專 題 企 劃

談破解非接觸式電子支付工具犯罪及案例研析

台北地檢署檢察官 林禎瑩

◆ 目次 ◆

關鍵詞

電子支付工具、RFID、悠遊卡

壹、前言

科技的進步為人類的生活帶來莫大的變化，而人類經濟活動所必需的交易媒介貨幣，從遠古時代具有天然崇拜性質的貝殼，到以金銀、金屬鑄造貨幣，以至因應大規模經濟而有紙幣之出現。至拜現代科技發達之賜，則演變出電子貨幣之產生，英文為Electronic money，參考歐盟（EU）、國際清算銀行（Bank fro International Settlements）、歐洲中央銀行（European Central Bank）之定義，乃指具備以電子化的方式儲存貨幣所代表的票面價值，而有晶片或微晶片的卡片或個人電腦為載具，以便儲值，且有預付的性質等特色[1]。本文所欲討論的，即是將電子貨幣以具有微晶片（microprocessor chip）即IC晶片之非接觸式載體為表彰之支付工具，在我國目前即為一般社會大眾日常生活不可或缺之悠遊卡及一卡通，另在國外則有英國倫敦牡蠣卡（Oyster Card） 、香港的「八達通」等，均和悠遊卡同樣係從交通卡發展而成為電子支付工具。日本則是於西元2001年，由Bi twalet公司於首先推出「Edy」電子支付工具的服務（現為「樂天Edy」卡），同年JR東日本也將此一概念應用到電子車票上，開始推出「Suica」卡，2005年JR西日本亦跟進推出「ICOCA」。2007年3月，日本電子貨幣的公司相互合作，結合不同領域的電子貨幣服務讓消費者使用， 提供私鐵、公車與便利商店間都能使用的電子貨幣服務，市面上並有首都圈私有鐵路聯盟的「PASOM」、日本7-11所發行的「nanaco」、EAON集團發行之「WAON」卡等[2]，此外尚有「manaca」、「PiTaPa」等總計不下數十種卡片[3]，在日本超商櫃檯結帳時，可見到讀卡機上標示可接受之前述各種電子支付工具的圖示，其多樣化讓人驚訝，稱之為電子貨幣的戰爭亦不為過。前述非接觸式電子支付工具，在日本通稱為「電子マネー」，應係以英文Electronic money直譯而來。

非接觸式電子支付工具，交易處理速度快、可靠度高、維修成本低，故特別適用於大眾運輸系統作為付費工具，另作為小額消費之購物使用，亦可不需攜帶現金在身上也能購物，在超市及便利商店結帳時，也省去找零的麻煩，提供了民眾便利之生活環境。惟現代科技如同刀刃之兩面，在帶來便利之同時，卻往往也成為有心犯罪者的

1 李宜儒，非銀行從事電子票證業務相關法律問題之研究，逢甲大學財經法律研究所碩士論文，2011年，頁10-14。

2 林書辰，日本電子貨幣市場戰略分析-以樂天Edy與Suica為例，淡江大學亞洲研究所碩士論文，2014年，頁20-21。

3 「電子マネー比較.com」網站，提供各種電子マネー之介紹與比較之說明。網址：http://kuchikomi0.com/，最後瀏覽日：2015年3月30日。

標的，新興犯罪因此而來。本文將先以非接觸式電子支付工具之技術與安全機制為介紹，並聚焦於實務案例之分析，期許能以科技結合法律之方式探究研析。

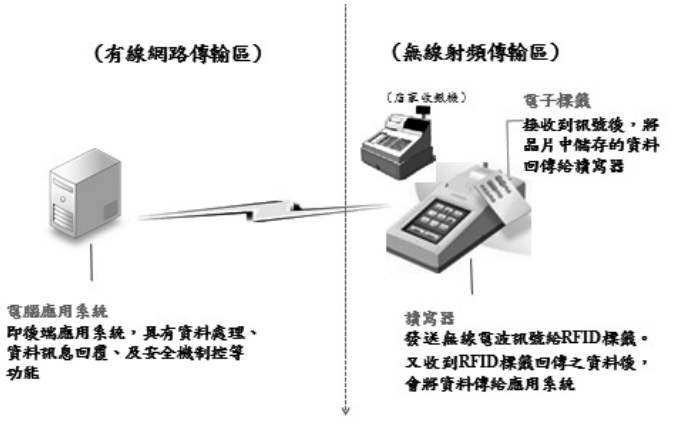
貳、非接觸式電子支付工具之技術與安全機制

一、技術背景

非接觸式電子支付工具，利用具有記憶、運算、統計以及資料處理之IC晶片，紀錄並運算電子貨幣餘額之電磁紀錄，而其技術架構，則是採用RFID（Radio Frequency Identification）之技術，中文稱為「無線射頻識別系統」，此技術被譽為本世紀最重要的前十大技術之一[4]。RFID早已存在一般人日常生活中，除本文探討之主題悠遊卡外，高速公路之ETC、信用卡之VISA WAVE，寵物身上植入之「寵物晶片」、商店或圖書館內的防盜晶片、門禁管制晶片卡等，這些都是RFID之實際應用。

RFID之技術，是一種通信技術，可透過無線電訊號識別特定目標並讀寫相關數據，而無需在識別系統與特定目標之間建立機械或光學接觸。RFID運作的原理，是透過無線通訊技術將電子標籤（Tag）內晶片中的數位資料，以非接觸的通訊方式傳送到讀寫器（RFID Reader/Writer）中，讀寫器再將擷取、辨識的電子標籤資料傳送給後端電腦應用系統，以便進一步處理、使用或加值運用這些資料。所以它的系統架構包含電子標籤（RFID tag）、讀寫器（RFID Reader/Writer）及電腦應用系統三大部分。

讀寫器（RFID Reader/Writer）與電腦應用系統即後端資料庫的傳輸，通常是架構在採用RFID之系統之企業內部的有線環境，為有線網路傳輸區，可以透過SSL等相關加密技術保護；而電子標籤（RFID tag）與讀寫器（RFID Reader/Writer）間之前端無線射頻傳輸區則為不安全之無線通道區域。RFID系統運作過程如下：



RFID系統架構圖（資料來源：作者製作。）

4 陳啟煌，RFID原理與應用，國立台灣大學計算機及資訊網路中心電子報，第0002期，2007年9月。網址：http://www.cc.ntu.edu.tw/chinese/epaper/0002/20070920_2005.htm ，最後瀏覽日：2015年12月30日。

是非接觸式電子支付工具，在RFID之技術架構下，以悠遊卡為例，悠遊卡為以電子形式儲存儲值餘額，並含有資料儲存及計算功能晶片之智慧卡[5]，因此，悠遊卡即為RFID的電子標籤[6]。

二、安全機制

非接觸式電子支付工具之交易安全機制，即是建構在RFID系統安全機制之下，因此區分為無線射頻傳輸區與有線網路傳輸區兩部份之安全機制為說明。

㈠ 無線網路傳輸區之安全機制：

無線射頻傳輸區之安全機制，則與RFID的晶片供應廠商及技術有關，目前主要的供應廠商及技術有二種，即荷蘭飛利浦Philips（現為NXP 恩智浦半導體公司）之Mifare，和日本SONY的Felica技術。我國之悠遊卡、一卡通及英國倫敦牡蠣卡（Oyster Card），均採用Mifare技術晶片。另採SONY所開發之的Felica技術，則有香港「八達通」卡，新加坡的「易通卡」，且在日本亦被廣泛使用，前述所提及之「Suica」、「ICOCA」、「樂天Edy」等，全部均採用Felica技術。SONY開發的Felica之所以會在日本普及，除SONY本身的品牌影響力外，還有Felica的處理速度。由於日本東京都與關西各大都市的車站均屬高流量之交通運輸系統，如果自動驗票機處理速度不夠快，將無法疏解人潮[7]。因此，採用Felica的非接觸式智慧卡，通行時間約0.1秒，與其他的非接觸式智慧卡比較，速度無出其右者[8]。

Mifare及Felica技術，在資料儲存結構、通訊流程、鑑別流程分別有其技術上之安全機制，任何讀寫器欲存取（讀寫）其晶片內容，均須先通過Mifare及Felica晶片內部處理機之認證[9]。Mifare使用稱為CRYPTO1的串流式密碼系統，Felica則沒有公開密鑰加密的規格。兩者之晶片供應廠商均宣稱晶片機制甚為安全，堅不可破。

惟自2008年以來，所公開發表之論文方法，包含：反向工程、密鑰串流還原攻擊法、側錄攻擊法等[10]。而世界各國與悠遊卡同採Mifare Classic晶片之英國倫敦的牡蠣

5 智慧卡具有微晶片(microprocessor chip)即IC晶片，因此又稱為IC卡(Integrated Circuit Card)、晶片卡(Chip Card)。IC晶片除有記憶的功能外，還有運算、統計以及資料處理的功能。參陳曉開譯，Catherine A. Allen & William J. Barr著，智慧e卡，2000年，頁263-274。轉引自吳乃瑋，台北悠遊卡服務品質、滿意度與忠誠度之研究，中華大學經營管理研究所碩士論文，頁7-8，2006年7月。

6 魯明德，電子票證的安全議題，網址：http://law.kcg.gov.tw/enactment/en8.pdf，最後瀏覽日：2015年12月30日。

7 參宋軒樓，智慧卡營運管理法律關係之研究，玄奘大學法律學系碩士論文，2010年，頁26。

8 RFID主要晶片供應商傳輸速度比較一覽表，參RFID 產業資料庫網站，網址：http://www.iservice.org.tw/db/know_content.php?id=158，

9 徐春進、史敦仁，捷運系統票證加密與通訊安全，捷運技術第38期，頁218，2008年2月。

10 李魁元，Mifare Classic模擬及安全性改良之研究，中國文化大學資訊管理系碩士論文，2012年，頁23-25。

卡、美國波士頓的查理卡等，也陸續自2009年以來傳出已遭學術單位破解之新聞，是悠遊卡之安全性在當時即因此曾受台北市議員之質疑[11]。

因此，吾人或許以為資料加密就安全了，其實安全是一個相對的概念，沒有無法破解的密碼，只有要用多少的資源去破解密碼，這資源包括時間、設備，而金鑰的長度關係著密碼被破解的時間。是任何安全的系統都有一天會被破解。任何人一旦取得金鑰，都可以針對目標卡片進行內部資料的修改。是資訊安全是長期工作，絲毫不能疏忽[12]。

有心者只要了解非接觸式電子支付工具，相關資料存於記憶體的位置後，接著再以寫入的指令，修改卡片的內容，將金額修改，如此便可竄改了儲存於電子支付工具內之儲值金額。此種攻擊手法之成功，也意謂RFID系統並沒有資料庫可供即時（Real-Time）驗證儲值金額[13]，攻擊者只要取得1張非接觸式電子支付工具，便可以在自己認為最隱密的地方進行破解，而遂行離線攻擊。此即本文所欲探討之破解，係針對本文上圖「RFID系統架構圖」紅色虛線右側、無線射頻傳輸區之安全機制部分，加以攻擊並破解其加密機制，而達成遂行竄改電子支付工具金額之電腦犯罪行為。

㈡有線網路傳輸區之安全機制：

有線網路傳輸區與一般網路類似，由RJ45纜線、集線器、路由器、光纖、網路交換機（Ethernet Layer3 Switch）、虛擬私人網路閘道器（VPN Gate way）、中繼伺服器、中央處理機、清算中繼伺服器（Clearance Middleware Server）及防火牆（Firewall）所構成[14]。有線網路傳輸區為讀寫器（RFID Reader/Writer）與電腦應用系統即後端資料庫間的傳輸，資料傳輸格式為每筆交易資料附加MAC（Message Authentiaction Code）後才傳送，MAC訊息確認碼讓後端電腦應用系統，驗證交易資料是否由該系統認可之讀寫器所傳出，以及在傳輸過程中是否已被竄改過，進而確保沒有假帳之虞[15]。

後端的資料安全性雖相對安全，惟後端資料庫既係電腦應用系統所組成，則亦有可成為電腦犯罪之標的，例如無故入侵、無故取得刪除或變更他人電腦之電磁紀錄或

11「悠遊卡遭破解？」，參聯合報新聞，2009年10月24日，網址：http://udndata.com/library/，最後瀏覽日：2015年3月30日。

12 魯明德，悠遊卡安全嗎？，網址：ttps://www.vhyl.gov.tw/code_upload/NewsInfo/file1_999_2605285..doc，最後瀏覽日：2015年12月30日。

13 參周立平、楊博宏， Mifare Classic的僅卡攻擊(Card-Only Attack)，第二十一屆資訊安全會議，2011年，頁125。

14 徐春進、史敦仁，捷運系統票證加密與通訊安全，捷運技術第38期，2008年2月，頁219。

15 註同上，頁219-220。

干擾系統等攻擊，均有可能發生。例如我國高速公路之收費系統ETC亦同為無線射頻識別系統RFID系統之實際應用，但近來曾發生3名國立大學之學生，在其等學校宿舍內，以電腦連接網際網路[16]，連線至遠通電收股份有限公司所架設之http://www.fetc.net.tw網頁並於網路討論系爭網頁可能存有之設計缺陷後，共同在系爭網頁網址後添加字串，以此方式利用電腦系統之漏洞，入侵遠通電收股份有限公司用以架設系爭網頁之電腦伺服器，取得遠通電收股份有限公司儲存於上開伺服器內檔案，而涉犯刑法第358條無故利用電腦系統漏洞入侵他人電腦罪嫌，嗣該3名大學生與遠通電收股份有限公司達成和解而獲檢察官不起訴處分[17]。此一案例即是屬於攻擊無線射頻識別系統RFID之後端電腦應用系統，亦即本文上圖「RFID系統架構圖」紅色虛線左側、有線射頻傳輸區之安全機制部分之情形。

參、實務案例研析

一、案例介紹

本文以我國之前所發生之某工程師破解悠遊卡、竄改悠遊卡金額之實務案例[18]為討論。

㈠ 犯罪事實

破解悠遊卡犯罪之實務案例為：被告係某科技股份有限公司資訊安全顧問，其曾研究悠遊卡之安全機制而知悉悠遊卡之傳輸技術為無線射頻識別系統原理（Radio Frequency Identification，縮寫為RFID），並於100年5月間，以美金399元之 代價，透過網際網路向設置於美國地區之proxmark3網站（網址為http://www.proxmark3.com）， 購買可作為RFID的側錄、讀取以及複製之proxmark3之設備1台，經閱讀國外有關破解悠遊卡加解密程式之論文後，利用電腦連接proxmark3之設備，並透過proxmark3之設備及自製之感應線圈接收及取得悠遊卡之密鑰串流，取得某一區段金鑰，再經過不斷重複嘗試鑑別蒐集足夠之密文，去取得其他的金鑰，又經比對悠遊卡加值後晶片記憶體之內容，查悉記憶體相關資料儲存之位置後，執行寫入的指令，而將悠遊卡晶片記憶體所記錄之儲值金額之電磁紀錄加以改變，竄改共計3張悠遊卡之電磁紀錄均為新臺幣（下同）9千元後，再分別持往便利商店使用消費取得商品。

16「入侵eTag官網　3男大生道歉」，參蘋果即時新聞，2014年8月26日，網址：http://www.appledaily.com.tw/realtimenews/article/new/20140826/458377/ ，最後瀏覽日：2015年3月30日。

17 臺灣士林地方法院檢察署103年度偵字第8790號不起訴處分書。

18 台灣士林地方法院101年度訴字第172號。

㈡ 法院判決

法院判決被告以不正方法變造悠遊卡，並持往超商查詢餘額，且成功消費取得商品，其後因其中一張悠遊卡交易失敗並致該悠遊卡鎖住，無法使用，惟該等悠遊卡中經變造之虛偽資料均已傳送至悠遊卡公司後臺電腦而製作財產權變更之紀錄，而此紀錄係製作其已預付將來消費對價予悠遊卡公司之財產權變更紀錄，自應成立刑法第339條之3第2 項之非法以電腦製作不實財產權變更紀錄得利罪。另被告所為，亦構成電子票證發行管理條例第30條第1項前段變造電子票證罪（此為判決時之條文規定，該條文嗣於民國104年6月刪除），及刑法第201條之1第1項變造支付工具罪。

行為人以科技之手法，破解悠遊卡儲值餘額電磁紀錄之加密方法，成功竄改悠遊卡儲值金額之電磁紀錄案例，犯罪手法部分以濫用電腦或違犯之具有電腦特質之犯罪行為[19]，為「電腦犯罪」；且行為人基於不法之意圖，以不正方法影響電腦資料處理的過程，藉此以取得財產利益的行為，屬於電腦犯罪中的電腦操縱形態之「電腦詐欺」[20]犯罪；又悠遊卡於98年1月13日立法院三讀通過「電子票證發行管理條例」，並經總統公告施行，賦予悠遊卡小額消費法源，為現今國人日常生活不可或缺的電子支付工具，具有財產價值，該儲值金額之電磁紀錄，為刑法上之準私文書，行為人擅自竄改變更，自會涉及刑法關於偽造、變造等罪章之刑責。是此案例涉及之範圍，包含電腦犯罪、電腦詐欺，及準私文書與電子支付工具偽造、變造等層面，以下分別敘述之。

二、準私文書、電子支付工具、電子票證等相關偽造、變造構成要件之檢討

㈠ 刑法偽造文書罪章構成要件之檢討

悠遊卡為非接觸式的智慧卡，亦是無線射頻識別RFID系統之電子標籤，悠遊卡內有記憶晶片與感應線圈，用以完成無線傳輸方式的交易。而記憶晶片裡儲存之相關資料，包含儲值金額等資料，均須透過讀寫器（Reader/Writer）等設備處理後，始得以顯現該記憶晶片內儲存之相關資料，核屬刑法第10條第6項之「電磁紀錄」。

又刑法第220條規定：「在紙上或物品上之文字、符號、圖畫、照像，依習慣或特約，足以表示其用意之證明者，關於本章及本章以外各罪，以文書論。」「錄音、錄影或電磁紀錄，藉機器或電腦之處理所顯示之聲音、影像或符號，足以表示其用意之證明者，亦同。」是依此條規定，凡顯示出聲音、影像或符號，依習慣或特約可作為

19 電腦犯罪之定義，參考林山田，論電腦犯罪，軍法專刊30卷8期， 1984年，頁2~8；林山田，電腦犯罪之研究，政大法學評論30期， 1984年，頁45~66。

20 電腦詐欺定義，參考林山田，評詐欺罪章中之新增三章，月旦法學雜誌49期，頁88，1999。黃榮堅，刑罰的極限，頁314，1999年。謝開平，電腦詐欺在比較刑法上之研究，國立台北大學法學系博士論文，頁33以下，2003。

一定用意之證明之錄音、錄影或電磁紀錄，均可作為準文書，而可作為刑法偽造文書罪之客體。悠遊卡內有記憶晶片所儲存之電磁紀錄，亦屬於刑法第220條之「準私文書」無訛。

又本案被告將悠遊卡內之記憶晶片所儲存之悠遊卡金額電磁紀錄之準文書，擅自竄改變更，自屬刑法變造準私文書。且被告之變造行為，有造成悠遊卡公司損害之虞，因此亦符合刑法第210條「足以生損害於公眾或他人」之要件。是核被告所為，該當刑法第220、210條變造準私文書罪，自應以該罪相繩。

㈡ 刑法偽造、變造支付工具罪構成要件之檢討

刑法第201條之1為偽造、變造支付工具罪規定，該條文所保護之行為客體，除所列舉之信用卡、金融卡、儲值卡三者之外，尚包括此三類卡片之相類似之概括規定「作為簽帳、提款、轉帳或支付工具的電磁紀錄物」，以補列舉條文之不足。是偽造、變造支付工具電磁紀錄罪，亦為本條文所明文處罰之範圍。

悠遊卡交易過程中，持卡人先給付悠遊卡發行機構即悠遊卡公司金額作為儲值金額，在持卡人持卡使用時始自動扣款。是悠遊卡是一種取代貨幣的支付方式，持卡人事先給付一筆金額予發行機構，利用悠遊卡內之儲存晶片，紀錄儲存現金的價值等相關資訊。持卡人持悠遊卡消費時，在交易完成時，透過讀寫器扣除卡片內所儲存的價值，以支付商品或服務，而特約機構將扣款紀錄交給發行機構，以領取當天的營收。是悠遊卡為刑法第201條之1之儲值卡，至為明確。

本案被告將悠遊卡、此一支付工具之電磁紀錄加以改變，核其所為，與刑法第201條之1變造支付工具電磁紀錄物罪構成要件相合致，自應以該罪之罪責論處。

㈢ 修正前電子票證發行管理條例第30條

「電子票證發行管理條例」於98年1月23日立法院三讀通過，電子票證以電子、磁力或光學形式儲存金錢價值，並含有資料儲存或計算功能之晶片、卡片、憑證或其他形式之債據，作為多用途支付使用之工具，具有財產價值，自會成為有心人士偽造、變造之標的。是當時立法通過之電子票證發行管理條例於第30條第1項規定「偽造、變造或未經主管機關核准發行本條例所規定之電子票證者，其行為負責人處一年以上十年以下有期徒刑，得併科新臺幣一千萬元以上二億元以下罰金。其犯罪所得達新臺幣一億元以上者，處七年以上有期徒刑，得併科新臺幣二千五百萬元以上五億元以下罰金。」以資規範偽造、變造電子票證之刑事責任。

惟悠遊卡係以無線射頻識別技術Radio Frequency Identification 即RFID技術，讓非接觸式卡片不需要插讀卡機，只要晶片接上感應線圈即可使用，不必拘泥於「卡片」

的外形。因此悠遊手機、飾品悠遊卡、行動電話薄膜悠遊卡及各種立體造型之外觀均有之。是電子票證未必有其固定之外形，且有心人士所圖者，無非係電子票證所儲存之有金錢價值之電磁紀錄，而該等電磁紀錄才是犯罪者所欲偽造、變造之標的，犯罪者只要能將電子票證所儲存之電磁紀錄予以偽造、變造，即可達其犯罪目的，此與信用卡、金融卡之偽造、變造，偽造集團除必須製作剪貼卡、白卡，或是偽造、變造一外觀上與真正信用卡幾可亂真之假卡的情形大不相同。惟當時電子票證發行管理條例第30條之條文用語，漏未將偽造、變造電子票證之電磁紀錄一併予以規範，此立法上之疏漏，造成解釋上僅規範偽造、變造電子票證之實體票證部分。再者，刑法第201條之1條文規定，就支付工具之偽造、變造罪已有詳細之規範，且亦能適用於電子票證，則何需疊床架屋，再有電子票證發行管理條例第30條之規定。

是上述條文經行政院於104年4月23日第3445次院會通過「電子票證發行管理條例」部分條文修正草案中，亦認為鑒於刑法第201條之1第1項就偽造、變造信用卡、金融卡、儲值卡等電磁紀錄物之刑度已定有規範，為回歸刑法之規定處理，擬刪除電子票證發行管理條例第30條關於偽造、變造電子票證刑罰之規定。而上開修正草案，業經立法院於104年6月9日通過，並經總統於同年月24日公布、同年月26日生效。是依最新之修正條文，偽造、變造儲值卡之電子票證相關電磁紀錄物之刑責毋庸再適用電子票證發行管理條例，而全部回歸刑法之規定處理，已充分解決法律適用衝突之疑慮，為正確妥當之法律修正。

三、電腦詐欺罪章構成要件之檢討

刑法第339條之3第1項規定：「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，而取得他人之財產者，處七年以下有期徒刑，得併科七十萬元以下罰金。」第二項規定：「以前項方法得財產上不法之利益或使第三人得之者，亦同。」第三項規定：「前二項之未遂犯罰之。」

本件被告利用電腦連接proxmark3之設備，並透過proxmark3之設備接收取得悠遊卡之密鑰串流，而取得某一區段金鑰，再經過不斷重複嘗試鑑別蒐集足夠之密文，去取得其他的金鑰，又經比對悠遊卡加值後晶片記憶體之內容，查悉記憶體相關資料儲存之位置後，執行寫入的命令，而將悠遊卡晶片記憶體所記錄之儲值金額之電磁紀錄加以改變，是否符合刑法第339條之3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，而取得他人之財產？

㈠ 悠遊卡是否屬於刑法之「電腦設備」？

1.「電腦設備」定義介紹

民國92年刑法修正通過並增訂第36章「妨害電腦使用」罪章，其立法理由說明中指出：「電腦網路犯罪向有廣義、狹義之分別，廣義之電腦犯罪指凡犯罪之工具或過程牽涉到電腦或網路，即為電腦犯罪；狹義之電腦犯罪則專指以電腦或網路為攻擊對象之犯罪。由於廣義之電腦犯罪，我國刑法原本即有相關處罰規定，毋庸重複規範，故本章所規範之妨害電腦使用罪乃指狹義之電腦犯罪。又按電腦使用安全，已成為目前刑法上應予保障之重要法益，社會上發生妨害他人電腦使用案件日益頻繁，造成個人生活上之損失益趨擴大，實有妥善立法之必要，因此種電腦犯罪所規範之行為及保護之對象，與現行刑法分則各罪章均有不同，應有獨立設章之必要，爰新增本章。」

是從立法理由可明白看出刑法修正時採狹義說，亦即專指電腦或網路為攻擊對象之犯罪[21]。而所謂「電腦」究為何指？我國法條上並未明文予以定義。一般所謂的傳統電腦，係指個人電腦（PC，即Personal Computer）最常見的為桌上型電腦及筆記型電腦；而隨著電腦製造技術及科技發展，近來之智慧行手機及平板電腦等相當普及，且為吾人日常生活所不可或缺之重要物品。

有學者認為，「所謂電腦，即電子計算機，係指得以執行程式命令，處理輸入、輸出、算術以及邏輯運算之電子裝置。其主要結構，係由輸入裝置（如鍵盤、麥克風、滑鼠）、處理器（CPU）、輸出裝置（如螢幕、喇叭或印表機）以及儲存裝置（如軟碟、硬碟、光碟等）等四個基本元件所組成。所謂相關設備，係指雖非電腦之主要結構裝置，惟得透過連線而將指令輸入電腦之輔助設備而言。例如終端機是。至電腦或其相關設備，係何人所有或持有， 並非所問。」[22]，依此見解作為電腦之主要結構有四個基本元件：1.輸入裝置（如鍵盤、麥克風、滑鼠）；2.處理器（CPU）；3.輸出裝置（如螢幕、喇叭或印表機）；4. 以及儲存裝置（如軟碟、硬碟、光碟等）。

另有論者認為本次修法係簡化法律問題，將受攻擊客體是有體物或無體物作區分標準，如果是有體物則以傳統刑法評價，例如搶奪磁片或竊取電腦；如為無體物則以電腦犯罪專章處理，例如駭客入侵網站竊取電磁紀錄[23]，如此區分簡明扼要，使實務界在處理個案時能快速掌握法律之適用。

---

21 陳憲緯，我國妨害電腦使用罪章法律適用之再檢視-以網路遊戲虛擬寶物竊盜為中心，國立臺北大學碩士論文，2012年7月，頁9。

22 甘添貴，虛擬遊戲與盜取寶物，臺灣本土法學雜誌第50期，2003年6月， 頁180。

23 葉奇鑫，刑法新修正妨害電腦使用罪章條文簡介，法務通訊第2140期，2003年6月，頁4。

美國為了抗制電腦犯罪，美國聯邦國會在1986年制定聯邦電腦詐欺及濫用防制法（The Computer Fraud and Abuse Act of 1986，CFAA）。CFAA對於「電腦」的定義是：「得以執行邏輯、計算及儲存功能的電子、磁性、光學、電子化學或其他高速資料運算裝置；以及其他相關，或是與上述高速資料運算裝置同工的資料儲存及通訊裝置。但是，上述的高速資料運算裝置不包含自動打字機、自動排版機、手持計算機或其他類似的裝置。」如此立法定義相當廣泛，所能涵蓋的類型亦相當的多。也因國會對電腦採取較開放之定義，美國法院對於電腦也採取了很有彈性的解釋[24]。

英國的電腦犯罪法制主要是由兩個法案組成，亦1990年制定之電腦濫用法案（Computer Misuse Act），處罰「禁止無權進入他人電腦行為」（Unauthorised access to computer material）、「禁止無權竄改他人電腦軟體」（Unauthorised modification of computer material）兩種行為；及 2006年警察與正義法案第五章增訂規範「有關禁止行為人故意破壞電腦系統之行為」（Unauthorised acts with intent to impair,or with recklessness as to impairing,operation of computer,etc.）及「行為人製造提供取得電腦犯罪之用的程式、軟體行為」之處罰規定（Making，supplying or obtaining articles for use in offence under section 1or 3）[25]。英國電腦犯罪法制，就電腦犯罪之處罰已有相當完整規範，惟其與美國法制之最大不同點，即為英國並無如美國定義何謂是「電腦」。

我國之法制未曾明訂「電腦」之定義，而因資訊科技之日新月異，對於「電腦」、「電腦系統」及「網路」等科技名詞定義不易，未免掛一漏萬，或未來法律適用無法跟上科技腳步，故仿照英國電腦濫用法案（Computer Misuse Act）之立法方式，對上開名詞不作定義[26]。如此之立法妥當適切，對於科技之日新月異，未來也許會出現刑法條文中無法涵括之犯罪類型或犯罪客體，故不於構成要件中加以明定是最佳之立法模式，惟仍須透過實務逐步將「電腦」的範圍界定出來[27]。

2. 悠遊卡與「電腦設備」

(1) 否定說之見解

是悠遊卡究竟是否屬於「電腦設備」？有論者以前述學者所列出之電腦之主要結構有四個基本元件：1.輸入裝置（如鍵盤、麥克風、滑鼠）；2.處理器（CPU）；3.輸出裝置（如螢幕、喇叭或印表機）；4.以及儲存裝置（如軟碟、硬碟、光碟等），及所

24 蔡榮耕，Matrix駭客任務：刑法第358條入侵電腦罪，科技法學評論5卷1期，2008年4月，頁114-115。
25 劉景嘉，刑法電腦犯罪立法之研究，國立臺北大學法律學系碩士論文，2014年，頁48-49。
26 甘添貴，刑法各論(上)，三民書局股份有限公司，二版，2010年11月，頁424。
27 陳憲緯，我國妨害電腦使用罪章法律適用之再檢視-以網路遊戲虛擬寶物竊盜為中心，國立臺北大學碩士論文，2012年7月，頁10。

謂相關設備，係指雖非電腦之主要結構裝置，惟得透過連線而將指令輸入電腦之輔助設備而言，因此認為相關設備應係指可透過電腦取得相關資訊之設備而言，典型的相關設備如終端機，因此並非如悠遊卡、信用卡、支付工具等。則悠遊卡既非「電腦或其相關設備」，故認為本件被告之行為不該當刑法第339條之3電腦詐欺罪嫌[28]。

(2) 肯定說之見解

肯定說之見解則認為悠遊卡是非接觸式的智慧卡（Smart Card），其內有IC晶片，而IC晶片除有記憶的功能外，還有運算、統計以及資料處理的功能。因此有學者指出「一般所謂的智慧卡，亦即具有儲存與處理個人金融資料功能的晶片，由於具備處理與儲存資料功能，智慧卡也可算是本罪所稱之『電腦及其相關設備』」[29]，如採此見解，本件被告之行為自有適用刑法第339條之3電腦詐欺及刑法第359條妨害電腦使用罪章等規範之餘地。

(3) 本文見解

悠遊卡係非接接觸式的智慧卡（Smart Card），和電腦的結構很類似，其內有IC晶片，而含有CPU、ROM、RAM、和EEPROM。其中CPU與電腦的CPU作用完全一樣，ROM中存放卡的操作系統，有如Windows或DOS作業系統；RAM的作用類似電腦中的記憶體；EEPROM的作用類似電腦中的硬碟。惟智慧卡與電腦最大的不同點在於，智慧卡在整個智慧卡系統的架構中，扮演2個重要的角色，即身份性和安全性。身分性就是指一張智慧卡，代表著一個系統的使用者，從智慧卡提供的ID號碼，系統就能方便地識別出誰在使用系統。同時，由於智慧卡儲存資料的穩定性和其物理的可攜帶性，所以智慧卡是一個很好的個人身份識別工具。安全性則是智慧卡的另一優勢，由其以智慧卡為支付工具時，更需確保交易安全，因此在卡片儲存結構及卡片與讀寫器間之通訊流程，均需有安全的加密及認證機制與演算方法，防止資料有衝突、洩密或遭竄改之問題。且由於智慧卡在智慧卡系統中，是儲存資料即電磁紀錄、和傳遞之載體，因此智慧卡的電磁紀錄儲存安全甚為重要。目前廣泛使用之智慧卡，使用的是EEPROM作為儲存電磁紀錄之記憶體，因EEPROM讀寫速度快，資料可反覆進行複寫。

由於智慧卡是在將EEPROM記憶體封裝在卡片同時，也將微處理器晶片（CPU），均封裝在卡片內，外部讀寫設備只能通過CPU與智慧卡內的EEPROM進行數據交換，在任何情況下，均不能再存取（access）到EEPROM中的任何一個單元。同時智慧卡中封裝了微處理晶片（CPU），因此EEPROM的資料界面（interface）在任何

28 陳子平，偽造支付工具電磁紀錄物罪與相關犯罪，月旦法學教室第111期，2012年1月，頁83-84。
29 蔡蕙芳，刑法第三三九條之三不正利用電腦取財得利罪，月旦法學教室第46期，頁75。

情況下，均不會與智慧卡的對外資料流相連接。

外部讀寫設備在與智慧卡進行資料交換時，首先必須發指令給CPU，由CPU根據其內部之ROM中儲存的卡片操作系統（COS）對指令進行運算並分析判斷，在確認讀寫設備的合法性後，允許外部讀寫設備與智慧卡連接。之後的資料操作仍然要由外部讀寫設備發出相應的指令，並且CPU對指令進行正確運算後，允許外部讀寫設備與智慧卡中之資料儲存區（RAM）進行資料交換。資料交換成功後，在CPU的控制下，利用智慧卡中的內部資料匯流將內部RAM中的數據與EEPROM中的資料進行交換。是資料處理的過程中，外部讀寫設備只和CPU溝通，同時也只能與資料緩存區RAM進行資料交換，根本無法實現對智慧卡中EEPROM資料直接進行存取。這樣也就實現了對智慧卡EEPROM資料的安全保護，因此智慧卡也具備資料安全保護措施[30]。

是在悠遊卡系統中，悠遊卡是資料儲存和傳遞的載體，且為確保系統安全，悠遊卡必須具備對資料儲存安全性之保護措施，以防悠遊卡內之資料被竄改。因此，外部讀寫器和悠遊卡連線後的資料操作，均要由外部讀寫設備發出相應的指令，悠遊卡則被動地進行通訊認證、資料交換及運算，悠遊卡並沒有獨立執行邏輯、計算及儲存功能之能力，並非電腦設備至明。則悠遊卡在整個交易系統中，並非電腦設備，真正的電腦設備，應係悠遊卡系統之後端電腦應用系統。而悠遊卡及讀寫設備，如同後端應用電腦系統之手腳延伸，負責在前端進行在安全認證及加密機制下之資料的運算及蒐集後，所有的交易資料都會透過網路，送回悠遊卡公司的後端電腦應用系統，以供稽核、對帳及營運管理，是本文採否定說。則本件被告之行為並非針對悠遊卡系統後端之電腦應用系統為攻擊，而係在悠遊卡系統之前端，變造悠遊卡內之電磁紀錄行為，且因悠遊卡並非本罪所稱之「電腦及其相關設備」，自無刑法第339條之3第1項電腦詐欺罪規範之適用甚明。

㈡ 是否製作財產權得喪變更紀錄而取得他人財產？

承前所述，本文認悠遊卡並非本罪所稱之「電腦及其相關設備」，惟應再進一步檢討的是，本件經被告變造電磁紀錄之悠遊卡3張，且均在超商內查詢餘額為變造後之金額9，000元而變造成功，承前所述，本文認悠遊卡並非本罪所稱之「電腦及其相關設備」，惟應再進一步檢討的是，本件經被告變造電磁紀錄之悠遊卡3張，且均在超商內查詢餘額為變造後之金額9，000元而變造成功，則此時是否如本件法院判決所認定「被告以不正方法變造如附表一編號一所示之悠遊卡，並持往超商查詢餘額，而使該

30 朱庆堂、陈汭新，一种基于智能卡的网络安全访问控制模型，计算机应用研究第23卷第9期，2006年9月，頁134。

悠遊卡中經變造之虛偽資料傳送至告訴人悠遊卡公司後臺電腦所製作之財產權變更紀錄」，而該當刑法第339條之3之罪？

1. 傳送虛偽紀錄至後臺電腦是否等同於製作之財產權變更紀錄

本件被告確實已經將該悠遊卡內之儲值金額資料變更完成，其持往超商查詢餘額成功，而使該悠遊卡中經變造之虛偽資料，傳送至告訴人悠遊卡公司後臺電腦，亦無疑問。但此時應探求並釐清之爭點在於，上傳虛偽資料是否與後臺電腦製作財產權紀錄劃上等號？亦即，上傳虛偽資料，是否代表後臺電腦即會依此上傳虛偽資料加以變更紀錄？

目前使用悠遊卡作為支付工具的業者，其交易資料都會透過網路，送回悠遊卡公司的後端電腦應用系統，由於資料涉及各業者的盈收分帳，為避免資料在傳送過程中，有被非法竄改造假之虞，因此悠遊卡公司對參與的業者，規範了交易資料的傳輸格式，其作法為每筆交易資料附加MAC（Message Authentication Code）後才傳送；在確認傳輸過程中沒被竄改，經過後端電腦應用系統匯總統計後，再與各業者進行分帳與對帳。是後端電腦應用系統，經過稽核、對帳及其他營運原始資料（raw data）之管道，自可判讀出悠遊卡之儲值金額是否遭到竄改[31]，此即本案悠遊卡公司終究還是發現了被告變造之悠遊卡有異常情形進而鎖定查獲之原因。

由本件被告被查獲之原因可以得知，作為悠遊卡系統後端電腦應用系統之後臺電腦，具稽核、對帳及擁有其他營運原始資料（raw data）管道之功能，可以掌握加值、消費的時間地點等紀錄[32]。是本件被告將已變造儲值金額之悠遊卡持往超商查詢餘額成功，而使該悠遊卡中業經變造之虛偽資料，傳送至悠遊卡公司後臺電腦，經後臺電腦稽核、對帳即發現異常，而既已發現異常，後臺電腦豈會准許變更為異常之虛偽紀錄？準此，該悠遊卡中經變造之虛偽資料確有傳送至悠遊卡公司後臺電腦，惟此時後臺電腦即發現異常，無依上傳之虛偽資料製作財產權變更紀錄之理。

2. 被告之犯罪故意及行為

何況依被告之犯罪故意及行為，均係針對悠遊卡系統之前端亦即無線射頻傳輸區部分（參本文上圖「RFID系統架構圖」紅色虛線右側部分）之攻擊，其將悠遊卡晶片記憶體所記錄之儲值金額之電磁紀錄加以改變，並持卡在超商之讀寫設備成功讀寫並消費而取得商品，被告對於後續虛偽資料是否上傳、後臺電腦是否變更電磁紀錄，本即超出其犯罪之故意及行為。

31 徐春進、史敦仁，捷運系統票證加密與通訊安全，捷運技術第38期，頁220，2008年2月。
32 陳子平，偽造支付工具電磁紀錄物罪與相關犯罪，月旦法學教室第111期，2012年1月，頁78。

是本件自悠遊卡系統之後端電腦應用系統之後臺電腦予以檢視，難認後臺電腦已製作財產權得喪變更紀錄，且後臺電腦之電磁紀錄是否變更亦超出被告犯罪之故意及行為，因認本件核被告所為，與刑法第339條之3之構成要件並未合致，而不能以該罪相繩。

㈢ 本罪與詐欺罪之關係

刑法第339條詐欺罪與刑法第339條之3之電腦詐欺罪之關係，有學者[33]認為「兩者不具特別關係，也不具補充關係，但電腦詐欺罪之罪質，當然含有詐欺之成分，因此，二者具有吸收關係，即電腦詐欺罪為吸收規定，普通詐欺罪為被吸收規定」。惟另有學者認為，參酌德國刑法第263a電腦詐欺罪與德國刑法第263條傳統詐欺罪，無論在結構上或價值上均具有等值性，因此認為電腦詐欺罪與詐欺罪應係擇一之排他關係，如果有人介入就是普通詐欺罪。如果沒有人介入之自動化過程，則屬於電腦詐欺罪[34]。

除前述之吸收關係、擇一關係外，亦有學者認為，普通詐欺和電腦詐欺間，因為彼此的行為對象並不相同；一為自然人、一為代替自然人的電腦，兩者之間應當是互斥。如果單純從規範本身來看，應當認為輸入資料指令詐欺與普通詐欺的構成要件，各自擁有不同的規範範疇。惟在具體個案的事實內容，同時跨越兩者規範時，例如行為人欺騙相對人，使相對人將不正確的資料輸入電腦，因此在電腦中製作財產得喪變更紀錄，而取得財產。此時同時構成普通詐欺及電腦詐欺之構成要件，則應當考慮電腦詐欺規定填補法律漏洞的規範目的，而以「漏洞存在」作為適用本條規定的前提，所以從這種填補既有規定法律漏洞的觀點來看，應當認為本條規定唯有在傳統財產犯罪規定不適用的情形，始得適用，而具有補充規定的性質[35]。

由前開之學說之探討情形，可知在具體個案同時符合電腦詐欺及普通詐欺之構成要件時，始有前述學說上之爭議，此與本件之案例事實經檢討後已認為不符合電腦詐欺罪之構成要件之情形有所不同。是基於普通詐欺及電腦詐欺罪，在結構及價值上具有等價性，本文認為本件之具體事實雖不該當刑法第339條之3之電腦詐欺罪，則此時應回歸刑法普通詐欺罪之構成要件予以適用。

是本件被告意圖不法所有，利用proxmark3之設備接收並取得悠遊卡之密鑰串流，而取得某一區段金鑰，再經過不斷重複嘗試鑑別蒐集足夠之密文，去取得其他的金

33 甘添貴，體系刑法各論(第二卷)，2000年4月初版，頁326。
34 蔡蕙芳，電腦詐欺行為之刑法規範，東海大學法學研究第18期，2003年6月，頁50。
35 謝開平，電腦詐欺在比較刑法上之研究，國立台北大學博士論文，頁144。

鑰，又經比對悠遊卡加值後晶片記憶體之內容，查悉記憶體相關資料儲存之位置後，執行寫入的命令，而將悠遊卡儲值金額之加以改變，經持卡至超商之讀寫設備使用，使超商之讀寫設備與業經被告變造儲值金額之悠遊卡間，成功完成資料交換，此時被告以此經變造電磁紀錄之悠遊支付工具付款之同時，也欺騙了超商及其所僱佣的店員。換言之，超商店員在看到並聽到，被告持用之變造電磁紀錄之悠遊卡與讀寫設備完成讀寫，並發出「嗶」聲時，造成超商店員因此陷於錯誤，而交付被告所購買之商品，致超商及悠遊卡公司均受有損害。是核被告所為，構成刑法第339條第1項詐欺取財罪，堪已認定。

四、妨害電腦使用罪章構成要件之檢討

刑法第359條規定：「無故取得、刪除或變更他人電腦或其他相關設備之電磁紀錄，致生損害於公眾或他人者，處五年以下有期徒刑、拘役或科或併科二十萬元以下罰金。」

本件被告無正當理由利用電腦連接proxmark3之設備，並透過proxmark3之設備接收取得悠遊卡之密鑰串流，而取得某一區段金鑰，再經過不斷重複嘗試鑑別蒐集足夠之密文，去取得其他的金鑰，又經比對悠遊卡加值後晶片記憶體之內容，查悉記憶體相關資料儲存之位置後，為寫入的命令，而將悠遊卡晶片記憶體所記錄之儲值金額之電磁紀錄加以改變，是否構成本條所規定之無故變更他人電腦或其他相關設備之電磁紀錄？

如前所述，悠遊卡是非接觸式的智慧卡（Smart Card），其內有IC晶片，而IC晶片除有記憶的功能外，還有運算、統計以及資料處理的功能。惟悠遊卡在悠遊卡系統中僅是資料儲存和傳遞的載體，且被動地與讀寫設備進行通訊認證、資料交換及運算，悠遊卡並沒有獨立執行邏輯、計算及儲存功能之能力，並非刑法第359條所稱之「電腦及其相關設備」。是本件被告之行為並非入侵悠遊卡系統後端之電腦應用系統，而係在悠遊卡系統之前端，變造悠遊卡內電磁紀錄之行為，且因悠遊卡並非本罪所稱之「電腦及其相關設備」，參以自悠遊卡系統之後端電腦應用系統檢視，既已發現有上傳虛偽資料之異常，難認後臺電腦已製作財產權得喪變更紀錄，且後臺電腦之電磁紀錄是否變更亦超出被告犯罪之故意及行為，因認無刑法第359之無故變更他人電腦或其他相關設備之電磁紀錄罪之適用。

肆、結論

非接觸式電子支付工具，所使用之RFID技術傳輸技術，架構包含電子標籤（RFID tag）、讀寫器（RFID Reader/Writer）及電腦應用系統三大部分；安全機制，區分為無線射頻傳輸區與有線網路傳輸區兩部份。各個系統架構及傳輸區，均有可能成為有心人士攻擊之目標。而各種不同的攻擊手法和標的之犯罪案件，考驗偵審機關如何掌握具體個案之相關科技手法，以正確認定事實及妥當適用法律。

科技進展帶來之利益，正如本文探討之非接觸式電子支付工具，提供了民眾便利之生活環境，且已成為現今一般人普遍使用之支付工具，此為科技進展帶來之裨益。然科技發達的同時，伴隨而來的即是新興類型之犯罪，挑戰法律人如何跨越科技議題之鴻溝。本文以結合科技及法律方式，了解非接觸式電子支付工具之破解及實務案例，期許法律人能抱持與科技接軌之開放態度，兼顧刑事法體系之思維，建構有效防制科技犯罪為理想與目標之資訊社會。