷害。

(1) 銀行帳戶的開戶作業：計畫周全的簡訊犯罪行爲，歹徒會事先規劃以銀行帳戶作爲受害者匯入存款的帳號，因此，歹徒勢必以不正當的方式開設或取得銀行帳戶，以便能夠掩飾其真正的身份。當受害者提出檢舉時，追查出的帳戶申請資料，不是利用假資料申辦的，就是冒用人頭所開設的戶頭，使偵查作業無法繼續往下偵辦。爲了避免銀行帳戶成爲歹徒犯罪的工具，銀行的開戶作業應該建立一套較嚴格的客戶身份確認措施，例如辨識身份證的真僞、填寫的資料是否完整且正確、是否有冒用人頭的傾向等等，以降低歹徒以不正當的方式取得可以掩飾其身份的銀行戶頭。



圖十一：銀行帳戶及匯款的監控作業流程

(2) 監控來自提款機所匯入的帳戶：從一些簡訊犯罪的案例研判，歹徒一般採取大量發送簡訊的方式來誘騙被害人上當，因此，同一時間收到簡訊而受騙上當的被害人應該超過幾十人甚至上百人，這些被害人會在相去不久的時段內將存款匯入歹徒指定的帳戶中。銀行透過轉帳交易監控作業可以將特定時段所蒐集到提款機匯款交易進行統計，將交易筆數過多的帳戶列爲異常匯款交易帳戶，交由後續的作業進行進一步的查證。

(3) 凍結可疑帳戶的提領或匯出作業：透過帳戶過去轉帳交易的歷史紀錄與該帳戶的申請時間，可以協助判斷異常匯款交易帳戶是否爲可疑的帳戶，若發現爲可疑的帳戶可以先凍結該帳戶提領與匯出的交易，再迅速請求相關單位協助調查與確認。此防範工作應該可以減少簡訊犯罪受害民眾的損失。

六、結論

行動電話除了具備高度的機動性外，普及率更高達 96.6% 居世界第二，業者爲了贏得商機更不斷的推出新的服務功能，手機簡訊就是 E 世代無線通訊中很受歡迎的訊息傳送方式。因爲廣泛被使用，也因此成爲歹徒用來行騙詐財的犯罪工具，依據最近的簡訊犯罪資料顯示，利用行動電話簡訊進行犯罪行爲有愈來愈多的趨勢，固然受害民眾都是在心存貪念下，才會成爲詐騙集團鎖定的對象，不過，我們卻不能容許這種犯罪行爲繼續爲害社會治安，如何有效嚇阻甚至打擊行動電話簡訊犯罪以維護社會秩序是刻不容

緩的工作。本文針對行動電話簡訊犯罪的行爲進行深入的剖析，以瞭解其犯罪的流程與步驟，且以立意抽樣方式，將最近發生的簡訊詐財案中，較具代表性且引起輿論注意的案例，以框架表示式來分析簡訊犯罪的行爲，進而協助建立行動電話簡訊犯罪的防範措施。剖析行動電話簡訊的犯罪行爲，可以從下面三個簡訊犯罪的關鍵步驟中取得重要的原始犯罪資料：

(1) 歹徒透過行動電話或網路電信公司傳送簡訊的過程中，所留下的「發話號碼」。
(2) 歹徒爲了取得被害人的信任，所留下的查詢或確認之「聯絡電話」。
(3) 歹徒爲了騙取被害人的錢財，要求被害人匯款或轉帳的「銀行帳號」。

針對簡訊犯罪過程中所留下的犯罪資料，本文整合搜尋、擷取、解譯、推導、篩選、分類、統計與分析等功能，提出一套行動電話簡訊犯罪資料探勘模式，此模式可以產生具完整性、正確性、一致性、有效性及高凝聚力的犯罪偵查資訊，以具體提昇行動電話簡訊犯罪偵查作業的效率與品質[4]。對於計畫周全的犯罪集團，早已預先掩飾可能留下的犯罪資料，使得大費周章所萃取出的犯罪資訊，無法派上用場。爲此，本文從犯罪行爲的掩飾及犯罪偵查的角度進行探討，彙集三方面的簡訊犯罪防範方式包括:行動電話門號的申請作業、簡訊資料傳送的監控作業及銀行帳戶匯款的監控作業，建立一套簡訊犯罪的防範措施，在歹徒的犯罪行爲未得逞前，立即終結其犯行，以有效嚇阻簡訊的犯罪行爲。

參考文獻

[1] 林宜隆，網際網路與犯罪問題之研究，中央警察大學出版社，2000 年。

[2] 賴森堂、林宜隆，“簡訊犯罪型態與防範措施之研究”， *2002 年第四屆資訊管理學術暨警政資訊實務研討會論文集*，2002：頁 472 -482。

[3] 賴森堂，“電子商務軟體品質量測模式”，*企業管理學報*，第 53 期，國立臺北大學企業管理學系，2002：頁 53-72。

[4] 賴森堂、林宜隆，“簡訊犯罪資料探勘模式之研究”， *2002 年第六屆資訊管理學術暨警政資訊實務研討會論文集*，桃園，中央警察大學，2002：頁 303-312。

[5] 賴森堂、林宜隆，“行動電話犯罪偵查資料探勘與量測模式”，*中央警察大學『資訊、科技與社會』學報*，第1卷第1期，2001：頁59-74。

[6] 賴森堂、林宜隆，“行動電話犯罪偵查資料蒐集模式之研究”，*第五屆資訊管理學術暨警政資訊實務研討會論文集*，2001：頁 203~210。

[7] 賴森堂，“提昇電信服務品質之法則式查核系統”，*實踐大學第三屆學術及實務研討會論文集*，2001：頁 III-B1-1~ III-B1-11。

[8] 賴森堂、林宜隆，“反綁票案偵防作業之研究—以行動電話爲例”，*第二屆網際空間：資訊法律與社會研討會論文集*，2000：頁 87~96。

[9] Chen, M.-S., Jan., J. and Yu., P.S., “Data mining: An overviewing from a database perspective”, IEEE Trans. Knowledge and data Engineering (8:6), 1996: pp.866-883.

[10] Han, J. and Kamber, M., *Data Mining: Concepts and Techniques,* Morgan Kaufmann Publishers, 2001.

[11] Hand, D.J., Blunt, G., Kelly, M.G. and Adama, N.M., “Data Mining for fun and profit”, Statistical Science, (15:2), 2000: pp. 111-118.

[12] Hartigan, J.A., *Clustering algorithm*, John Wiley, New York, 1975.

[13] Liu, B., Hsu, W. and Ma, Y., “Integrating classification and association rule mining”, *Proceedings of the Int. Conf. Knowledge Discovery and Data Mining (KDD’98)*, 1998: pp.80-60.

[14] Quinlan, J.R. “Induction of decision trees,” Machine Learning, (1), 1986: pp.81-106,.

[15] Westphal, C. and Blaxton, T., “Data Nining Soluations – Methods and Tools for Solving Real-World Problems”, John Wiley & Sons, Inc., 1998.
[16] Digital cellular telecommunications system (Phase 2); Event and call data (GSM 12.05 version 4.3.0), European Telecommunications Standards Institute 1997.
[17] IMEI Allocation and Approval Guidelines, GSM MoU Association Permanent Reference Document: TW.06, 1998.