第一章　緒論

壹、研究背景與研究目的

隨著數位科技之發展，整合製造、銷售、流通與金融之商業自動化和電子商務環境的建立與應用，已成為數位匯流下的知識經濟發展必然的走向。除電子商務(electronic commerce)已有突飛猛進的發展外，電子支付系統(electronic payment system)與電子貨幣(e-money)等金流機制之發展，在金融服務更趨電子化之時，諸如網路銀行(cyberbanking)與網路電子貨幣等交易方式，即成為金融創新服務的重要指標，大大提昇了商業交易的支付效率；近年來更由於電信、資訊及傳播科技之匯流趨勢，致使傳統銀行服務結合行動通訊科技，整體金融服務逐漸呈現朝向行動銀行(mobile banking)等交易方式發展的趨勢。

為迎接電子商務潮流及多元化電子付款趨勢，並鑑於電子金融與相關付款機制對貨幣市場整體金流影響甚深，先進國家多已著手規劃相關交易環境之建置，並賦予其法律依據。反觀我國財政部僅於民國88年6月底公布財政部台財融字第88725263號「個人電腦銀行業務及網路銀行業務服務契約範本」(以下稱「網路銀行服務契約範本」)，供消費者向銀行申請網路銀行服務之使用，以及財政部民國89年8月8修訂之「金融機構辦理電子銀行業務安全控管作業基準」祈使國內電子金融監理制度及運作更為健全，惟目前尚無相關法令可供相關消費者或銀行加以遵循；至於行動商務之金流相關規劃，亦已成為相關機關積極研擬規劃之重要發展方向。

另有鑑於電子交易環境之新興服務所涉之資料儲存、流通與利用等問題之解決，顯見複雜性與困難度，如何兼顧鼓勵各項服務之發展與確保民眾資訊之安全，以增進消費者對科技服務的使用信心，不僅

是我國邁入資訊化社會的重要課題，亦是國際間普遍之規範重點。我國對於電子交易之金融法制環境，除前開網路銀行服務契約範本等作為交易基礎規範，及其他以自律機制等方式控管各該電子交易之資訊安全外，並應兼顧「電腦處理個人資料保護法」就隱私權保障等提供基礎規範相關之法制配套。

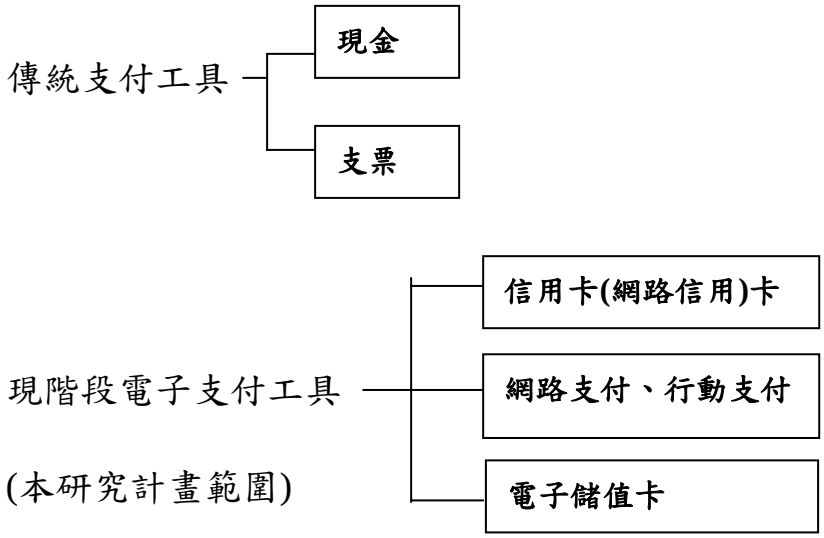
為因應金融服務電子化及整合的趨勢，本研究擬針對新興之電子金融應用服務中，政府相關機關管理機制之建立，期就電子金融服務發展、交易資訊安全及隱私權保障等相關事項，提出具體建議，以利政策規劃之參考依據。

貳、 研究內容與範圍

本研究案之研究範圍，重點在電子金融服務與電子付款機制中，屬於網際網路範疇之管理規範，關於其他非屬網際網路之電子金融服務與電子付款機制部分，將與其他於本研究案中排除之部分利用專章一併討論；另由於本研究側重企業與消費者間之相關問題研究，故對於電子銀行研究部分，有關清算程序及大額支付等節，將不予討論。其次，管理規範部分，重在於電子金融服務與電子付款機制種種程序內國法之相關規定，其中包含現行國內外規範，未來國際規範趨勢，以及國內修法走向，惟對於國際條約或國際慣例討論之部分，若有參考價值，僅提供修法建議，且亦將在前述專章中一併列入討論；再者，因本研究案側重在電子金融服務與電子付款機制，故對於網路店家利用電子通路之訂約模式、電子資料保護，或其他安全機制，除非於價金之給付或貨物之交付時牽涉到電子金融服務與電子付款機制，否則將不列入討論；而在電子金融服務與電子付款機制之運作流程中，牽涉到當事人或第三人之民事或刑事責任，皆列入本研究範圍；又本研

究案側重於金融機構與消費者間(B2C)相關規範與機制，對於金融機構與金融機構間，或金融機構與其他系統或管理機構間之規範暫於專章中略為討論，但對消費者權利義務有所影響之部分，則會納入研究。

以下為傳統支付工具與現階段電子支付工具之種類：



參、 研究方法與進行步驟

一、研究方法

本研究計畫所採之研究方法如下：

(一) 文獻分析方法

首先透過各項資料來源，認識歐、美等國家電子金融服務與電子付款機制及相關法制狀態，以及我國現行相關法規、制度。

(二) 專家訪談方法

經由對相關官員、業者、以及本領域內之專業人士的訪談，獲得不同面向之意見。

二、進行步驟

(一) 將透過網際網路、期刊、書籍文獻等來源所獲得之電子金融服務與電子付款機制資料(主要集中在電子支付)，加以研究、分析、比較。

(二) 經上述整理比較分析所得之結果，找出目前我國電子支付方式所面臨之法律問題，並試圖為相關法律問題尋求解決之途。

(三) 經由對相關官員、業者、以及本領域內之專業人士的訪談，以使就產、官、學三方意見予以融合，同時以不同面向之意見研究問題。

肆、問題提出

電子付款工具是為了解決電子商務付款所應運而生的付款機制，由於本身沒有實體，因此，可以透過網際網路來進行付款，比傳統付款工具節省成本和時間，讓消費者享受到科技進步所產生之便利。

然而，電子付款工具的發行需透過銀行進行儲值，或我國實施電子票據均需透過銀行或公正的第三者組織，才得以進行轉換儲值或身分驗證的動作，其使用之流程較傳統之付款工具複雜。而且，初期相關標準訂定不易，亦無相關法令可供電子付款工具之發行者與使用者遵循，電子商務相關的服務不論在軟體或硬體市場上，都是廠商爭食的大餅，對消費者而言，可能因其所需支付的成本而造成廠商推動電子支付工具的阻力，這些都是電子付款機制推動時所會面臨到的問題。

另外，由於使用網際網路的電子支付機制的特性，相較於傳統之付款工具，電子付款除了配合電子商務而能透過數位化的方式來使用外，就交易安全及隱私權之保護，亦是值得探討的議題。

影響電子付款工具的安全因素可大略分為技術、法律與管理三方面，除了可透過技術之設計，使交易安全與消費者之隱私權獲得保障外，有關電子付款機制相關之法律與其管理對交易安全與消費者隱私權之保護亦非常重要，因為法律是為了彌補技術的不足，有效的管理機制，更進一步能補充電子付款工具使用之交易安全與對消費者之保障。

電子支付機制乃係新興之付款工具，其交易之結果雖與傳統現金相去不遠，惟在使用電子方式為付款工具之交易中，因使用電子支付機制為付款工具所涉及之當事人，及其所可能產生之問題，與傳統交易之當事人僅限於買賣雙方並不相同，故而電子付款之管理機制之建立與其相關法令之訂定，於網際網路如此普遍使用之現代，實為一刻不容緩的議題。

第二章　電子金融之概況與分析

壹、網路金融概況

所謂電子金融(e-Finance)，泛指以網路金融(online banking)為主，經由網際網路(Internet)所從事的各項金融相關服務。迥異於傳統上的實體(臨櫃)服務，而係以虛擬化(visualized)、電子化(electronic)方式提供金融業務的服務型態。簡言之，是資訊科技(IT)因應網際網路結合金融業務快速發展的產物，更是適應電子商務(e-Commerce)與行動商務(m-Commerce)發展需要而產生的網路世代金融運行模式。

一、網路金融與支付系統

網路金融的發展基本上決定於網路經濟和電子商務發展的內在規律；析言之，網路金融於現行商業支付系統中已屬不可避免之交易模式，謹依序敘明如次：

(一) 揆諸近年來的實務發展，網路金融於電子商務體系已屬不可或缺之交易模式。包括商務資訊、資金支付和商品配送三階段的電子商務，未來具體呈現將分成資訊流、資金流和物流的三個面相。商業活動中，銀行能否在網上提供電子支付服務，已成為電子商務中最具關鍵的致勝因素，服務創新的風尚所及，網路金融勢將成為今後金融業不可或缺的交易與支付介面。

(二) 承前所述，電子商務的發展改變了金融市場的競爭格局，從而促使金融業走向網路化。電子商務使網上交易擺脫了時間和空間的限制，資訊獲得的成本比傳統商務運行方式大幅降低，表現在金融市場上就是直接融資的活動比以前大幅增加。電子商務的出現動搖了傳

統金融行為在價值鏈[1]中的地位，使傳統金融機構失去了在市場競爭中所具有的資訊優勢。

(三) 金融網站的設立，可以應對數以萬計的用戶查詢和交易業務而不降低服務品質，同時使交易成本大幅降低。根據著名研究機構 Booz Allen & Hamiltor 估計，處理同一筆交易的費用，虛擬形態的網路銀行作業成本相較於實體形態的銀行作業成本降低約一百多倍[2]。基此，電子商務的發展有助於金融機構大幅降低經營成本，提高經營效率，此乃網路金融得以出現並迅速發展的最主要原因。

二、網路金融制度建構

以金融重鎮的美國而言，網路金融是二十世紀的最後五年才開始出現和發展，與傳統金融的磨合還處於市場發展推動下的商業實踐和探索。但從過去其快速發展的五、六年的過程來看，基本可以歸納出網路金融的主要特性：

(一) 業務創新

網路金融以客戶為中心的性質決定了它的創新性特徵。為滿足客戶的需求，擴大市場占有率(Market Share) 和增強競爭實力，網路金融必須進行業務創新。這種創新發生在金融的各個領域，例如在信貸業務領域，銀行利用網際網路上搜索引擎(Search Engine)軟體，為客戶提供適合其個人需要的消費信貸、房屋抵押信貸、信用卡信貸、汽

[1] 價值鏈：美國作業成本科技公司 (ABC Technologies) 及美國供應鏈局 (The Value Chain Authority) 曾聯合界定何謂價值鏈：價值鏈是一種高層次的物流模式，內容由原材料作爲投入資產開始，直至爲原料透過不同過程售予顧客爲止，當中作出所有的增值活動都可包括在價值鏈中組成部分。參見何謂價值鏈，易通網，http://www.easipass.com/ytsce/wl/ytsce_wlsy_03.htm (last visited on 2005.09.10)。

[2] 狄衛平，網路金融研究與發展策略，金融研究，http://www.acsi.gov.cn/web/NewsInfo.asp?NewsId=1234 (last visited on 2005.09.10)。

車消費信貸服務；在支付業務方面，新出現的電子帳單傳送和付款[3] (EBPP，Electronic Bill Presentment & Payment)通過整合資訊系統來管理各式帳單(保險單據、帳單、抵押單據、信用卡單據等)。在資本市場上，電子通訊網路(ECNs，Electronic Communication Networks)[4] 為市場參與提供了一個可通過電腦網路直接交換資訊和進行金融交易的平臺，有了 ECNs，買方和賣方可以通過電腦相互通訊來尋找交易的物件，從而有效地消除經紀人和交易商等傳統金融仲介，大幅降低交成本。

(二) 管理創新

管理創新包括兩個方面：一方面，金融機構放棄過去以單獨機構拓展業務的策略管理思想，充分重視與其他金融機構、資訊技術服務商、資訊服務提供商、電子商務網站等的業務合作，達到在市場競爭中實現雙贏的局面。另一方面，網路金融機構的內部管理也趨於網路化，傳統商業模式下的垂直式管理模式將被一種網路化的扁平組織結構所取代。

(三) 市場創新

---

[3] EBPP 是指「帳單電子化及線上付款機制」的解決方案，也就是將原流通的實體帳單經電子化處理成爲電子帳單然後再傳遞給客戶，當客戶收到電子帳單後可利用「線上」付款機制立刻繳款同時得到電子收據。EBPP 的概念至少在 4 年前即已被提出，其提出的目的是在解決企業及政府單位最困擾的營運成本(實體帳單寄送的紙張、處理、印刷、郵寄…等費用及代收通路所抽取的手續費)。但 EBPP 目前推行的成效不彰，主要原因是在於「線上」付款機制所產生的電子收據的認證、相關法令尚未完備及消費者的認同度三方面。參見何謂 EBPP, Easyuse, http://www.easyuse.com.tw/news_20030330-2.htm (last visited on 2005.09.10)

[4] 1990 年代末期，美國 Nasdaq 系統設立了電子傳輸網路系統 (Electronic Communication Networks, ECNs)。基本上 ECNs 是一個提供投資者間直接交易服務的網站，ECNs 的設立提供了市場流動性與競爭程度。利用 ECNs 可以大量減少不必要的人力支出，將省下的經費用做軟體開發以及安全維護的改善經費。參見楊澤泉教學網頁，華爾街的完全競爭 http://www.ba.ncku.edu.tw/teacher/yong/econom_life/eco/11.htm (last visited on 2005.09.10)

由於網路技術的迅速發展，金融市場本身也開始出現創新。一方面，為滿足客戶全球交易的需求和網路世界的競爭新格局，金融市場開始走向國際聯合，如 2000 年 4 月英國倫敦證券交易所、德國法蘭克福證券交易所宣佈合併[5]。另一方面，迫於競爭壓力，一些證券交易所開始轉型為上市公司，以便將股票資金以更富有創意的方式與其他的交易所、發行體、投資者及市場參與者建立策略合夥關係和聯盟。

(四) 合作監理

由於資訊技術的發展，使網路金融監理呈現自由化和國際合作兩方面的特點：一方面過去分業經營和防止壟斷等傳統金融監理政策被市場開放、業務整合和機構集團化的新模式所取代。另一方面，隨著在網路上進行的跨國界金融交易量越發巨大，一國的金融監理部門已無法完全控制本國的金融市場活動。因此，國際間的金融合作監理就成了網路金融時代的另一項特色。

[5] 建立泛歐證券市場之協議，由於電子、電信科技之發達打破了時空之障礙，企業爲達經濟規模之擴充迫使企業走向全球化之整合及合併，因此對資本市場有了更大的需求，於是八大歐洲證券交易所簽署的協議備忘錄確認了歐洲聯盟的長期目標，亦即爲歐洲的績優股創立一電子交易系統來集中交易，未來希望能將歐洲三百大上市公司的股票交易集中在一共同之電子委託畫面，並協調相關之法規及規範，期能以更低的成本、更有效率及便利之證券市場基礎建設，使得所有參與的國家均能自歐洲資本市場之發展中獲益。原本八家歐洲證券交易所希望成爲全球最大的證交所，但是因爲成本太高而作罷，以成立跨國的績優股單一交易系統取代原先方案。參見汪萬波，全球重要證券暨期貨市場之最新發展趨勢，http://w3.tse.com.tw/plan/essay/451/Wang.htm (last visited on 2005.09.10)

貳、電子金融業務

隨著電腦、網路、資訊技術的發展和日益融合，網際網路(Internet)已進入社會生活的各個領域和各個環節，無論是機關、單位還是家庭、個人，都可以通過其獲取網路資源，交換資訊。全新的電子商務是在網際網路的廣闊聯繫與傳統資訊技術系統的豐富資源相互結合背景下應運而生的一種相互關聯的動態商務活動，這種基於網際網路的電子商務給傳統的交易方式帶來了一場革命。通過在網上自由傳輸的一串串位元組，基於廣泛互聯和完全開放式平臺，網際網路實現了低成本、高效率的經營模式，包括各種金融業務。

一、電子商務

電子商務將參與商務活動的各方：商家、顧客、銀行或金融機構、信用卡公司或證券公司和政府等利用電腦網路統一的融入在電子商務中，全面實現線上交易的過程「電子化」。電子商務包括兩個基本環節，即：交易環節和支付結算環節，主要涉及的是企業及個人的對外交易部分，不可避免地要發生支付、結算和稅務等對外的財務往來業務，勢必要求企業與企業之間、企業與銀行之間能夠通過網路進行直接的轉帳、對帳、代收費等業務往來，而支付結算業務絕大多數是由金融專用網路完成的。因此，離開銀行，便無法完成網上交易的支付，從而也談不上真正的電子商務。是故，電子商務的應用普及必須有金融電子化作保證，即通過良好的網上支付與結算手段提供高質高效的電子化金融服務。資訊技術和網路為金融電子化創造了條件，電子銀行、電子錢包、電子付款以及智慧信用卡等已開始應用。但是，要真正發揮金融電子化對電子商務的保證作用，還需要建立完整的網

路電子支付系統，提供驗證、銀行轉帳對帳、電子證券、帳務管理、交易處理、代繳代付等全方位的金融服務和金融管理資訊系統。

二、電子支付

電子支付是指以商用電子化工具和各類電子貨幣為媒介，以電腦技術和通信技術為手段，通過電子資料儲存和傳遞的形式在電腦網路系統上實現資金的流通和支付。由於運作模式的不同，各種支付系統在安全性、風險性和支付效率等方面有著不同的特點。

三、電子金融與金流

金流主要乃處理電子商務中的付款機制，所傳遞的資料主要為消費者的付款資料，如何在便利及穩定性外亦兼顧消費者的付款權益，是金流機制中必須考量的重要技術。關於電子金流模式，詳述如下：

(一) 銀行轉帳

不論是網路銀行線上轉帳或是虛擬帳號 ATM 轉帳，均可降低消費者對於線上刷卡的疑慮。消費者轉帳的同時，商家通常能在第一時間收到款項，惟消費者一般須負擔跨行手續費支出。

1、網路銀行線上轉帳

目前為了匯款人的安全，網路轉帳不得轉帳到非約定帳號[6]。因此，消費者必須另外約定商家帳號，對於消費者而言並不方便。

2、虛擬帳號ATM轉帳[7]

---

[6] 爲配合行政院反詐騙措施，自九十四年六月一日起，對於金融卡『非約定轉帳每日限額由每日 10 萬元改爲 3 萬元』，但繳交水、電、瓦斯、稅款、電信、交通規費及罰鍰、學費等項目，不受 3 萬元限制。參見台北富邦銀行網站－發燒新聞，http://www.taipeifubon.com.tw/sub_html/news.htm(last visited on 2005.09.10)。

[7] 拜網路科技之賜，已有愈來愈多銀行設置網路虛擬 ATM，民眾只要進入相關銀行的網站，點選「網路 ATM」，就可如同操作一般實體 ATM 般，進行各種轉帳、查詢、繳款等交易，可以說是，除了電腦無法吐出鈔票外，各種實體 ATM 的功能一應俱全。目前已有 9 家銀行設置網路 ATM，但各銀行的命名不同，例如第一銀行稱爲「eATM 網

當消費者選擇以此種方式付款時，系統會自動產生一組交易帳號給消費者，消費者只需到任何一台ATM，或是採用任何轉帳方式，將交易款項轉入此組帳號，即可完成繳費動作，銀行可依虛擬帳號設定的銷帳 ID 回饋資料予商家憑以自動銷帳。

3、實際帳號ATM轉帳

網路店舖商家可提供實際銀行帳號，消費者只需到任何一台ATM，或是採用任何轉帳方式，將交易款項轉入此組帳號，即可完成繳費動作。款項可直接入帳，但是必須以人工處理，無法自動銷帳(圖表1)）。

圖表1：目前國內虛擬帳號與實際帳號之ATM轉帳成本比較表

轉帳類型成本類別	商家成本	消費者成本
虛擬帳號ATM 轉帳	● 依往來銀行或代收代付業者規定。	● 需支付17元轉帳費用。
實際帳號ATM 轉帳	● 0元	● 需支付17元轉帳費用。

資料整理：玉山銀行；2005年6月

(二) 郵局劃撥

網路商家可在郵局開立劃撥帳戶，待消費者下單購物之後，可使

路理財機」、國泰世華銀行稱爲「網路提款機 myATM」，其他銀行多直接稱爲「網路ATM」，即使名稱不同，均提供如同實體 ATM 的功能，但基於軟體設計的差異，在使用的便利性、親近性上，則有些許落差。何謂網路 ATM? 臺灣銀行解釋，就是結合「晶片金融卡」、「晶片讀卡機」，配合運用各銀行設置的網站，在網路上取得各項金融服務，項目包括餘額查詢、自行或跨行轉帳、約定或非約定帳戶轉帳，及網路購物、轉帳、繳款、投資等交易。事實上，過去已有許多銀行設置「網路銀行」的功能，但民眾向銀行申請網路銀行使用後，卻不時發生民眾個人資料外洩情形，導致接受度逐漸降低。去年(2004)在主管機關要求下，銀行積極換發晶片金融卡，正好配合提供另一個全新網路 ATM 機會。參見李靚慧，網路 ATM 繳款卡便利，自由電子報，http://www.libertytimes.com.tw/2005/new/apr/6/today-stock1.htm (last visited on 2005.09.10)

用郵局劃撥單將款項劃撥至指定的帳戶。受制於郵局的營業時間，此方式對消費者及商家而言便利性較不足。

(三) 貨到付款或便利商店取貨付款

所謂的「貨到付款」是由物流業者在配送商品時，順便向消費者收取款項的方式。目前，提供貨到付款服務的廠商以宅配業者及郵局為主，消費者亦可自行至便利商店取貨付款，惟此部分對商家除有延遲收款銷帳之不便外，還需考量可能產生之退貨、換貨成本。

(四) 信用卡刷卡

以往信用卡刷卡必須下載傳真信用卡刷卡資料的離線交易，現在愈趨普遍的線上信用卡交易，信用卡線上刷卡可說已成為B2C電子商務付款主流，在信用卡交易流程中會牽涉到的角色包括：

1、商人銀行(Merchant Bank)

也就是網店商人帳戶(Merchant Account，讓商店得以接受信用卡付款的銀行帳戶)所在地銀行。

2、帳務處理機構(Processor)

為商店處理刷卡交易相關業務者，可能是銀行，稱之為收單銀行(Acquiring Bank)，也可能是承包這項業務的經紀公司，稱之為獨立銷售團體(Independent Sales Organizations, ISO)，或商家服務供應商(Merchant Service Provider, MSP)。

3、信用卡交易網路(Credit Card Processing Network)

由威士卡(VISA)或萬事達卡 (MasterCard) 建立，連結商家銀行與收單銀行的網路。

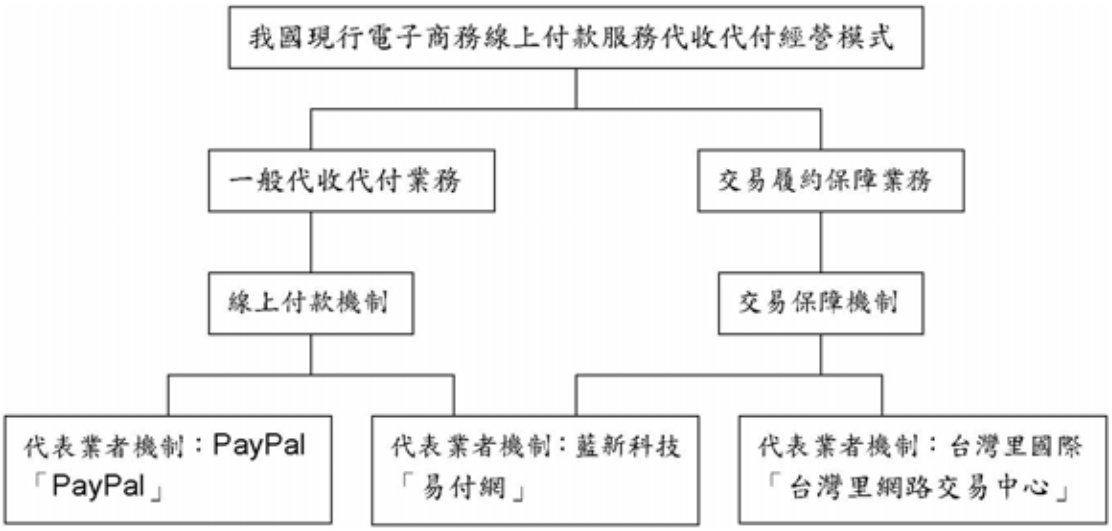
4、發卡銀行(Issuing Bank)

信用卡交易從過去強調安全模式的 SET 模式，在考慮商家與消費者的使用便利性後，逐漸以導入 SSL 模式居多，惟因 SSL 欠缺身

份驗證及不可否認性，導致網路上的盜刷及持卡人否認交易之情況頻傳，不僅造成消費者付款疑慮，而且依收單銀行規定，通常商家須承擔持卡人否認交易的風險，因此，如何加強信用卡交易安全，更是消費者及各方業者長久以來關心的課題。

(五) 代收代付業者興起

圖表 2：我國現行電子商務線上付款服務代收代付經營模式架構圖

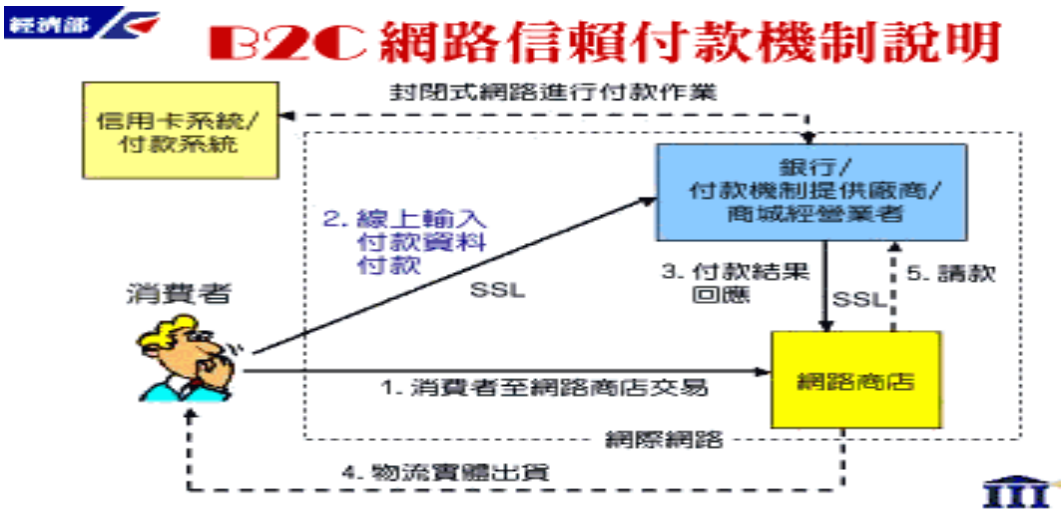


資料來源：經濟部「電子商務環境整備及企業對個人電子商務推動計畫」：線上付款服務之電子商務法制研究報告－線上代收代付經營模式法制研析；2004 年 5 月 www.ec.org.tw/doc/ 線上代收代付經營模式法制研析報告.pdf

昔時，欲進入電子商務市場的業者或個人，常受制網站建置成本而無法架設完善的購物金流機制，或是囿於金融體系對於資本額及營業額的審核，而無法申請金流服務，令其左支右絀；加上網路虛擬的特性，網路交易的風險及不確定性較其他實體交易高等因素，因此有許多網路經營業者認為金流的控管機制誠為實務上較不易處理的困難點。

代收代付業者在這種情形之下，以其資訊專長為網路商家建置整合、多元並客製化的付款機制，自然能得到中小型商家的認同，惟目

前我國並無法令規範此等新興商業模式。由於線上付款代收代付業務涉及金流之特性，儼然已成為特殊型態之金流機制，尤有甚者，國內代收代付業者台灣里網路交易中心[8]為取得消費者信賴，亦已發展B2C網路信賴付款機制。B2C網路信賴付款機制不同於其他線上付款方案，主要是以消費者的角度出發，其「付款頁」位於付款機制業者系統或網站，避免網路商店經手付款資料的方式，改善消費者所擔心的付款資料(如信用卡號、有效截止月年等)被盜取與濫用的問題。在使用上，消費者無須預先進行任何額外的申請或驗證作業，也不需改變原先銀行、商店及消費者(持卡人)之間的權利義務關係，並可適用於VISA、MasterCard等各種卡別之信用卡。對於網路商店而言，採用B2C網路信賴付款機制，可開拓擔心線上付款的消費者之潛在市場，同時也可避免持有信用卡卡號等付款資料的持有風險，此外網路信賴付款機制不僅與國際上各種新興付款機制(如Visa 3D Secure、儲值小額付款等)等完全相容，也可提早享受多種網路付款機制所帶來的網購便利。其運作架構如下圖：（參見台灣里網路交易中心：何謂信賴付款機制 http://www.twv.com.tw/trust.htm）



[8] 台灣里網路交易中心，http://www.twv.com.tw/a04.htm(last visited on 2005.09.10.)

四、電子支付的交易模式與安全性

在電子商務中無論採用哪一種付款工具，都必須具備以下幾個條件：安全性、處理成本低、且廣為全球金融市場所接受，而安全性是第一位的。所以，保證支付工具的真實與識別該使用者的合法身份就是金融業在網路環境下實現電子支付所面臨的問題。解決這一問題的關鍵是使用安全的電子支付模式，目前實現安全電子支付的主要模式包括：

(一) SSL 支付模式

1、SSL (Security Sockets Layer)

即安全通道層協議，主要用於提高應用程式之間的資料的安全係數，採用公開金鑰和私密金鑰兩種加密[9]：在建立連接過程中採用公開金鑰；在會話過程中使用私密金鑰。加密的類型和強度則在兩端之間建立連接的過程中判斷決定。它保證了客戶和伺服器間事務的安全性。

2、SSL 協議在運行過程中可分為六個階段：

(a) 建立連接階段：客戶通過網路向服務商打招呼，服務商回應；

(b) 交換密碼階段：客戶與服務商之間交換雙方認可的密碼；

(c) 會談密碼階段：客戶與服務商之間產生彼此交談的會談密碼；

(d) 檢驗階段：檢驗服務商取得的密碼；

[9] 公開金鑰加密法是採用兩把不同的金鑰，一把稱爲公開金鑰，另一把稱爲私密金鑰(Private Key)，意即公開金鑰爲公開對外，而私密金鑰則不可公開。在公開金鑰演算法中，以私密金鑰加密的資訊只能由相關的公開金鑰所解密，反之亦然。因此當某甲利用某乙的公開金鑰對訊息加密後，只有某乙可以利用其私人所有的私密金鑰將此訊息解密，因此可以保證某甲欲傳送給某乙的訊息只有某乙可以看到。反之，當某乙利用其唯一的私密金鑰對某個文件加密後，任何人都可以用某乙所公開的公開金鑰對此文件解密，因此可以確定此文件確爲某乙加密。公開金鑰的優點在於其安全性和鑑別性高；但是，由於公開金鑰演算法複雜度高，因此在非對稱式金鑰演算法其加解密速度比對稱式金鑰演算法要緩慢許多。故一般加密技術都將兩種金鑰技術合併使用。參見 PKI 與 Web Services Security 標準與應用研究，EC 研究報告，2003 年 6 月，http://www.nii.org.tw/cnt/info/Report/20030602.htm(last visited on 2005.09.10)。

(e) 客戶認證階段：驗證客戶的可信度；

(f) 結束階段：客戶與服務商之間相互交換結束資訊。

當上述動作完成之後，兩者之間的資料傳輸就以對方公鑰進行加密後再傳輸，另一方收到資料後以私鑰解密。即使盜竊者在網上取得加密的資料，如果沒有解密密鑰，也無法看到可讀的資料。在電子商務交易過程中，由於有銀行參與，按照 SSL 協定，客戶購買的資訊首先發往商家，商家再將資訊轉發銀行，銀行驗證客戶資訊的合法性後，通知商家付款成功，商家再通知客戶購買成功，將商品寄送客戶。

3、在 SSL 協定中主要提供三方面的服務：

(a) 認證用戶和伺服器，使得他們能夠確信資料將被發送到正確的客戶和伺服器上；

(b) 加密資料，以保證資料在傳送過程中的安全，即使資料被竊，盜竊者沒有解密密鑰也得不到可讀的資料；

(c) 維護資料的完整性，確保資料在傳送過程中不被改變。

4、SSL 協定的缺點：

首先，客戶的資訊先到商家，讓商家閱讀，這樣，客戶資料的安全性就得不到保證；其次，SSL 只能保證資料資訊傳遞的安全，而傳遞過程是否有人截取就無法保證了。所以，SSL 雖實現電子支付所要求的保密性、完整性，但是在信用卡卡號傳輸時卻可能遭攔截。

(二) SET 支付模式

1、簡介

SET (Secure Electronic Transaction) 即安全電子交易模式，是由 Visa[10]和 MasterCard[11]兩大信用卡組織提出的以信用卡為基礎的電子

[10] Visa, http://www.visa.com.tw/index.shtml (last visited on 2005.09.10)
[11] MasterCard, http://www.mastercard.com/tw (last visited on 2005.09.10)

付款系統規範，用來確保在開放網路上持卡交易的安全性。SET 規範使用了公開金鑰體系對通信雙方進行認證，利用 DES[12]、RC4 或任何標準對稱加密方法進行資訊的加密傳輸，並利用 Hash 演算法鑑別消息的真偽、有無篡改，以維護在任何開放網路上的個人金融資料的安全性。SET 體系中還有一個關鍵的認證機構 (CA，Certification Authority)，此機構根據 X.509 的標準發佈和管理證書。

SET 協定規定發給每個持卡人一個數字證書。客戶(持卡人)選擇一個口令，用該口令對數位證書和私鑰、信用卡號以及其他資訊加密存儲。這些與一個 SET 協定的軟體一起組成了一個「SET 電子錢夾」。

2、SET 協定的工作流程如下：

(a) 支付初始化請求和回應階段

當客戶決定要購買商家的商品並使用 SET 錢夾付錢時，商家伺服器上銷售時點系統(Point of Sale, POS)軟體發報文給客戶的瀏覽器 SET 錢夾付錢，SET 錢夾則要求客戶輸入口令然後與商家伺服器交換「握手資訊」，使客戶和商家相互確認，即客戶確認商家被授權可以接受信用卡，同時商家也確認客戶是一個合法的持卡人。

(b) 支付請求階段

客戶發一報文，包括訂單和支付命令。在訂單和支付命令中必須有客戶的數位簽名，同時利用雙重簽名技術保證商家看不到客戶的帳號資訊。只有位於商家開戶行的被稱為支付閘道的另外一個伺服器可以處理支付命令中的資訊。

(c) 授權請求階段

[12] DES (Data Encryption Standard) 密碼系統是美國早期 (1977) 的國家密碼標準，被美國工業界應用了 20 多年，鑰匙長度爲 56bits。參見 DES (Data Encryption Standard) 密碼系統，http://tw.knowledge.yahoo.com/question/?qid=1105053106410 (last visited on 2005.09.10)

商家收到訂單後，POS 組織一個授權請求報文，其中包括客戶的支付命令，發送給支付閘道。支付閘道是一個網際網路伺服器，是連接網際網路和銀行內部網路的介面。授權請求報文通過到達收單銀行後，收單銀行再到發卡銀行確認。

(d) 授權回應階段

收單銀行得到發卡銀行的批准後，通過支付閘道發給商家授權回應報文。

(e) 支付響應階段

商家發送購買響應報文給客戶，客戶記錄交易日誌備查。

在 SET 協定中，定義了五種實體：持卡人 — 擁有信用卡的消費者；商家 — 在 Internet 上提供商品或服務的商店；支付閘道 — 由金融機構或第三方控制，處理持卡人購買和商家支付的請求；收單行 (Acquirer) — 負責將持卡人的帳戶中資金轉入商家帳戶的金融機構；發卡行 — 負責向持卡人發放信用卡的金融機構。涉及 SET 交易的有持卡人、商家和支付閘道三個實體。認證機構需分別向持卡人、商家和支付閘道發出持卡人證書、商家證書和支付閘道證書。三者在傳輸資訊時，要加上發方的數位簽字，並用接收方的公開密鑰對資訊加密。實現商家無法獲得持卡人的信用卡資訊，銀行無法獲得持卡人的購物資訊，同時保證商家能收到貨款的 SET 支付的目標。

3、SET 協議在安全性方面主要解決五個問題：

(a) 保證資訊在 Internet 上安全傳輸，防止資料被駭客或內部人員竊取；

(b) 保證電子商務參與者資訊的相互隔離，客戶的資料加密或打包後通過商家到達銀行，但是商家不能看到客戶的帳戶和密碼資訊；

(c) 解決多方認證問題，不僅要對消費者的信用卡認證，而且要對線上商店的信譽程度認證，同時還有消費者、線上商店與銀行間的認證；

(d) 保證網上交易的即時性，使所有的支付過程都是線上的；

(e) 仿效 EDI 貿易的形式，規範協定和消息格式，促使不同廠家按照一定的規範開發軟體，使其具有相容性和互操作功能，並且可以運行在不同的硬體和作業系統平臺上。

4、SET 協議的缺陷

自 1996 年 4 月 SET 協議面市以來，得到了 IBM、HP、Microsoft、Netscape、VeriFone、GET、Verisign 等許多大公司的支持，促進了 SET 的發展。但 SET 仍然存在一些問題：

(a) 只適用於客戶已安裝「電子錢夾」的場合；

(b) 使用成本高：在一個典型的 SET 交易過程中，整個交易過程可能需花費 1.5 分鐘至 2 分鐘；

(c) 協議複雜：SET 證書雖也遵循 X.509 標準，但格式比較特殊。

(三) 3D Secure

3D-Secure 的模式是改良 SET 在推廣及運用上之不便，所衍生出來的機制，重新把現行網路信用卡交易架構區分為發卡銀行區域(Issuer Domain)、收單銀行區域(Acquirer Domain)和跨作業系統區域(Interoperability Domain)即 3D-Secure (3-Domain Model)。

發卡銀行區域：管理、核對登記的持卡人身分，並且在網路購物時進行持卡人身分之鑑定。

收單銀行區域：確保參與網路交易的商店是在與收單銀行簽訂的協議書規定進行，同時為身分鑑別之易提供驗證。

跨作業系統區域：建構共同的通訊協定及服務來促成各收單銀行區域和各發卡銀行區域兩者的資訊交換。

在這種安全交易架構，3D Secure 系統包含了編碼技術、邏輯通行管制、實體資料保護及網路安全，此機制對持卡人來說，就是其在網路特約商店進行線上刷卡購物時，除了原先需填寫的信用卡卡號及到期日外，還必須加填一組持卡者自設的安全密碼，才能獲得授權。其隱私與交易安全可以得到保障，並可有效整合持卡人的資訊，能大大減少網路偽卡盜刷及交易糾紛問題，以確保交易的安全性，進而提升持卡人對網路交易的信心。基於 3D Secure 標準，VISA 推出了 Visa 驗證服務(Verified by VISA)。其操作平臺能夠透過網路經遠端登入，及時確保參與網路交易的 VISA 持卡人與網路特商店獲得銀行授權，也能夠保護 VISA 持卡人進行網路交易時所輸入的資訊不會在網路傳輸過程中被攔截或產生任何變動[13]。

（四）晶片金融卡

鑒於磁條卡保密安全機制不足，較易被側錄偽造[14]；且受其原始設計功能所限，無法成為新興業務模式之有效支付工具。銀行公會爰以國際趨勢(目前世界各國紛紛改採晶片卡的國家包括新加坡、韓國、香港、馬來西亞、德國、比利時、挪威、芬蘭等)，依據民國 90 年 2 月 5 日「金融業務電子化委員會第六十一次會議」之決議事項，成立「磁條金融卡晶片化」專案暨工作小組，負責評估金融卡晶片化

[13] 線上付款新機制-(3D Secure), http://promotion.ezpay.com.tw/epaper/041007/20041007.htm (last visited on 2005.11.10)

[14] 我國磁條金融卡累計發卡量近 8,000 萬張，其中流通卡數約爲 6,000 餘萬張。傳統的磁條金融卡密碼防範應無問題，缺點是在磁條資料爲明碼傳輸，加上磁條資料複製容易，因而引起不肖之徒躍躍欲試。

作業執行方案及研提跨行共用規範，供主管機關和各金融機構據以辦理[15]。

晶片金融卡係由金融機構將持卡人之金融帳戶相關資料，由原本存放在磁條內改為存放在晶片上，除提高交易之安全，可運用卡片業務範圍亦增加；另在卡片背面會顯示跨行交易之金色金框之標誌。一般而言，晶片金融卡大小尺寸與外型與目前磁條金融卡相同，惟最大差異在於卡片正面上左方嵌入一個外觀呈現金色的「晶片」。晶片金融卡具有與原磁條卡相同功能[16]，且具有資料儲存、保護、權限控管與密碼學邏輯運算能力等特性，具有較高安控機制。

晶片金融卡在交易安全設計上，解決現行磁條金融卡被盜錄危機，晶片卡持卡人之密碼儲存於晶片中無法盜錄，而身分識別改於端末設備以離線方式完成檢核持卡人密碼。持卡人密碼通過後，其交易訊息附加由晶片卡產製之交易驗證碼或簽章，再經由端末設備、代理機構及財金資訊股份有限公司等(各節點均有押解碼)，將訊息原封不動轉送給發卡行，由發卡行檢核驗證碼或簽章，就可判斷持卡人之合法性，決定是否同意交易之進行，訊息傳輸過程，不再需要傳輸密碼資料。

---

[15] 財金資訊股份有限公司，http://www2.fisc.com.tw/dev_biz/combocard-1.asp(last visted on 2005.11.20)。

[16] 晶片金融卡包括：(1) 國內交易功能－提款、轉帳、繳費(稅)、查詢等基本交易功能。(2)國外交易功能－可利用磁條密碼及功能至國外貼有 VISA Plus 標誌之 ATM 提領外幣現金。(3) 新增功能－如：購貨、退貨、預先授權、授權完成交易等功能，補足電子商務上金流通路不足的問題。附加功能上可結合國際組織晶片金融卡之卡片業務、具企業儲值及消費(Online/Offline)交易功能、具動態密碼(On Time Password)應用功能、具結合銀行公會 FXML 憑證晶片卡功能。除了跨行交易已規劃共同之功能外，晶片金融卡因有大量的記憶儲存空間，發卡行可以定義晶片金融卡自行的其它交易種類與功能，進行更多自行加值之服務，例如動態性密碼(One Time Password)、自行規劃之交易功能、驗證碼或簽章之應用、企業聯名卡、紅利積點卡(或儲值卡)、員工卡或校園卡等之組合運用，提高自行之多樣化加值服務，進行差異化行銷，滿足客戶之各類需求，共創雙贏之局面。除以上功能外，亦可與國際組織之卡片業務及企業之儲值卡功能結合使用，但須進行約定功能。

整個交易安全設計，係由晶片卡與發卡行(End To End)決定，即發卡行決定卡片之密碼邏輯與基碼長度，與其他交易過程處理節點無關，故即使不法者從中盜錄交易資料，也無法製造偽卡，產製假交易；有效解決訊息在網路間傳遞與被盜錄之風險，防止磁條卡側錄盜用情事[17]。

在此交易安全機制之下，身分及交易識別功能由晶片卡及發卡行負責，故內含讀卡機之端末設備，例如個人電腦、轉帳繳款櫃員機(Kiosk)、Point -Of -Sale (POS)機、內含讀卡機之行動電話或個人數位助理(Personal Digital Assistant, PDA)等，只要代理行(收單行)允許連接，皆可以進行相關之交易，並不限於目前之自動提款機上。

在應用實例上，包括：(1) 網路 ATM 應用 － 晶片金融卡可在虛擬通路進行轉帳、購物付款、繳(費)稅。(2)中華電信 MOD 應用 － 晶片金融卡可透過 MOD 進行轉帳、購物付費等。(3) 企業儲值卡之應用 － 晶片金融卡可作為商家小額付款工具。(4) 結合行動電話 JAVA SIM 應用 － 晶片金融卡與行動電話結合，作為行動付款交易工具。金融控股公司法開放後，銀行業除了彼此的競爭外，更增加了各種金融業的競爭，如何緊密地結合銀行體系與異業結盟更形重要。現今銀行利用各種聯名卡來與異業結盟，但其缺點是一張聯名卡只能與某一異業來合作。而晶片金融卡不只可容納多量異業結盟所需資料，更可以即時做應用下載至晶片上，省卻換卡/重製及寄送的成本。銀行金融體系下的各項金融產品當然更可以自由地搭載於晶片金融卡及 ATM 上，進行更進一步的交叉行銷(Cross Selling)[18]。不只如此，

[17] 財金資訊股份有限公司，另一次金流通路革命晶片金融卡讓銀行服務加值，http://www2.fisc.com.tw/dev_biz/combocard-4.asp(last visted on 2005.11.20)。

[18] 茲以壽險公司之保單貸款爲例，對於有付款需求之企業，可透過金融機構既有通用型作業平台之跨行共用機制，提供持卡人(保戶)金融交易及保單貸款服務。由於晶片金融卡本身未設計任何業務欄位，因此壽險公司可與金融機構合作，由企業本身或金融機構

銀行及結盟業者更可以導入客戶忠誠度回饋機制(Loyalty Program)，針對客戶的 ATM 交易，產品購買次數與金額做資料的登錄與分析，進而提供更優厚的回饋計畫[19]。

(五) 小結

SSL 協定是國際上最早應用於電子商務的一種網路安全協定，在一些發達國家有許多網上商店至今仍然在使用。在美國幾乎所有提供安全交易的線上網址都依靠網景公司的安全套接層(SSL)提供安全交易，SSL 保護使用公用密鑰編碼方案傳輸的資料。幾乎無人否認，SSL 在限制電子竊聽方面很有效。相比之下，SET 標準則是於消費者、商家和銀行三方進行網上交易的國際安全標準。網上銀行採用 SET，確保交易各方身份的合法性和交易的「不可否認性」，使商家只能得到消費者的訂購資訊而銀行只能獲得有關支付資訊，加上 3D Secure 技術的改進，確保交易資料的安全、完整和可靠，為消費者提供一個快捷、方便、安全的線上購物環境。而國內目前推行的晶片金融卡，可謂已結合數位簽章認證及未來可能相容辨識技術的新模式，對於確保交易安全與防止帳號密碼遭攔截等，提供不錯的防制措施。

五、電子支付工具

國際通行的電子支付工具和支付手段主要有電子信用卡、電子支票、電子現金、及網路銀行等。

發卡，晶片卡之發卡機構代號欄位則以合作金融機構之代號爲主，卡號由壽險公司與金融機構協議訂定之，或於卡片備註欄內註明。則持卡人(保戶)可持晶片金融卡至 ATM 選擇提款交易，交易訊息經跨行系統傳送至合作金融機構後，金融機構向壽險公司請求授權，壽險公司經審核持卡人保單相關資訊及額度後，授權合作金融機構通知代理機構付款並完成交易，使持卡人(保戶)可由便利之管道取得貸款；或亦可透過轉帳等其他交易達成。參見財金資訊股份有限公司，二十一世紀主流支付工具晶片金融卡之功能與應用，http://www2.fisc.com.tw/dev_biz/combocard-4.asp#d(last visted on 2005.11.20)。

[19] 財金資訊股份有限公司，晶片金融卡於銀行 ATM 上的應用，http://www2.fisc.com.tw/dev_biz/combocard-4.asp#b(last visted on 2005.11.20)。

(一) 電子信用卡

信用卡支付是電子支付中最常用的工具，信用卡可以在商場、飯店、車站等許多場所使用。可採用刷卡記帳、POS 結帳、ATM 提取現金等方式進行支付。在電子商務中最簡單的形式是讓用戶提前在某一公司登記一個信用卡號碼和口令，當用戶通過網路在該公司購物時，用戶只需將口令傳送到該公司，購物完成後，用戶會收到一個確認的電子郵件，詢問購買是否有效。若用戶對電子郵件回答有效時，公司就會從用戶的信用卡帳戶上記錄這筆交易的費用。

隨著技術的發展，信用卡的卡片由磁條發展為能夠讀寫大量資料、更加安全可靠的智慧卡，稱之為電子信用卡。電子信用卡也可以說是一種基於 WWW 瀏覽器或與流覽器結合的電子支付工具，它可以顯示使用者的餘額，並且在相互認可的情況下，進行劃撥資金。有一些電子信用卡或智慧卡還可以進行無線資料通訊，使電子支付更具生命力。

(二) 電子支票(Electronic Check, e-Check)

電子支票是利用數位化手段，用數位化資訊徹底取代實體支票。實質上，電子支票的支付過程與傳統支票的支付過程是一致的，只是電子支票完全拋開紙質的媒介，其支票的形式是通過網路傳播，顯現在電子螢幕上，並用數位簽名代替傳統的簽名方式。現在，歐美國家實體支票的使用已經逐步減少[20]，一方面是因為實體支票的處理成本較高[21]，支付速度慢；另一方面，由於資訊安全技術的應用使實

[20] 2003 年二月，美國聯邦準備銀行金融服務政策委員會主席 Cathy Minehan 宣布，爲因應美國支票使用數量的縮減，美國境內的隸屬聯邦準備銀行的支票交換處理中心，將於兩年內逐步的從原來的 45 個據點縮減爲 32 個據點。在歐洲，英國因大力投資電子支付機制，轉帳卡與信用卡在過去十年間，年平均成長率達 27%，十年成長率達 241%，因此支票使用量每年降幅約 3.5%，同期間總降幅達 31%。參見劉容志，未來的支付系統主流—電子支票: 談支票系統之演進與發展趨勢，財金資訊第 28 期(2003.06)，頁 5。

[21] 據 2001 年美國之統計，每張支票的平均處理成本爲 1.25 美元，整體處理成本近五百

體支票轉化為電子支票成為可能。1996 年美國金融服務技術財團研製出的電子支票交易系統現在仍在廣泛使用。2002 年新加坡開發了亞洲第一大電子支票系統，此外，Netbill[22]和 Netcheque[23]等電子支票系統也在試用當中。將來電子支票的應用將會更加廣泛。

我國中央銀行為解決電子商務金流問題，提昇全國支付系統效率，滿足企業交易多元化需求，特於民國 89 年 12 月提出「發展電子支票計劃」，報請行政院經建會核定為「知識經濟發展方案具體執行計劃」之一，責由台灣票據交換所執行研發事宜，並與財政部、經濟部、銀行公會及數家銀行代表，共同規劃、建構電子票據各項業務規範與系統機制。

電子票據係指以電子方式製成之票據，以電子簽章取代實體之簽名蓋章，包括：指定受款人且劃平行線之電子支票、委託金融業擔當付款之電子本票及金融業者付款之電子匯票。「發展電子支票計畫」專案，為應實際業務需要，已將發展計劃範圍擴大，除支票(限指定受款人且劃平行線之支票)外，尚包括「銀行擔當付款本票」、「銀行承兌匯票」等兩類，均為交換所交換清算之票據，統稱「電子票據」。電子支票上，包含票據應載事項及簽章部分之說明。應載事項包括：(1) 電子票據應記載之事項與實體票據相同；(2)受款人之欄位不得空白，並以記載受款人身分識別碼為之；(3)加註電子信箱號碼；(4) 以單一受款人為限；以及(5) 該受款人之身分識別碼得以指定受款人收

億美元，見前註。

[22] NetBillis designed to support very low-cost transactions involving electronic goods. One central and distinguished claim of the NetBill protocol is that it satisfies goods atomicity, and this will be the focus of our analysis. In NetBill, all money-related activities are centralized at the bank and take the form of transfers between accounts; consequently, arguing money atomicity is straightforward. See Netbill, http://www.usenix.org/publications/library/proceedings/ec96/full_papers/wong/html/node5.html (last visited on 2005.09.10)。

[23] See Netcheque，http://gost.isi.edu/info/NetCheque/ (last visited on 2005.09.10)。

款行帳號代之。在簽章部分，電子票據之簽章，應以數位簽章為之。[24]

電子票據的使用，具有保障資料安全、使用方便、提昇支付效率[25]及具備法律保障等特點。在保障資料安全方面，電子支票採取了「集中登錄保管制度[26]」，用以防範電子文件遭受複製影響票據權利人之權益，即保障票據權利人之唯一性。另外由於使用 PKI (Public Key Infrastructure)機制，加上統一採用銀行商業同業公會全國聯合會訂定之電子安控憑證規格。可防止冒名傳送假資料、防止資料內容被竄改、防止當事人否認傳送資料，並確保資料隱密性。在法律保障方面，依據「電子簽章法」第四條第二項及第九條第一項之規定，並以「票據法」為法源依據，訂定「金融業者參加電子票據交換規約」(訂定參加電子票據交換之金融業者與交換所間之作業規範)與「電子票據往來約定書(範本)」(訂定參加電子票據交換之金融業者與其存戶間之業務規範)。截至民國 93 年 12 月 31 日止，辦理電子票據業務之大型商業銀行有九家。不過實際運用的普遍性情況仍有待觀察，蓋由於國人多係在企業對企業間進行傳統的票據交易，個人使用支票的習慣與國外相比，並不普遍。

---

[24] 參見台灣票據交換所-電子票據，http://www.twnch.org.tw/echeck/(last visited on 2005.11.10)。

[25] 在使用方便性方面，使用者只要具備一般可上網的電腦及憑證載具與讀取憑證設備即可使用電子票據。可與企業內部資源規劃作業系統(ERP)整合，透過與應付帳款(A/P)、應收帳款(A/R)之連動，可自動簽發應付票據或處理應收票據。可利用附件檔，攜帶傳票或發票資料，方便勾稽票據、發票或訂單。經辦或稽核人員可透過瀏覽器或其 ERP 系統，進行電子票據查詢或複核。另在提升支付效率方面，透過電子票據，可以節省繁複人工作業。也減少空白票據遺失顧慮及掛失止付問題，並可進行跨區交換。見前註。

[26] 所謂「集中登錄保管制度」，係指發票人簽發電子票據，經付款行驗符其委託付款之識別碼後，由付款行傳送台灣票據交換所保管，該票據之背書轉讓、融資、取消融資、存入託收、撤票、撤銷付款委託、取消撤銷付款委託、退回、作廢、贖回(退票後退回發票人、退票後轉讓發票人)、提示交換、退票交換及受司法及行政機關所發之執行命令等登錄，皆經由交換所處理。見前註。

美國在進行電子支票的計畫外，另一種解決傳統支票交換的計畫為「影像交換(Image Truncation)」。所謂「影像交換」是指客戶使用支票，商家存入銀行後，收票行不再把實體支票送達票交所，而是將支票正反兩面掃描成影像檔，再加上發票人與收票人之帳戶號碼、日期與金額等票面記載訊息，以電子檔之格式經由網路送至票據交換所，執行交換，並再轉送回發票行，票交所或發票行經適當的授權後，可根據影像檔重印該支票，此既所謂「替代支票(Substitute Check)」，它可以代替原始憑證，送交需要存留該支票之銀行或客戶。「影像交換」在技術上已完全成熟，但在法令上，支票影像檔如果未被授予有如同傳統支票般的憑證地位，票據交換所將不能執行交換。因而聯邦準備銀行(Federal Reserve Bank, FRB)著手推動「21 世紀支票交換法案(Check Truncation Act) 」，簡稱 「Check 21」法案，並於 2003 年 10 月通過，2004 年 10 月實施。藉由該法，可以解決支票電子影像檔的憑證地位，並建立影像交換的保護機制下的清算作業，避免善意第三者因交換處理偶發錯誤而造成損失[27]。

(三) 電子現金(e-Cash)

電子現金，又稱為數位現金。簡單來說，就是以電子方式存在的貨幣現金。實質上代表一定價值的數位呈現，或者說電子現金就是實體現金的電子化，因此電子現金同時擁有現金和電子化兩者的優點。目前，比較有影響的電子現金系統有 E-cash[28]，Netcash[29]，Cybercoin[30]，

[27] 不過該法的通過與實行，並未對消費者提供一種完整的保障，原因在於該法的內容中並未真對消費者的隱私權保障有任何規定，更且甚者，雖然在法律上，替代支票與傳統紙本支票在法律上之效力相等(legal equivalent)，但是在舉證鑑定上，卻無法從替代支票上測出筆壓(pen pressure)或是筆跡鑑定(handwriting analysis)。參見 Consumer Union Opposes the Check Truncation Act, http://www.consumersunion.org/finance/checkwc102 (last visited on 2005.11.10)。

[28] ECash is a computer generated system which allows items to be purchased by credit card.，參見 ECash，http://www.ecash.com/ (last visited on 2005.09.10)。

[29] NetCash will enable new types of services on the Internet by providing a real-time electronic payment system that satisfies the diverse requirements of service providers and

Mondex[31]和 EMV[32] (Europay, MasterCard, VISA)現金卡等。電子現金具有人們手持現金的基本特點，同時又具有網路化的方便性、安全性、秘密性。因此，電子現金必將成為網上支付的主要手段之一。

(四) 網路銀行

網路銀行是指利用網際網路和網際網路技術，為客戶提供綜合、統一、安全、即時的銀行服務，包括提供私人和公家機構的個人或團體的全方位的銀行業務，還可以為客戶提供跨國支付和結算等其他貿易、非貿易的銀行服務。自從 1995 年 10 月，美國的安全第一網路銀行 SFNB (Security First Network Bank)[33] 誕生以來，網路銀行已經成為金融機構拓寬領域，爭取業務增長的重要手段，網路銀行的範圍涉及到電子支票兌付、線上交易登記、支票轉帳等幾乎全部的金融業務。

---

their users. Among the properties of the NetCash framework are: security, anonymity, scalability, acceptability, and interoperability. 參見 NetCheque，http://gost.isi.edu/info/netcash/ (last visited on 2005.09.10)。

[30] Cybercoin，Cybercoin - Computer-Lexikon, Glossar, Wörterbuch - Informationsarchiv.net. http://www.informationsarchiv.net/clexid_436.shtml (last visited on 2005.09.10)。

[31] Mondex 即是電子現金，它的主要用途在於取代日常小額消費的鈔票及硬幣。Mondex 卡擁有現金的特性，例如：人與人之間的轉值；人與商家的轉值；人對銀行的提款轉帳等功能。此外，Mondex 卡還有一個比現金更優良的特點，即是它能安全地通過電子管道 (如：電話、網際網路等) 來作人對人、人對商家、人對銀行的遠距轉值。參見 什麼是 Mondex？，關於宏碁－最新消息，http://global.acer.com/t_chinese/about/news.asp?id=368(last visited on 2005.09.10)。

[32] EMV 爲 Europay、MasterCard 及 VISA 三大國際組織就付款系統 (Payment System) 所制定之晶片卡相關規格，此三大組織於 1999 年 2 月共同成立之 EMVCo 組織，主要任務便維護 EMV 付款晶片卡標準，並確保該標準在世界上之互通性與於付款環境之可用性。EMV 規格原爲 EMV 96 Version 3.1.1，EMVCo 組織於 2000 年 12 月公告 EMV 2000 Version 4.0，2004 年 5 月再公告 4.1 版。 參見 EMV，財金資訊股份有限公司，http://www2.fisc.com.tw/share/security-4.asp (last visited on 2005.09.10)))

[33] 〈Security First Network Bank (SFNB)〉「安全第一網絡銀行」(Security First Network Bank 簡稱 SFNB)是全世界的第一家網路虛擬銀行(virtual bank)，於 1995 年 10 月 18 日開業。銀行所提供的日常服務諸如存款、支付和轉帳、信用卡等等，完全是在網際網路上運作，而 SFNB 除了在亞特蘭大設有總部以外，並沒有任何的分行。

隨著資訊通訊科技(Information ＆Communication Technology, ICT)之日新月異，電子商務(Electronic Commerce)[34]。為協助產業運用電子化技術參與電子商務，發展台灣成為全球高附加價值產品製造及服務中心，行政院國家資訊通信發展推動方案(National Information & Communication Initiative，簡稱「NICI 方案」)，推動方向與策略之一係以建置產業金流自動化作業系統，強化資金移轉及支付效率，具體措施包括如建立金融機構與產業間金流電子化作業系統，建置跨行支付平台，推動建置網路銀行，結合各類型加值網路服務，推動供應鏈電子化金流作業，強化金流服務管道，以及建構電子支票交換機制，提昇工商業支付效率等[35]。

[34] 廣義的電子商務定義係指「結合資訊科技與各種通訊技術，並透過電腦間連線以電子化方式從事各種商業活動」，故企業運用資訊科技改善經營方式(如企業資源管理系統(Enterprise Resource Planning, ERP)、供應鏈管理系統(Supply Chain Management, SCM)、電子市集(e-Marketplace) 等均屬之。另參考美國商務部所公布的電子商務白皮書(1997年)，概分電子商務爲兩大類：企業間(Business to Business, B2B) 與企業與消費者間(Business to Consumer, B2C) 電子商務，復依電子商務可能的應用領域，尚可包括政府與企業(Government to Business, G2B)、政府與民眾間(Government to Civil, G2C)、消費者間(Consumer to Consumer, C2C)等。除本文另有說明外，係採廣義電子商務定義與上述分類方式。

[35] 其他具體措施建議包括：推動各金融機構建置金融電子資料交換(FEDI)系統；配合經濟部推動宣導電子簽章法之宣導會，務必使所有業者或客戶瞭解電子簽章法；請經濟部儘速制訂相關施行細則,公告憑證機構名單，提供金融業者參考採用；協調票據交換所電子支票憑證採用金融業標準；應用政府研發經費,加速金融電子商務推動。參閱行政院NICI，90 年產業自動化暨電子化會議金融業分組總結報告，2001 年 11 月 2 日。

參、網路銀行

一、制度特色與發展前景

(一) 業務智慧化、虛擬化

傳統銀行，其分行是物理網路，主要借助於物質資本，通過眾多銀行員工辛苦勞動為客戶提供服務。而網路銀行沒有建築物、沒有地址，只有網址，其分行是終端機和網際網路帶來的虛擬化的電子空間，主要借助智慧資本，客戶無須銀行工作人員的幫助，可以自己在短時間內完成帳戶查詢、資金轉帳、現金存取等銀行業務，即可自助式地獲得網路銀行高質、快速、準確、方便的服務。

(二) 服務個性化

傳統銀行一般是單方面開發業務品種，向客戶推銷產品和服務，客戶只能在規定的業務範圍內選擇自己需要的銀行服務，而網際網路向銀行服務提供了互動式的溝通管道，客戶可以在訪問網路銀行站點時提出具體的服務要求，網路銀行與客戶之間採用一對一金融解決方案，使金融機構在於客戶的互動中，實行有特色、有針對性的服務，通過主動服務贏得客戶。

(三) 金融業務創新的平臺

傳統銀行的業務創新主要圍繞資產業務，針對商業銀行的資產負債業務，進行資產證券化，對金融產品進行改造與組合，滿足客戶和銀行新的需求，而網路銀行側重於利用其成本低廉的優勢和網際網路豐富的資訊資源，對金融資訊提供企業資信評估，公司個人理財顧問、專家投資分析等業務進行創新和完善，提高資訊的附加價值，強化銀行資訊仲介職能。

隨著網路整體水準的提高和綜合實力的增強，網路對國民經濟增長的貢獻會不斷提高，將成為一個行業，成為金融業發展的一種趨勢，今後網路銀行發展的潛力很大，市場前景廣闊。其未來發展包括：

(一) 產業金融與網路結合的趨勢將會加強

隨著人們思想觀念的轉變，傳統工作方式的更替，資本市場的發展，直接融資比例的提高，大批企業將會設立自己的網站網頁，消費者也會積極投身於網路銀行之中，網路企業的擴展，網路消費者的增加，使眾多的網路企業從開展電子商務轉而向網路銀行結合相互持股，大企業集團將與傳統銀行合作共同建立網路銀行，提高網路金融服務業務，產業金融網路化結合將使眾多企業和消費者對網路金融信任度提高、對網路平臺的依賴性增強，網路用戶端群將穩定發展，網路銀行的經濟效益會顯著提高。

(二) 網路銀行業務將向多樣化、創新化發展

網路銀行的出現，使傳統銀行經受一場技術革命，傳統銀行業務將受到挑戰，網路銀行具有靈活強大的業務創新能力，不僅可延伸改造傳統的業務，而且會不斷設計業務新品種，創新業務方式，滿足客戶多樣化的需求，網路銀行利用現代金融技術，大力開展網上交易，網上支付和清單業務，拓寬業務範圍、增加業務收入，利用網路銀行為企業和居民進行資金餘額查詢、帳戶轉移，銀行業務通知等基本業務服務，並利用網際網路作為行銷管道，交叉出售產品和服務，如存款產品、消費信貸、保險、股票交易、資金託管等高級業務，且不斷進行升級換代，拓寬技術創新空間和領域。

(三) 網路銀行業務的創新將會推動金融市場網路化發展，並可能再現綜合性市場

隨著網路銀行業務的深入開展，迫切需求外匯市場、黃金市場、資本市場、貨幣市場、保險市場及金融衍生產品市場網路化長足發展；反過來，這些市場網路化的發展也能提升和促進網路銀行的進一步發展。網路金融市場的地區整合和行業互動將會帶動整個金融市場深化網路金融市場和非金融市場之間界限模糊，距離縮短，各類市場將混為一體，並且可能出現綜合性市場。

(四) 網路銀行全球化、國際化發展趨勢明顯

隨著經濟全球化和金融國際化發展腳步的加快，世界各國銀行業運用併購重組方式積極向海外擴張，採取多種途徑、方式擴展業務，佔領世界市場。

二、他山之石

(一) 網路銀行的發源地 － 美國

1995 年 10 月 18 日，全球第一家純網路銀行 － 安全第一網路銀行(Security First Bank)在美國誕生，它代表著銀行界一個新的革命崛起。客戶不論身在何處，只要有一個電腦屏與網際網路介面，輸入該行的網址就可以享受該行的「24 × 7」服務 (每週 7 天，每天 24 小時)。服務專案涉及開戶、存款、轉帳、申請信用卡、申辦貸款、購買保險及進行金融投資的買賣等，用戶如需提取現金，用該行的信用卡到附近的 ATM 上提款即可。隨後，資產達 1,000 億美元的舊金山市威爾士．法戈銀行(Wells Fargo)集團也開辦了網路銀行。Wells Fargo 通過一種發達的室內系統提供網路銀行服務，從開業到 1998 年 6 月，其線上用戶從 2 萬膨脹到 45 萬。一些專門為會員提供金融服務的信用協會也不甘落後，相比於銀行必須注重乾淨利潤而言，信用協會著眼於更好地為會員服務，因而更易於採用新技術，擁有 303

名會員及 14 億美元資產的聖安東尼奧地區的安全服務聯邦信用協會從 1997 年 2 月起，提供基於網際網路的家庭銀行業務，會員們通過 IE 或 Netscape，就可以與協會的網站相連接。同時，一些資產小於 25 億美元的社區銀行也發現，網路是其實現行銷管道多元化的良好工具，並相繼採取各種方式提供網路銀行業務，以加深顧客的忠誠度。

(二) 歐洲國家

在歐洲，英國和瑞士先行發展網路銀行，如英國的 Barclay Bank 宣佈將關閉 50 家分行，用此資金來發展網路銀行業務，國民西敏寺銀行也表示將在投資 1 億英鎊以發展網路銀行業務。瑞典的 SEB 和荷蘭銀行則通過網路銀行進行跨國兼併收購，這樣既避開了各國政府對外國財團收購本國銀行設下的重重障礙，又避免了合併後機構和分行重疊等問題，且成本相對低廉。摩根史坦利的報告將網路銀行稱之為「馬提尼銀行」，因為馬提尼酒的口號是：隨時、隨地、隨意，網路銀行爆炸性的增長將迫使歐洲傳統銀行大幅削減支出以保持贏利。在未來的 3 年中，歐洲的網路銀行數量將是現在的 3 倍，歐洲的網路銀行將從原有的 20 家增長到 55 家。線上金融服務的金額將達到 4,400 億歐元，占金融市場的 15％。到 2003 年，網路銀行業務在瑞典將佔有最大的占有率，約 50％，其次是瑞士，占 36％。第三是德國，占 25％。根據 Forrester Research 的數據則顯示，歐洲網路銀行的使用人口，已經超過 6,000 萬，等於每 5 個歐洲人就有 1 人使用。[36]

(三) 日本

面對洶湧而來的世界網路經濟的浪潮，日本經濟界人士普遍感到了危機。他們普遍認為，日本在網路經濟方面至少落後美國三至五

[36] E 天下網站--連 SONY 也開網路銀行，
http://www.techvantage.com.tw/content/040/040150.asp (last visited on 2005.09.10)。

年，這與號稱世界第二經濟大國的地位極不相稱，因此下決心將醞釀已久的網路銀行儘快實踐。

2000 年 9 月 7 日，日本金融再生委員會(FRC)在會議上決定，頒發准經營許可證給正在籌備中的網路專業銀行「日本網路銀行」(日本網路銀行以櫻花銀行為主體)。至此，日本首家網路銀行宣告誕生。並於 10 月份正式營業。此家網路銀行將被命名為 Japan Net Bank，50％的股份將由櫻花銀行所持有，而住有銀行、富士通及日本生命保險則將各持 10％的股份。而剩餘的 20％股份則將由 NTT 東日本，NTT DoCoMo，三井物產及東京電力平均持有，此家網路銀行亦成為首家旗下股東成員包含非金融機構的銀行。2001 年 4 月，新力就正式成立線上金融機構「新力銀行」（Sony Bank），是繼 2000 年 10 月成立的日本網絡（Japan Net）後，日本出現的第二家網路銀行。新力銀行的總資本金為 375 億日圓（約新台幣 118 億元），新力出資 80％，其餘由櫻花銀行、JP 摩根各出資 16％和 4％。新力銀行並不設實體營業所，而是以網路和 ATM 櫃員機作為服務媒介，因此經營費用大幅降低，並可把節省下來的經費作為提高存款利率之用。新力銀行提供了存款、投資信託、小額貸款、轉帳等服務，以個人為主要服務對象，並不接受企業用戶。用戶在線上開戶之後，主要服務界面稱為「Money Kit」，共有 22 種服務工具，只要輸入個人帳號與密碼即可使用。除了存款、查詢餘額、交易詳細說明等一般功能之外，還可設定結婚、生小孩等時間軸，由銀行幫忙做個人化的財務規劃。

三、交易模式的發展

網路銀行的發展模式將被分為：大銀行發展模式、社區銀行發展模式和純網路銀行發展模式三個部分進行分析。

(一) 大型銀行的網路銀行發展模式

對於大型銀行而言，網路銀行通常是一個獨立的事業部或者是銀行團控股的子公司，成為其發展新客戶、穩定老客戶的手段。實務中，這些虛擬機構幾乎總是比大型銀行中其他部門發展快得多。以加拿大的歷史最悠久銀行 — 蒙特利爾銀行為例：其在 1997 年擁有 34,000 名員工，1,250 個分支機搆和 700 萬名顧客；在 1996 年 10 月設立了名為 Mbanx 的網路銀行，據預測在 5 年內，其網路銀行的客戶會達到 1 億以上。

大型銀行在發展網路銀行業務時可以通過兩種方式，一是收購已有的純網路銀行；二是組建自己的網路銀行分支機搆。本文將分別舉例說明：

1、收購現有的純網路銀行

加拿大皇家銀行(Royal Bank of Canada, RBC)是加拿大規模最大、經營能力最好的銀行之一。在超過一個世紀的時間裏，加拿大皇家銀行在美國只從事金融批發業務。1998 年加拿大皇家銀行以 2 千萬美元收購了安全第一網路銀行(SFNB)除技術部門以外的所有部分，此時該網路銀行的客戶戶頭有一萬個，其存款餘額早在 1997 年就超過了 4 億多美元。

加拿大皇家銀行的策略目的，一是在於擴大其在美國金融市場的業務和股份。加拿大皇家銀行以收購安全第一網路銀行(SFNB)的方式步入美國金融零售業務的市場，利用安全第一網路銀行(SFNB)吸收的存款投資於加拿大的中小企業，獲取收益；更重要的是，加拿大皇家銀行利用這次收購，將業務拓展至一個新興的、快速發展的領域。這次收購使加拿大皇家銀行立即站在網路銀行發展的最前端，況且在美國設立一家傳統型分行需要 200 萬美元，而維持安全第一網路

銀行這樣一個 10 人機構的費用要遠遠低於任何一家傳統分行，所以完全是一次低成本、高效益兼具的典範。

2、發展自己的網路銀行

威爾士·法戈銀行(Wells Fargo)是這方面典型的例證。這個位於加尼福利亞州的銀行，是美國最大的銀行之一，在 10 個州擁有營業機構，管理著 1,009 億美元的資產。早在 1992 年，威爾士·法戈銀行就開始建設其自己的作為網路和以網路銀行服務為核心的資訊系統。實際上，威爾士·法戈銀行真正的網路銀行開業要比安全第一網路銀行(SFNB)要早幾個月，至 1997 年 12 月，通過網路與威爾士·法戈銀行交易的客戶已超過 43 萬，遠遠多於安全第一網路銀行(SFNB)。

威爾士·法戈銀行建立網路銀行的策略目的在於適應客戶交易偏好的改變和降低經營成本。在開發其網路銀行業務時，威爾士·法戈銀行通過調查發觀，客戶不僅需要查詢帳戶餘額、交易記錄、轉帳、支付票據、申請新帳戶和簽發支票等基本網路銀行業務，還需要一種有關帳簿管理、稅收和財務預算的服務。他們便在 1995 年，與微軟貨幣(Microsoft Money)、直覺(Intuit)和快訊(Quicken) 建立策略聯盟，利用他們的套裝軟體提供這方面的服務。在降低成本方面，每天有 40 多萬客戶通過網路與威爾士，法戈銀行進行交易，據銀行自己估計，每 200 萬筆交易從銀行櫃面服務轉向網路服務將節省 1,500 萬美元，即每筆交易節省 7.5 美元。至 2000 年末，威爾士·法戈銀行預計將擁有 100 萬的網路用戶，隨著客戶從分行向低成本的網路轉移，他們將節約大量的費用。

(二) 社區銀行的網路銀行發展模式

信託銀行(Intrust Bank)是一家位於肯薩斯州的社區銀行。信託銀行建立網路銀行的策略目的是為了與美洲銀行(Bank of America)等

大型銀行在競爭中維持均衡態勢。其建立網路銀行僅是作為策略防禦作用，並僅將網路銀行視為防止當地客戶流失的手段之一。信託銀行作為一家社區銀行，一直將目標客戶市場定義為當地的客戶。當新興的網路銀行出現，並對以地理位置確定目標客戶市場的策略產生強大衝擊時，發展自己的網路銀行以保證在目標客戶市場中的佔有率，是信託銀行最好的選擇。今天他們的網路用戶端可以進行遠端交易，並即時檢查交易情況。客戶們不僅可以在網路上看到自己信用卡的使用情況，而且可以看到該行經紀人服務所提供的投資計畫。信託銀行還打算將語言識別系統投入網路服務，以便對使用遠端交易零售商的身份進行鑒別，加強網路的安全性。

(三) 純粹網路銀行的發展模式

對於純網路銀行的發展模式而言，也有兩種不同的理念。一種是以印第安那州第一網路銀行[37](First Internet Bank of Indiana, FIBI)為代表的全方位發展模式；另一種是以休士頓的康普銀行[38](CompuBank)為代表的特色化發展模式。

1、全方位發展模式

對於應用這種發展模式的網路銀行而言，他們並不認為純網路銀行具有侷限性，反而認為隨著科技的發展和網路的進步完善，純網路銀行完全可以取代傳統銀行。這些純網路銀行一直致力於開發新的電子金融服務，以滿足客戶的多樣化需要。為吸引客戶和中小企業，

[37] 第一個提供全面服務的網路銀行，First Internet Bank of Indiana，1999 年 2 月 22 日開始營業 https://www.firstib.com (last visited on 2005.09.10))))))))。

[38] COMPUBANK 總部設在休斯頓的 COMPUBANK 擁有 600 萬美元的運營資金，已獲得了美國幣貨監理官的批准，可以在美國全境運作。同時，它已在聯邦保險公司受保，儲戶的最高受保存款金額爲 10 萬美元。網路銀行的功能在於承擔網上交易的金融風險，爲客戶提供金融擔保。在網路銀行的支援下，購貨者只需提供銀行帳號，其支付能力、信用歷史由銀行來檢查並完成對交易的擔保工作。網路銀行的安全性機制由國際著名的大型電腦企業提供，例如 IBM 的"安全電子商務(SET)"，由支付閘道(Payment Gateway)、電子收銀機(e-Till)及電子錢包(e-Wallet)等各種產品解決方案組成，爲網路銀行提供水滴不漏的電子商務付款機制。參見 http://www.compubank.com (last visited on 2005.09.10)))。

純網路銀行必須提供傳統型銀行所提供的一切金融服務。印第安那州第一網路銀行正準備推出「中小企業貸款服務」，改變純網路銀行沒有企業線上貸款的歷史。

2、特色化發展模式

持有這種觀點的純網路銀行也許更多一些。此等銀行認為純網路銀行具有侷限性，與傳統型銀行相比，純網路銀行所能提供的服務要少得多，例如，因為缺乏分支機構，無法為小企業提供現金管理服務；也不能為客戶提供安全保管箱。純網路銀行若想在競爭中獲取生存必須提供特色化的服務。這類銀行的代表就是康普銀行，這家位於休士頓的純網路銀行只提供線上存款服務。在康普銀行的高級管理人員看來，純網路銀行應該專注於具有核心競爭力的業務發展，至於其他的業務可以讓客戶在別的銀行取得。康普銀行認為，客戶可以在網際網路上發現想要的一切，如果一家銀行想將客戶侷限在自己提供的業務中是絕對錯誤的。

除這種極端的情況以外，其他純網路銀行的特色化發展模式也很具有借鏡價值。耐特銀行(Net，B@nt)是僅次於安全第一網路銀行(SFNB)的純網路銀行，在 1999 年第一季末，該行存款已經達到 3,327 億美元，在後者被收購以後，它成為純網路銀行業的先驅。其服務的特色在於以較高的利息吸引更多的客戶。最高執行長葛利姆斯(G.R. Grimes)認為，每一個純網路銀行的客戶都是從其他銀行吸引過來的，所以吸引客戶在純網路銀行的策略中應是第一位的，而利息則是吸引客戶的最佳手段。在這種理念的指引下，耐特銀行在 1999 的第一季末，其客戶接近 25,000 人，是前一年的三倍。而且這個增長速

度還在加快，耐特銀行在 Gomez[39]的綜合排名中僅次於安全第一網路銀行(SFNB)和威爾士·法戈銀行，位列第三，在其他項目中也表現不俗。

四、跨國電子銀行業務之風險管理與監管[40]

(一) 近年來，隨著資訊技術的進步，許多國家的電子銀行業務已經突破國界，開始了跨國經營之路。雖然目前仍存在許多制約條件，但由於以下三個方面的因素，使得跨國電子銀行業務成為銀行業未來發展的趨勢之一：(1) 消費者越來越習慣於使用銀行的電子化服務管道，並感受到了它的便捷性；(2) 資訊技術不斷進步，使銀行提供的跨國電子銀行服務更安全、更便捷、成本也更低；(3) 銀行競爭加劇迫使銀行在產品和服務管道上不斷創新，不斷開闢海外市場。

為了迎接電子銀行跨國經營帶來的挑戰，同時也為確定電子銀行國際化的正確策略，有必要對跨國電子銀行業務中存在的風險及如何對其進行管理和監管進行研究。參考國際機構(如 Electronic Banking Group, EBG)的意見，本文將跨國電子銀行業務定義為：某一銀行在一個國家(或地區)向另一個國家(或地區)的居民通過網路提供線上的金融產品和服務的交易活動。

也就是說，跨國電子銀行業務的服務提供方在一個國家(或地區)，而服務接受方在另一個國家(或地區)，兩者通過網際網路完成交易。許多國際性大型銀行在多個國家建立有形分支機構，由這些分支

[39] 美國 Gomez Advisors 網站創建於 1997 年，每年兩次對網路證券公司的服務品質進行綜合比較，在美國業界認同享有權威地位。Gomez 常把券商的服務品質分成 5 個評價要素，根據其對客戶重要性的不同而給予不同的權重，這 5 個評價要素一般是：方便程度，顧客信任，網站資源，客戶服務，綜合成本；此外，Gomez 根據投資者的偏好和交易行爲將其分成四類：頻繁交易者，嚴肅投資者，計畫投資者和一站式投資者。

[40] 秋月，跨國電子銀行的業務怎樣進行風險管理與監管，計世網 http://www.ccw.com.cn/cio/research/hangye/htm2004/20040715_10LN9.asp(last visited on 2005.09.10)。

機構向所在地居民提供的線上金融產品和服務，因為它是一種實體交易，與國內電子銀行業務沒有多大區別，各國一般也按國內電子銀行業務進行管理，因而不包括在此處所定義的跨國電子銀行業務之中。

(二) 在實務中，或有經由以下標準來判斷外國銀行是否向本國提供跨國電子銀行業務：

1、該外國銀行的網站上是否使用本國語言，是否使用本國貨幣單位標明交易物件。由於語言和貨幣單位往往暗示著銀行的目標客戶群，因而借助網站使用的語言可以幫助判斷外國銀行是否意在向本國提供電子銀行業務。由於有些語言如英語在幾個國家通用，還有些國家同時使用幾種官方語言，所以這一標準有時並要與其他標準結合起來使用才能有效。

2、該外國銀行的網域名稱[41]是否使用本國保留的名稱(如網址名稱與本國國內的某一知名品牌相同)；或者該外國銀行的網站設計成足以使本國消費者誤認為該銀行座落在本國範圍內。

3、該外國銀行是否在本國電視、報紙、郵件上做廣告或開展其他市場行銷活動。如果是的話，一般就比較明確地意味著該外國銀行將本國居民作為目標客戶。需要指出的是，目前還沒有一套完善的、國際通行的指標體系來界定跨國電子銀行業務，各個國家監管當局一般是根據經驗和個案的具體情況來作判斷。

(三) 跨國電子銀行業務的風險識別巴塞爾銀行監管委員會(BCBS)[42]的電子銀行組織將電子銀行業務的主要風險歸結為策略風

[41] 網域名稱(Domain Name)就是俗稱的網址，是用來辨別 IP 位址的名稱，在 URL 中打入此一位址即可瀏覽某一網頁，功能上像門牌號碼用以定設位址座標。

在命名網域名稱時，多以"www"爲開頭，緊接著爲網站名稱，再來是代表該網域所屬領域，例如："gov"爲政府單位，"edu"爲教育單位，"org"爲非營利機關，"mil"爲軍事單位，"com"爲商業機構，"net"爲網路機構。最後再加上網站註冊地區，例如：在我國註冊的網站，會在網域名稱的最後一部份加上"tw"，日本以"jp"爲網域結尾，英國以"uk"爲網域結尾。由於網際網路是由美國國防部(ARPA)的研究項目起源而生的，美國的網域名稱不用在網址最後加上國家名稱。

險、信譽風險、操作風險、法律風險、信用風險、市場風險、流動風險(EBG, 2000)，跨國電子銀行業務的發展，雖然並沒有增加一些以前我們沒有識別的新風險類別，但它幾乎影響到上述所有風險類別，使這些風險表現形式和程度有了很大的不同，其中以操作風險、信譽風險和法律風險增加得最為顯著。

1、操作風險

由於網路的開放性、匿名性和技術複雜性，電子銀行業務面臨比傳統服務管道更大的操作風險，如來自外部的非法進入，來自內部的越權使用資料，"駭客"和病毒攻擊，系統故障導致的資料丟失等。而跨國電子銀行業務的開展使這一風險顯著增大，因為它涉及到使用不同國家的網路設施，要與並不熟悉的外國 ISP 等服務商合作，要適應不同國家的規定要求和不同的客戶習慣等等，使得銀行電子系統在客戶身份鑒別、資料保護、業務審計、客戶隱私保護等方面更容易出現漏洞和延誤。操作風險過大也是目前制約跨國電子銀行業務發展的主要原因之一。

2、信譽風險

跨國電子銀行業務使銀行面臨更大的信譽風險。一個銀行貿然開辦跨國電子銀行業務，控制不好的話可能使其多年辛苦建立起來的信譽毀於一旦。在目前情況下，人們對鋼筋水泥構築起來的實實在在的銀行有更多的安全感，對使用電子銀行服務管道尤其是國外的電子銀行服務多數是嘗試性的，一次嘗試失敗就很可能使客戶完全否定這一

---

[42] 1975 年由 10 國集團國家中央銀行行長建立了巴塞爾銀行監管委員會(BCBS，The Basle Committee on Banking Supervision)。並於 1975 年簽署了《巴塞爾協定(Basle Concordat)》，成功地制定了最低限度的監管準則；其後，對當時未達成協議的事項進行審議的同時，進一步強調監管應跟上國際銀行業發展的形勢並與之相適應。1997 年 9 月正式頒佈了《有效銀行監管核心原則》。此外，巴塞爾銀行監管委員會為強化國際性銀行業務規則，在成員國監管當局之間達成了有關協議，其中最有名的協議是關於銀行自有資本比率的《巴塞爾協議》。

服務管道，如果某國外銀行在一個國家僅提供電子銀行服務，那客戶嘗試的失敗將導致對該銀行整個服務的否定，該銀行在此地的信譽將受到嚴重損害。

3、法律風險

對國外法律的不熟悉和電子銀行相關法律本身的不完善、不確定性使法律風險也顯著增大。目前，各國都在積極探索與電子銀行相關的法律問題，但到目前為止仍然很不完善，特別是缺乏國際公認的法律規範體系，因而發展跨國電子銀行業務面臨的是一個正在演進中的、帶有很大不確定性的法律環境，再加法律的國別差異，開展跨國電子銀行業務法律風險比較大。

(四) 跨國電子銀行業務的風險管理開展跨國電子銀行業務雖然存在眾多的風險，但它代表著未來銀行發展的趨勢，是搶佔國際市場的重要管道，因而是機會與風險並存，惟有加強風險管理和外部監管，才能做到既抓住機會又將風險控制在可接受的範圍之內。電子銀行跨國業務的風險管理首先要遵守並真正落實 2001 年 5 月 BCBS 發佈的「電子銀行風險管理指引 」，該指引對所有電子銀行業務均具有指導作用，按照該指引完善內部風險管理措施對跨國電子銀行業務的風險管理尤其具有重要意義，是跨國電子銀行業務風險管理的基礎。

按照該指引的精神，主要應在三個方面採取措施以加強風險管理：

1、董事會和最高管理階層要履行對風險進行整體監控(oversight)的職責。

具體而言，至少應當做到如下幾點：(1)董事會和最高管理階層應當建立起有效的風險管理機制，包括建立明確的責任制度、政策規定和控制措施；(2)董事會和最高管理階層應當對安全控制流程的關鍵部分進行評估並置於掌控之下；(3)董事會和最高管理階層要建立起全面的、持續的、審慎的有效管理機制以正確處理技術外包(outsourcing)等與第三方技術服務商的關係。

2、要有完整有效的操作和安全控制體系

至少要做到：(1)在透過網路交易時，客戶的身份的確認要有適當的認證措施；(2)通過適當機制，提高電子銀行交易的不可否定性；(3)資料庫、應用程式、系統管理等崗位要適當分工；(4)確保交易、記錄和客戶資料的資料完整性，所有電子銀行交易都要留有紀錄(即交易過程是可查的)，對敏感資料要根據其重要程度採取相應的保全措施等。

3、透過有效措施控制法律和信譽風險

這些措施包括：(1)在網站上披露足夠的資訊以使客戶在交易前對銀行的身份和受監管狀況有充分的瞭解，以增加客戶對銀行的信心；(2) 按客戶所在國的隱私保護要求提供相應保密措施；(3) 制定專門計畫並裝備相應設施以應對突發事件，保證服務和交易的持續性，以避免因服務中斷或資料丟失引發的信譽損失和法律糾紛。

除上述三個方面外，本文認為至少還應在以下幾個方面進行努力，以加強跨國電子銀行業務的風險管理：

1、與相關方面進行經常的、充分的資訊溝通

也就是說，在開展業務之前和開展業務過程中，銀行應當盡可能多地與東道國的監管部門、合作夥伴進行溝通，表達自己的意願，瞭解對方的要求。溝通的內容主要在二個方面：一是技術層面，如當地

(東道國) ISP 的技術平臺、使用和管理制度等，這些與操作風險有關；另一個是法律和制度層面的，開展跨國電子銀行業務的銀行最常見的風險就是無意中違反了當地的一些法律法規或政策，因為當地的一些機構，會對一個外來銀行提供的金融產品給於特別的關注，他們會根據各自的角色提出各自的要求，這些要求不僅可能與銀行母國的規定有較大的差異，同時它們本身也可能不成體系，甚至相互不協調，這樣就給跨國銀行遵循當地法律增加了難度，因而銀行要經常關注當地法律法規的動態，與各有關部門經常保持溝通。

2、明確產品邊界

在提供服務前，一定要通過適當管道如網站等明確提供其跨國電子銀行產品和服務的邊界資訊，即要明確界定哪些國家哪些人屬於其服務對象，以及客戶具有的權利和應承擔的義務。因為一個銀行在虛擬市場，面臨的不僅有居民，還有非居民，而居民與非居民的服務風險是有明顯差異的，所以銀行在設計虛擬市場電子服務品種時就要考慮其風險承受能力，並根據風險承受能力確定服務物件即產品邊界，最後還要有效地將產品邊界資訊傳遞給客戶。

(五) 跨國電子銀行業務的監管。電子銀行的監管本來就是一個富有挑戰性的問題，跨國經營之後更成為監管難題，難點主要在於管轄權邊界不清晰，業務交易找不到合適的計算時點，銀行容易逃避監管等。

1、監管順序

確定監管順序就是對母國與東道國的監管職責進行分工。與傳統銀行跨國經營相似，在對電子銀行跨國經營進行監管過程中，母國負有第一位的監管責任，因為它是銀行的註冊地，對銀行情況更為熟

悉，監管措施也更為有效；雖然東道國是跨國電子銀行業務中利益受影響的主要一方，但由於資訊不對稱，監管手段和措施有時也鞭長莫及，因而東道國往往處於最後監管者的位置。它一般先對在本國開展電子銀行業務的外國銀行是否存在有效的母國監管作出判斷，如果有，東道國就主要協助母國進行監管，並進行必要的補充監管，補充監管是指對本國有要求而外國銀行的母國沒有要求的內容進行監管。如果該外國銀行不存在有效的母國監管，東道國就承擔起主要監管責任。需要強調的是，不管存不存在有效的母國監管，東道國都要與母國的監管者保持有效的溝通與協作，例如資訊的共用、政策的協調等等，最好是雙方建立起常設的機構來負責協調雙方的監管事宜。

2、母國的監管

母國可以將所有電子銀行作為同一類監理客體，而不管其是經營國內業務，還是經營跨國業務。母國監理的內容主要包括市場進入、資本金充足率、存款保護、風險控制等。市場進入是規範電子銀行業務發展，降低電子銀行風險的第一道門檻，各國(或地區)在這方面制定了不同的標準，例如，香港金融管理局規定在香港開辦電子銀行業務，首先要滿足與傳統銀行同樣的審慎標準，且必須在當地至少有一個實體形態的營業機構，必須有可行的經營計畫，必須有完善的風險管理與安全控制，必須明確規定客戶的權利和義務，如果技術外包還要符合香港金融管理局制定的“外包指引”的規定。在資本金充足率和存款保護方面不需作特殊的規定，可以執行與傳統銀行同樣的規定。風險管理則應如 BCBS 發佈的指引那樣加以要求，並進行必要的檢查。

3、地主國的監管

地主國在電子銀行跨國經營中是最末端的監理者，在母國監理缺位的情況下其監理是否有效直接關係本國存款者的利益和本國的金融秩序。地主國監理內容包括市場進入、營運監管，其中營運監理分二種情況，一種是在母國監理有效的情況下協同監理；一種是在母國監理不足情況下的主導監理。

對外國銀行在本地開展電子銀行服務的市場進入條件一般包括資本金或資產規模要求、母國監管效率要求、銀行技術系統效率及安全性要求等，如香港金融管理局規定：外國銀行在本地區開展電子銀行服務要有代表處，要在母國的有效監理之下，總資產必須在 160 億美元以上等等，只有符合條件的外國銀行才能獲准在本地開展電子銀行服務。

協同監理是指地主國對有效母國監理的協助監理。地主國在協同監理方面，首先，應當與母國監理者建立起有效的溝通管道，瞭解母國監理的內容及效率，對母國監理的有效性進行經常性評估；其次，它應當通知母國有關本國的監理要求與考慮，相關法律政策如發生變動應及時通知母國監理者；同時，還應及時提供監理物件在本地的活動情況；此外，還要根據本國的特殊考慮建立起補充監管措施。

在外國銀行的母國監理可能不足的情況下，地主國成為該銀行業務監理的主要依歸。在這種情況下，地主國可以選擇拒絕頒發牌照，禁止其在本國經營電子銀行業務；也可以比照國內電子銀行的監理要求，命其在本地設代表處或存儲風險準備金等。如果由於法律規定(如銀行法中未將渠等形態納入銀行定義範圍)等原因，而未將這種業務納入核准制度範圍，則應協同其他政府部門，採取更為靈活的監理措施加以控管。

五、風險管理

承上所述，為順應網路通信技術的迅猛發展，銀行的組織結構、經營理念、運作模式、服務方式等已發生重大變革。在金融服務業競爭激烈的今天，以網路技術改造傳統銀行服務、發展網路銀行業務已成為銀行業必然的選擇。

(一) 網路銀行的優勢

與傳統商業銀行相比，網路銀行具有許多競爭優勢已如前所述。整合起來，不外乎有以下三點。

1、成本競爭優勢

網路銀行可以大幅地降低經營服務成本，創造巨大的利潤空間。在傳統銀行經營開支中，人員工資和租金占比最大，而網路銀行服務則通過電腦處理各種客戶需求，無須依賴眾多密集的分、支行網路，從而節省大量人力資源和經營成本，符合現代銀行降低成本、提高效益的經營思路。

2、差異型競爭優勢

開展網路銀行業務不受時空地域限制，可最大限度地擴大業務規模，並向客戶提供個人化的金融服務產品。傳統商業銀行的行銷目標只能細分到某一類客戶群，很難提供一對一客戶服務。即使能提供，成本也比較高。而網路銀行能在低成本的情況下實現一對一服務，從而形成差異性服務。由於無須理會時間及地域限制就可處理銀行交易，客戶可隨時隨地處理網上個人財務安排，因此特別吸引高薪階級的客戶，而這正是當前銀行必爭的領域。

3、知識優勢或無疆界競爭優勢

在現代資訊技術條件下，特別是在當前網路經濟環境下，銀行競爭的優先選擇因素是知識因素。經濟全球化和資訊化使銀行之間的競

爭從有形資本轉為無形資本，從土地、資金和人才的競爭轉為人力資本、資金、思想觀念和知識的競爭。作為網路銀行，通過利用資訊技術和資源，可以為自身提供競爭所需要的知識要素和手段。

(二) 網路銀行的風險

網路銀行是一種虛擬銀行，不容忽視的是，網路銀行的發展在提高銀行服務效率的同時，也存在一些潛在的障礙和隱患。網路銀行除了具有傳統銀行經營過程中存在的各種風險之外，還由於其特殊性，存在著基於虛擬銀行服務類型而衍生的業務風險和基於資訊技術所導致的技術風險。

1、網路銀行實用上的風險類型[43]

網路銀行的風險類型呈複雜性和多樣性，目前國際國內主要的網路銀行風險可以歸納為以下幾種類型：

(1) 盜用他人身份與密碼，進行資料竊取。因為網際網路服務在給銀行和用戶提供共用資源的同時，也為竊取銀行業、用戶秘密資料的非法“侵入者”敞開了大門。一些竊賊盜取銀行或企業秘密賣給競爭對手，或因商業利益，或因對所在銀行或企業不滿，甚至因好奇盜取銀行和企業密碼，瀏覽企業核心機密。據美國官方統計，銀行每年在網路上被偷竊的資金達 6,000 萬美元，而每年在網路上企圖電子盜竊作案的總數高達 5～100 億美元之間，其平均作案值是 25 萬美元，而持槍搶劫銀行只有 7,500 美元。這些侵入者多數為解讀密碼的高手，作案手段隱蔽，不易發現，通常能夠查獲的約為六分之一，而只有 2%的網路竊賊被抓獲。

[43] 我國網路銀行的風險及其防範，電子商務研究，http://www.dzsw.org/Article/ShowArticle.asp?Pay=yes&ArticleID=978(last visited on 2005.09.10)。

(2) 網路詐騙。網路詐騙已成為世界上第二種最常見的網路風險。一些不法分子透過發送電子郵件或在網際網路上提供各種吸引人的免費資料等引誘使用戶，當用戶接受他們提供的電子郵件或免費資料時，不法分子編寫的病毒也隨之進入用戶的電腦中，並偷偷修改用戶的金融軟體；當用戶使用這些軟體進入銀行的網址時，修改後的軟體就會自動將用戶帳號上的錢轉移到不法分子的帳號上。網路詐騙包括市場操縱、內線交易、無照經紀人、投資顧問活動、欺騙性或不正當銷售活動、誤導進行高科技投資等網路詐騙。據北美證券管理者協會調查，網上詐騙每年估計使投資者損失 100 億美元。

(3) 電腦駭客。稱非法入侵電腦系統者為“駭客”，是美國麻省理工學院的學者首先提出的。克羅地亞的 3 名中學生在操縱電腦遨遊網路世界時，進入了美國軍方的電腦系統，破譯了五角大樓的密碼，從一個核資料庫中複製了美國軍方的機密檔。據美國參議院一個小組委員會的估計，全球企業界 1995 年損失在「駭客 」手中的財富達 8 億美元，其中美國企業損失 4 億美元。由於對「駭客 」闖入國家安全防務系統的擔憂，甚至擔憂未來的「電子珍珠港襲擊 」。目前已經有許多國家具有製造電子炸彈的能力；這對國家金融安全的潛在風險是極大的。

(4) 電腦病毒。電腦病毒對銀行電腦系統形成了巨大的威脅。據英國(金融時報) 報導，在 1996～1997 年的 18 個月中。世界範圍新發現的電腦病毒數量幾乎翻了一番。平均每個月新發現的電腦病毒數從過去 200 種上升到 500 種左右。全世界已知的電腦病毒已達 18,000 種，尚有上百種待查明的電腦病毒在流傳。1999 年 4 月 26 日的 CIH 病毒的爆發，就使大多數電腦的 C 槽資料被毀。此外，隨著國際網際網路的普及，銀行的電子信件也成為電腦病毒傳播的主要管道。

(5) 資訊污染。正如在工業革命時期存在工業污染，資訊時代也有資訊污染和資訊過剩。大量無序的資訊不是資源而是災難。隨著網際網路用戶數和網路業務量的急劇增加，也帶來了新的問題，包括大量「商品廣告 」等網上「垃圾 」。美國線上公司每天處理的 3,000 萬份電子信件中，最多時有三分之一是垃圾郵件，從而佔據了許多寶貴的網路資源，加重了網際網路的負擔，影響了網路銀行發送和接受網路資訊的效率，更嚴重的是風險也隨之增加。

2、網路銀行的業務風險

網路銀行的業務風險主要包括法律風險、實用性風險、信譽風險等。網路銀行的法律風險源於違反相關法律規定、規章和制度，以及在網路交易中有關權利與義務沒有清晰的規定，缺乏相應的網路消費者權益保護規範[44]。金融立法架構主要基於傳統金融業務，使銀行在網上開展業務時無法可依，客戶與網路銀行很容易陷入法律糾紛之中。因此，利用網路提供或接受金融服務、簽訂契約，面臨著相當大的法律風險。銀行容易陷入不應有的糾紛之中，結果使交易者面對交易行為及其結果產生更大的不確定性，增加網路銀行的交易費用，甚至影響網路銀行的健全發展。

實用性風險主要是指由於客戶自身條件和需求內容的不同，要求網路金融機構所提供的服務也各不相同而造成的風險。由於金融機構的經營理念不同，有的強調穩健性，有的側重快捷性。穩健型網路銀行視交易安全為第一，但在網上實際交易時存在手續繁雜、認證過程較長等弊端；快捷型網路銀行進行交易時一般速度較快，認證解密時間較短，但安全性有所降低。眾多的差異導致客戶對網路金融機構的不同認識，客戶在進行線上交易時會根據自己的實際需要，對各個機

[44] 我國行政院消費者保護委員會於民國 94 年 3 月 31 日訂定「網路交易定型化契約應記載及不得記載事項指導原則」，詳參附件。

構的交易及特點進行認真的比較，以選擇能夠充分滿足自身需求的網路金融服務。因此實用性在網路金融中具有獨特的地位與作用，若在工作中不加以重視，就會導致失去客戶的後果。另外，對開展網路銀行服務的金融機構來說，提供一個可靠的網路系統是至關重要的。如果金融機構不能持續地提供安全、準確和及時的網路金融服務，金融機構的信譽將受到損害。而且一家機構出現問題，客戶就會認為採用與該機構相同或相似的系統或產品的其他金融機構也存在安全隱憂，致使客戶流失。對於重大的安全事故，無論它是由外部攻擊還是內部攻擊引起的，都將降低公眾或市場對該金融機構的信心，進而對整個網路金融系統的安全性和可靠性產生懷疑。在極端情況下，這可能會導致金融系統的崩潰。

3、網路銀行的技術風險。

由於網路銀行對於自動化程度較高的技術和設備的高度依賴性，和傳統的銀行相比較，技術風險成為網路銀行所面臨的最大、最特殊的風險。這些風險主要來源於以下幾個方面。

(1) 技術架構的合理性

如果網路銀行系統不能將多種業務系統進行適當整合，那麼銀行將由於交易處理發生的錯誤而暴露出重大的運作風險。

(2) 系統安全性

開放的電子資訊傳輸管道使銀行的安全暴露在新的風險之下，形成了新的安全風險問題。

(3) 資料完整性

資料完整性是系統安全的一個重要組成部分。如果銀行沒有建立一個有效的控制程式，資料在傳遞和接受過程中就可能發生遺失或轉換變形，造成資料不完整。

(4) 系統的有效性

如果銀行沒有制定一個有效的運行持續性計畫和事故應急計畫，系統的超負荷運行和損耗就可能影響銀行一貫提供的產品和服務，引起潛在的聲譽風險。

(5) 內部控管：

如果銀行不具備充分到位的內部控管措施，那麼銀行就不能有效防範來自內外部的欺詐行為。

(6) 業務外包：

很多銀行機構過於依賴少數幾個外包商，這種對少數外包商的集中依賴性可能會產生系統性影響。雖然網路銀行都設有多層安全系統，並不斷出現新的安全技術及方案，以保護虛擬金融櫃檯的平穩運行，但是網路銀行的安全系統仍然是網路銀行服務業務中最為薄弱的環節。系統安全風險不僅會擾亂或中斷正常服務，給銀行帶來直接的經濟損失，而且還影響網路銀行的形象和客戶對網路銀行的信任水準。

綜前所述，我國網路銀行與發達國家相比，仍存在許多問題，在創建和發展網路銀行的同時，應從以下幾方面努力防範未來網路銀行可能發生的業務風險。

1、建立網路安全防護體系

其主要目的是在充分分析網路脆弱性的基礎上，對網路系統進行事前防護。主要通過採取物理安全策略、訪問控制策略、建構防火牆、安全介面、數位簽章等新興網路技術的拓展來實現。

2、加快發展網路加密技術

近年來，世界加密技術的市場規模巨大，達到幾十億美元，並呈現迅猛發展的態勢。美國在加密技術電腦軟體的開發方面具有世界領

先地位，較其他在加密技術方面先進的國家如以色列、瑞士、俄羅斯和日本等還略勝一籌。我國應儘快學習和借鑒美國等發達國家的先進技術和經驗，加快網路加密技術的創新、開發和應用，包括亂碼加密處理、系統自動簽退技術、網路使用記錄檢查評定技術、人體特徵識別技術等。

3、發展資料庫技術，建立大型網路銀行資料庫

通過資料庫技術存儲和處理資訊來支援銀行決策。要防範網路銀行的資產風險，必須從解決資訊對稱、充分、透明和正確性著手，依靠資料庫技術儲存、管理和分析處理資料，這是現代化管理必須要完成的基礎工作。(1) 網路銀行資料庫的設計可從社會化思路考慮資訊資源的採集、加工和分析，以客戶為中心進行資產、負債和中間業務的整合管理。(2) 不同銀行可實行借款人信用資訊共用制度，建立不良借款人的預警名單和「黑名單」制度。(3) 對有一定比例的資產控制關係、業務控制關係、人事關聯關係的企業或企業集團，透過資料庫進行歸類整理、分析、統計，統一授信的監控。

4、加速電子商務和網路銀行的立法進程

針對目前網路金融活動中出現的問題，借鏡先進國家的經驗，建立相關的法律，以規範網路金融參與者的行為。電子商務立法首先要解決電子交易的合法性、如怎樣取用交易的電子證據，法律是否認可這樣的證據，以及電子貨幣、電子銀行的行為規範，跨國銀行的法律問題。其次，對電子商務的安全保密也必須有法律保障，對網路犯罪、電腦洩密、竊取商業和金融機密等也都要有相應的法律制裁，以逐步形成有法律許可、法律保障和法律約束的電子商務環境。

5、加入 WTO 後我國銀行金融業面臨的問題

儘快熟悉和掌握國際上有關電腦網路安全的標準和規範，如掌握和應用國際 ISO 對銀行業務交易系統的安全體系結構等，制定一套較為完整的國際標準，以便我國網路銀行在風險防範上與國際接軌。[45]

六、觀察與檢討

1、資訊時代大型銀行的發展趨勢——網路銀行。

隨著數位經濟的到來和網際網路的普及，傳統型大型銀行 300 年來賴以生存的基礎已發生不可逆轉的變化。網際網路將全世界的電腦緊密地聯繫在一起，為銀行提供一個利用虛擬方式發展金融業務的新途徑。大多數的金融業務在網際網路都可以用最低的成本和最快的速度完成；同時一切金融資訊和資金結算都可以在這裡傳輸與交流。目前已使用網路銀行業務的客戶中多以年輕族群為主，其將成為未來銀行業未來的主流客戶。所以任何銀行無論資金多麼雄厚、實力多麼強大，如果忽視網路銀行的發展，都將在未來的數位經濟時代受到懲罰。相之，如果能利用這個機遇，將自己的優勢與網路銀行相結合，也將會邁向前所未有的發展前景。對於大型銀行而言，總是會有更多的選擇機會，不管是收購網路銀行的發展模式，還是自我組建網路銀行的發展模式都是不錯的選擇。

2、小型銀行服務要強調金融服務特色化

鑒於網路銀行投資少、維持費用低、使用範圍廣、隨時隨地可進行交易、業務功能強大、資訊傳遞快捷等優勢，其產生為小型銀行戰勝大型的金融集團提供了可能性。但是由於網路銀行業務的差異性小，所以行業的進入壁壘很低，在此情況下，必需要強調自己的服務

[45] 我國網路銀行的風險及其防範，電子商務研究 http://www.dzsw.org/Article/ShowArticle.asp?Pay=yes&ArticleID=978(last visited on 2005.09.10)。

特色。只有特色化的服務才可以贏得市場制勝的法寶 — 客戶。對小型銀行來說，市場定位一定要清晰，才能在與大型銀行的競爭中維持均勢。

3、銀行業要重視網路人才的培養，特別是同時具備網路知識和金融知識的人才培養。

網路銀行業務的順利進行，不僅需要完備的金融知識，更需要具備充分的網路知識。在網路銀行網站的建設和維護方面，要有具備電腦網路硬體知識的人才；在網路銀行網頁和網路金融新產品開發方面，要有具備電腦軟體發展知識和具備銀行業務知識的人才。威爾士·法戈銀行在自己的網路銀行開業前的第 2、3 年就開始著手進行準備工作。對於小型銀行而言，單獨進行人才儲備的成本也許會很高，可以通過人才的外聘或策略聯盟的形式，獲取外部的套裝軟體，以降低成本。

4、銀行業必須重視網路銀行業務的技術保證

網路銀行需要很先進的技術作為其支持力量。在硬體方面，需要有功能強大的伺服器、甚或如指紋鑑定或其他生化辨識功能功能的安全性自動櫃員機；在軟體方面，需要網路安全系統、語音識別系統、電子轉帳系統、管理資訊系統等眾多軟體系統集合而成。

5、銀行業還須重視市場行銷的作用，建立服務品牌

正如前所述，網路銀行的進入壁壘很小，所提供金融服務的差異化也很小，因此銀行業一定要重視市場行銷的作用，建立自己的服務品牌，以獲得更多的客戶[46]。

[46] 徐昕，西方網路銀行的發展模式及啓示國際金融研究 ，ACSI(中國國家信息化專家諮詢委員會)，
http://www.acsi.gov.cn/web/NewsInfo.asp?NewsId=1239 (last visited on 2005.09.10)。

第三章　小額付費機制及其他新興電子支付方式探討

壹、前言

完整電子交易從民事角度包含三個環節：電子交易契約的達成、標的物的交付以及電子支付。我國民法以及電子簽章法對電子簽章的規範在法律層面上已經滿足了線上交易契約應用的需要；標的物的交付(尤其是有形物的交付)基本上仍為傳統民法所規範；至於電子支付方面的立法闕如和若干法律障礙乃是目前急需解決的現實問題。所謂小額付款機制，在本文中尤指由個別消費者向商家或向其他消費者進行的電子支付行為。首先，小額付款並不必然是一個金額的概念；雖然通常而言，消費者在交易行為中支付的金額一般低於商家之間的交易金額，但它關注的是支付行為者及其固有的特徵，而非金額大小本身。其次，小額付款系指在線上交易中的支付行為；既包括 B2C 交易中消費者對商家的支付，也包括 C2C 交易中消費者之間的交付，但非交易專案中的支付行為如親友之間的匯款則不在此處討論之列。最後，小額付款機制中的媒介應當做較為廣義的理解；通過網際網路的支付是其典型形式，但通過電話、行動電話等遠距離通訊方式的支付也不應排除在外。目前我國甚為盛行的小額付款機制。除了一般的電信帳單及信用卡仍在小額付款領域占有一席之地外，儲值卡的支付方式已經歷市場考驗，成為網際網路世界中盛行的付款工具，較知名之單一用途者如遊戲橘子的 GASH，多用途者則有玉山銀行發行之 eCoin、藍新科技 ezPay 等(詳見圖表 3)

圖表3：國內目前重要之小額付款工具總整理資料整理：玉山銀行；2005年6月

產品	性質	市況描述
Hinet AAA	Virtual use 行動付款	只要是Hinet用戶,於付款介面輸入Hinet 的User ID 及 password 即可，便利性極強。針對海外消費者另外提供點數卡「e 金卡」於網站販售。
Seednet	Virtual use 點數儲值&電信帳單混合制	台灣 ISP 本身的服務多以預賣點數「Pre-Pay」為主，純 ISP 賬單的數量並不大。
eCoin	Virtual use 現金儲值卡	由玉山銀行正式經財政部依法許可發行之首張現金儲值卡(Virtual)，其儲值方式含信用卡、便利商店、ATM 等銀行通路。
PayVa 網路錢包	Virtual use 現金儲值卡	由華南銀行發行，儲值方式僅限銀行通路，與 eCoin 同為銀行發行。
悠遊卡	Real POS 現金儲值卡	類似香港八達通卡,以交通為主之「非接觸」IC 儲值卡，原由台北票證公司發行，2005 年 3 月標遴選銀行團隊合作發行悠遊聯名卡，悠遊卡聯名卡是指包含悠遊卡、信用卡及電子錢包3 項功能的電子卡片,其中電子錢包持卡人得以將所儲值之金錢價值，作多用途的小額消費。
Mondex Taiwan	Real POS Virtual use	Master 國際組織推出，採用接觸式晶片付款，自 2004 年 12 月 15 日起，搭配讀卡機亦可在網路上消費使用，無須輸入任何個人資料，直接扣款即可消費．為國內第一張在實體店舖及網路商家皆可使用的卡片。
Paypass	Real POS	由 Master(萬事達))國際組織推動，台灣「南部 7 縣市交通電子票證」將採用接觸式與非接觸式支付功能結合的 Combi 卡，預計 2005 年 10 月由玉山銀行與國泰世華共同

		發行，接觸式支付係以 Mondex 功能為主。
Visa Wave	Real POS	由 Visa 國際組織推動，係非接觸式晶片信用卡支付方式，由中國信託於 2005 年 3 月開始於台灣發行

貳、小額付費

一、小額付費制度特色

(一) 支付雙方相距較遠

網際網路日益蓬勃把整個世界變成了一個地球村，在網路上選購商品的時候，支付價款的雙方也就可能在同一城市，也可能相隔千里。而且，突顯電子交易之益處絕非是在隔壁鄰家小店的網站上選購，而是與相距遙遠的出售者進行採購和支付。

(二)支付雙方互不相識。

在傳統交易下，消費者至少也是對商家的形象、地理位置和風格作風有個大體瞭解。但是，由於電子交易的雙方相距遙遠，買賣雙方在大多數情況下互不相識，甚至可能沒有任何除所交易商品之外的認識。支付行為就必須在這種不熟悉的狀態下發生。

(三) 支付金額較小，但數量巨大。

由於是消費者的支付行為，所以一般金額比較小。然而，每一筆的金額雖小，交易和支付的人次卻相當驚人。消費者的眾多人數，採購商品的多樣化等因素，都促使小額付費的發生要比商家之間的大額付費更加頻繁。

承前所述，小額付費的特點相對地影響小額付費所必須該當的以下要件：

(一) 便捷性需求。

電子交易給買賣雙方帶來便捷，所以電子支付也應當體現便捷性，否則就會使電子交易的益處蕩然無存。

(二) 安全性需求。

安全性需求向來是電子交易中一個重大的理論和實踐課題。電子支付中的安全性需求一方面表現在對支付物件的安全性需求，比如支付款項的準確和支付行為無瑕疵的要求；另一方面表現在對線上交易之外的安全性需求，比如密碼和個人金融資訊的保密。電子支付的安全性需求與電子交易雙方不相識的特性以及和網路的開放性特徵是分不開的。

(三) 低成本需求。

小額付費的低成本需求系指電子支付行為本身所需的成本需要達到最低。由於小額付費的標的金額通常較低，高比例的支付成本則會使消費者望而卻步。這裏的成本既包括經濟成本，又可以包括時間成本(即，完成電子支付所花費的精力)。同時，小額付費數量巨大的特性又使降低支付成本成為可能。

一般而言，小額付費的安全性需求與便捷性需求及低成本需求有一定的矛盾關係。滿足安全性需求的投入往往會帶來不便捷和高支付成本；而一味降低支付成本和增加便捷性則可能忽略安全性的需求。理想的電子支付模式要在這三種需求中尋求最優化的平衡。

實體世界之新型態小額付費機制，近年來在業者持續研發及推動下，未來勢必更加蓬勃發展。觀諸市場上對小額付費機制需求日益殷切，主要原因如下：

(一) 網際網路公司經營型態的改變，帶動了使用者付費的觀念，而寬頻普及化也加強了消費者購買數位商品(Digital Goods)的強烈意願。由於都是小金額交易，因此，小額付費機制成了網際網路上最迫

切的需求。

(二) IC 智慧卡的技術與成本已接近一個普及的臨界點，各種應用百家爭鳴，小額付費便是其中最重要的功能之一，支付工具晶片化可望成為一種趨勢。

(三) 便利商店與電信業者的金流角色

掌握金流不再是銀行專利，便利商店挾其廣布通路及二十四小時營業的優勢，漸漸發展出代收各項帳單費用、取貨付款及點數卡販賣等金流模式，雖然對商家而言其金流成本相對提高，唯其便利性仍讓業者難以割捨。尤有甚者，統一超商更自行發行預付儲值卡「icash」[47]。全家便利商店則於2005年5月另行發展虛擬物流即時購服務(Virtual Distribution Center)，付費後憑一組個人識別碼(Personal Identification Number, PIN)，即可開通使用，首波商品主打線上遊戲點數卡及大哥大儲值卡。

電信業者則以其帳單體系成為小額付費領域重要的金流服務中心。相較於須預先儲值的小額付費方式，此系統可滿足消費者先享受再付費的需求，對消費者具有相當的吸引力，而且其計費系統可精確地收取極小金額的計時商品。目前中華電信、Seednet、台灣大哥大、速博、遠傳和台灣固網等皆提供此項服務。

(四) 行動付款新風潮

Mobile Payment乃指「以行動裝置作為付款工具的一種付款機制」，目前主要的應用均是發生在行動電話上。Mobile Payment可應用在許多不同的場合，範圍由行動電話上的各種內容資訊，如遊戲、占卜、音樂、新聞，乃至飯店、餐廳消費費用，甚至是線上賭場的賭

[47] icash 係採接觸式晶片付款方式，可以重複加值，加值後可持卡在全國 7-11 消費。統一超商於 2004 年 12 月正式發行 icash 後，以短短不到 3 個月的時間，卡片發行量已突破 120 萬張、儲值金額突破 7 億元及每日交易超過 10 萬筆，為小額消費支付卡片化奠定了基礎。

金等均可適用。由於全球目前仍無統一的標準，以致各國Mobile Payment的發展情況各異。

另外，在智慧卡(Contact-less Payments)的應用也已屢見不鮮之際，近距離無線通訊傳輸(Near Field Communications, NFC)則是結合電子錢包與行動付款的概念，將行動電話變成日常交易支付的便利工具。Motorola於2004年的10月12日宣布將進行一項結合行動電話與萬事達卡(MasterCard) PayPass 技術的計畫，並採用近距離無線通訊傳輸(NFC)技術，未來行動電話用戶將可透過行動電話快速且便利地付款。

更且甚者，除了把行動電話當成掃描器之外，也可以利用P2R (Point to Reader；單點對掃描器)的方式，擴大行動電話條碼應用範圍的可能性。2005年年初，中華電信和華納威秀推出行動電話訂電影票的服務，消費者只要利用行動電話上網訂票，中華電信就會透過簡訊傳給消費者一組條碼，接著在看電影前將行動電話端的條碼，在專屬的櫃檯前經過掃描器一掃，就可以取票看電影了。

可預見的是未來的新款行動電話將可執行多種付款應用，甚至包括可當作大眾運輸工具的非接觸式車票；此外，行動電話也將成為非接觸式的閱讀器之用，如再結合安全密碼功能，將可保護用戶個人的金融資料， 並確保交易可以安全地進行，以利於行銷活動之推展，而行動電話所創造的小額消費風潮，也可望形成一種新的「現金經濟」(Cash Economy)。

三、我國常用的小額付費系統

小額付費機制因為交易金額較小，相對於大額付費的安全要求較低，因此多使用安全程度較低且運算處理較快的私密金鑰密碼系統

(Secret-key cryptographic system)或雜湊函數(Hash function)。目前小額付費系統大多是由公正的第三者，讓顧客利用大額付費系統購買仲介商所發行或是代售的數位儲值卡，消費者可以利用儲值卡中的點數到任意或特定的商家進行消費。此外，為了提高交易效率、降低成本，儲值卡所使用的加密系統較傳統的電子付費機制簡單。國內在小額付費的系統包括：

1. SSL 信用卡機制

詳見本報告第二章第16至17頁。

2. 行動付款行動電話詳見本章第68至70頁。

3. 數位儲值卡

儲值卡也是另一種在台灣相當普及的小額付款方式，因為台灣地狹人稠，儲值卡透過便利商店販售，不但方便而且ICP廠商可以發行自有品牌的，對於消費者也有類似球員卡保值的作用。數位商品在台灣已經打開市場的線上遊戲即是以儲值卡的方式付費，例如遊戲業者華藝國際的WGS (Web Gold Services) 就是一套小額付費機制，原為用於線上遊戲收費，WGS會員在購買「WGS點數卡」後，就可利用網站上儲值的方式來進行付費。消費者一旦加入WGS 線上會員，等於開立個人戶頭。此外還有平實數位網路為網路虛擬人物訐譙龍樂捐所出的數位交易卡，都是先預付一筆金額的錢再進行消費。此種付款方式通常在便利商店的通路即需被抽取20％～40％不等的上架費，另外需付給付款系統業者5％左右的佣金，以及1.5％回饋給發卡單位。而郵局也加入數位儲值卡的服務，以全省近1,300家分支局為發行據點。

5. 智慧卡

智慧卡上面有 IC 晶片，用來記載消費與持卡人的身份認證，這張卡片目前還具有行信用卡的雙重功能，IC 晶片上也可以記有事前從銀行下載的小額款項，方便消費者到商家消費時使用。

四、以消費者觀點比較台灣線上小額付費機制

1、安全性

目前財政部規定線上交易的合法範圍為加密金鑰(DES Key) 需大於等於56 B its、憑證金鑰 (RSA Key)需大於等於1024 Bits的安全標準，目前只有SET信用卡機制與智慧卡符合財政部的標準，其餘的機制因為均需透過瀏覽器來使用，安全性應與SSL機制相當，而瀏覽器上的安全機制受限於美國安全機制出口的規定，安全性都不高。

2、隱私性

以消費者交易時所傳輸的個人基本資料與交易金額等資訊來看，SSL信用卡機制因為在商家端就可以被解密知道一切資訊，因此隱私性最低,行動付款跟數位儲值卡因為消費者交易時只需輸入帳號跟密碼，沒有傳輸個人資料，而且交易過程中經過第三者，因此交易資訊不容易被商家竊取。至於SET信用卡機制與智慧卡只有在銀行端或認證中心才會解開使用者基本資料，商家端只會收到交易金額，因此隱私性最高。

3、使用便利性

SET信用卡機制因為申請流程相當繁雜，需要使用者親自到金融機構辦理並領取帳號、密碼與電子錢包，而且僅限於在本機電腦上交易，與消費者平日隨時隨地可消費的習慣有出入，雖然SET的安全性高，但使用的方便性卻很低。智慧卡目前因為使用規模不高，有讀卡機的個人與商家均不甚多，因此雖然智慧卡只需將卡插入讀卡機即可

交易，但對於消費者來說，讀卡機的設備無法與行動電話般可隨時移動，方便性仍不甚理想。至於SSL信用卡機制與行動付款跟數位儲值卡因為沒有使用地點的限制，消費者只要記得卡號或帳號、密碼等就可以交易，極具方便性。

4、交易成本

SSL與SET信用卡機制，因為必須與商家、發卡銀行、收單銀行、VISA、Master等拆帳，手續費高達3～5%，不只對消費者增加額外的費用，對商家來說，小額產品的價格低，甚至有十元以下的交易款項，以刷卡交易毛利太低，因此就小額交易成本來說，連商家都不願意提供線上刷卡的服務，更何況SET還需申請認證與安裝電子錢包，消費者往返及安裝的時間成本也很高。智慧卡雖然可以當作現金卡，將現金存在智慧卡中使用，但是目前購置讀卡機的成本尚高，而且以台灣來說，目前並沒有一家銀行的使用規模高達類似香港匯豐銀行，所以在將現金存入智慧卡的過程中還是以信用刷卡的方式下載現金；至於行動付款與數位儲值卡原本就是針對線上小額付費所設計，因此在交易成本上比信用卡基礎的設計低上許多。

5、使用規模

以目前台灣線上付費機制來說，SSL信用卡因為只要擁有信用卡即可使用此種付費機制，使用規模最高，而SET與智慧卡因為還需另外申請電子錢包、認證與讀卡機，過程相當繁雜，且無法透過線上處理，導致使用規模一直無法提升。國內目前個人擁有行動電話的普及率極高、線上遊戲的成功使數位儲值卡的使用規模逐漸增加，在國內都為這兩種付款機制創造不少的基礎使用者。

圖表4：國內線上小額付費機制分析表(本研究整理)

付款機制評估指標	SSL信用卡	SET信用卡	智慧卡	行動付款	數位儲值卡
安全性	中	高	高	中	中
隱私性	低	高	高	中	中
使用便利性	高	低	中	高	高
交易成本	高	高	高	低	低
使用規模	高	低	低	中	中

五、針對小額付費機制之建議

綜上所述可以歸納出幾點建議，或可供國內內容網站相關業者選擇付費機制或付費機制系統廠商設計小額付費機制之參考：

1、政府與廠商應加強付款機制安全性與隱私性之宣導

許多消費者不敢在網路上消費的主要原因在於擔心付費系統的安全性不夠，雖然目前多數付費系統廠商都宣稱付費系統安全無虞，但是並沒有具體的宣導付費機制的安全保障為何。再者，目前許多網路付費糾紛為交易過程中消費者的資料外洩導致消費者權益損害，因此政府跟付費機制廠商應該加強加盟廠商的認證，並確保交易過程中消費者的資料只有在銀行端、認證中心或政府等公正第三者查核下才能調閱。

2、線上信用卡機制成本過高

雖然目前線上信用卡的使用規模已經到達一定程度，但是就小額付款來說，30元以下的商品並無法使用線上刷卡，而且1,000元以下用刷卡付費對商家來說毛利太低。此外，信用卡每次交易的手續費又比其他機制昂貴，因此線上信用卡還是比較適合用於中大額的付款。

3、智慧卡需朝多用途發展

目前智慧卡在台灣的應用，由於使用規模尚未建立、初期的硬體

設備昂貴，雖然可以離線同儕間的付款，但是以目前來說還是有發展的瓶頸，未來可能朝結合行動電話SIM卡與信用卡的方式邁進。以目前台灣行動電話普及率高達七成來說，行動電話的專屬性高，不但可以當作個人身份的驗證，結合智慧卡IC晶片中的安全機制，更可以提升安全性與使用方便性。

4、電信業者與ISP應發展公平第三者認證

透過行動電話及ISP帳單付款對消費者來說付款成本低廉、多種帳單可合併計算，且消費者可以先消費後付款，若選擇以電信帳單出帳，縱有遲延也不會要求支付遲延利息。但是由於電信業者與ISP握有消費者的眾多基本資料，因此付款機制中間應該要有可信賴的第三者做為監督，避免消費者的資料外流，也防止不肖商家的詐欺，以提高付款機制的安全性與隱私性。

5、數位儲值卡要統一標準

雖然經由線上遊戲成功的推動線上小額付費，讓數位儲值卡的使用規模逐漸增加，但是就目前每種遊戲都推出屬於自己的儲值卡，導致家數太多，缺乏互通性，以消費者觀點當然希望能夠互通，以避免每一種儲值點數都會剩餘所造成浪費。由於網路購物的商品種類繁多，價格也難以區分大額、小額，因此未來的付費系統應該著重在不同場合、不同價格可以讓消費者選擇不同的付費機制，據此廠商應該衡量消費者的使用方便性與付費系統的建置成本，設計符合消費者在實體世界中可以選擇不同付款方式的付款系統。

參、新興的電子支付方式

一、行動付款

案例一：世界最大的付款機制提供者 PayPal (以電子郵件地址為虛擬的銀行帳號)，擁有五千四百萬的使用者，2004 年第一季的總營收已達一億五千萬美元；案例二：香港的 CSL，美國的 Verizon 及韓國的 SK(以行動電話號碼為虛擬的銀行帳號)也都在 2004 前半年開始提供行動虛擬帳戶的服務；案例三：日本的 NTTDoCoMo (以行動電話號碼為 EasyCard)在 2004 年的第一季，開始提供非接觸式的行動付款機制(FeliCa，採近距離無線通訊傳輸 NFC 技術)。

根據 Global Mobinet Study 於 2002 年 2 月所作的調查指出：44％的行動電話使用者有意嘗試行動電話作為小額交易的工具；2002 年 11 月 Gartner Research 的調查顯示：46％西歐國家民眾已使用行動行動裝置支付帳款；2004 年 12 月 TNS Omnibus 的調查也揭露：超過 30％的英國行動電話用戶有意以行動電話進行小額付款，16 歲到 24 歲的年輕族群的意願更高達 56％。

行動支付業務是由行動通信商、行動應用服務提供商(MASP)和金融機構共同推出的、構建在行動業務支撐系統上的一個行動資料增值業務應用。行動支付系統將為每個行動用戶建立一個與其行動電話號碼關聯的支付帳戶，其功能相當於電子錢夾，為行動用戶提供一個通過行動電話進行交易支付和身份認證的途徑。用戶通過撥打電話、發送短信或者使用 WAP 功能接入行動支付系統，行動支付系統將此次交易的要求傳送給 MASP，由 MASP 確定此次交易的金額，並通過行動支付系統通知用戶，在用戶確認後，付費方式可通過多種途徑實現，如以信用卡進行簽帳、行動虛擬帳單、用戶電話帳單等，這些都將由行動支付系統(或與用戶和 MASP 開戶銀行的主機系統協作)來完

成。行動支付如配合 EMV 晶片卡設計，並與強勢的通路商結合，將直接影響原本由銀行經營的支付業務[48]。

交易程序簡單方便是行動付款第一個成功關鍵因素，如同巴克裏(Buckley)行動付款第一定理所述：如果交易程序比信用卡或現金支付要來得複雜，那麼行動付款就永遠不可能成功。其他左右行動付款成功與否的關鍵因素還包括：安全、可靠與私密。行動商務市場如要擴大，許多相關的配合機制需先解決，付款就是其中一個重要的議題，唯有在安全金流機制的搭配之下，行動購物市場才能真的起飛。目前行動商務發展的阻礙原因有三：安全機制尚不足以對帳務與交易資訊作足夠的防護；其次是欠缺全面、普及且一體適用的付款模式；另一個因素則是尚未出現足夠大的市場規模可以支撐服務供應商的營運成本，並滿足消費者低成本的考慮。[49]

以付款週期來看卡片產品，大致上可分為：

(一) 信用卡：先消費後付款，用戶先向行動電話業者預存信用卡資料，待交易時，透過行動電話或網頁進行身份及額度的認證後進行付款(認證時持卡人須輸入信用卡背面後三碼)。整個交易過程皆以 SSL 的技術對傳輸的內容進行加密。此付款方式較適用於大額的付款，額度上限依發卡銀行所核為準，任何信用卡可使用的地方都可使

[48] 一旦殺手級通路先後發展出專屬的儲值卡系統，並利用晶片卡的技術特點，從事轉帳、消費等業務，屆時銀行在支付工具的優勢何在？當然在法規的約束下，現階段對銀行仍有一定的保護，但不管是從技術上或是實務上來說，封閉式的儲值卡要跨出單一通路的門檻並非無法克服，但當夠份量的儲值卡應用形成後，要求使用更便利的民意將會讓政府或金融機構很難自外於這股趨勢。因此銀行在晶片卡的應用應該扮演領導的角色，而不應僅是採取防禦性的作法，否則挾帶強大通路影響力與行銷資源的殺手級通路，將會是銀行在支付業務上的新勁敵。Visa 目前正在開發行動支付系統，未來只要擁有一隻行動電話與 Visa 卡，可以立刻透過行動電話購物並完成交易，讓支付環境更爲輕鬆方便。參見二 OO 五年智慧卡博覽會明日在台北國際會議中心開幕，工商時報，2005/5/4。

[49] 台灣區電子電機同業公會,新世代行動生活應用國際研討會(通信產業聯盟 RFID 交流會長王嵩峰會議中之發言)，http://www.teema.org.tw/publish/moreinfo.asp?autono=2639, 最後瀏覽日期:2005/11/16

用為其優點。惟對於商家沒有特殊的利基、所得獲得之帳務處理費較低、有呆帳的風險；

(二) 行動虛擬帳號：可透過行動電話或行動電話業者網頁申請此虛擬帳號。此虛擬帳號即為銀行代碼+行動電話號碼。用戶得此虛擬帳號後應先預存一定金額，方得使用。使用時，得透過行動電話或網頁進行付款，傳輸過程皆以 SSL 的技術進行加密。預存現金，轉帳時須輸入預設密碼。較適合中額的付款；額度上限新台幣一萬元(財政部規定)；較適用於 P2P、網路拍賣及低於新台幣一萬元以下之消費。此方式係為了符合現行法規須與銀行異業合作、沒有呆帳風險；

(三) 電信帳單：透過每月電信帳單來付款。較適用於小額的付款；每月額度依各家行動通信商所訂；較適用於電子商品。須花大錢在建置帳務處理系統、較高之營運成本、有呆帳風險(因額度有上限，所以風險亦有限)。

二、IC 智慧卡

智慧卡(Contact-less Payments)的應用已屢見不鮮之際，如：香港的八達通卡(Octopus)可在交通工具與便利商店使用，其利用近距離無線通訊傳輸技術(NFC)，結合電子錢包與行動付款的概念，將行動電話變成日常交易支付的便利工具。2005 年 12 月，經濟部通訊產業發展推動小組計畫將與行動電話、金融、電信、系統平台等十四家業者代表，共同簽署近端行動交易服務計畫聯盟合作備忘錄，希望透過跨領域的合作，共同推廣台灣在行動商務的應用服務[50]。這項計畫預定

[50] 在這項合作計畫中，經濟部與台北智慧卡公司將擔任計畫聯盟的統籌與管理角色，中華電信、台灣大哥大、遠傳電信等電信業者負責電子錢包加值及行銷推廣工作，明基負責 NFC 相關的行動電話設計及開發，萬事達卡、威士卡負責信用卡付款機制的建立配合，台灣飛利浦則提供核心的 NFC 晶片模組技術，最後由台北捷運公司進行實際的商業營運。主要內容是開發 NFC 相關技術的行動電話，結合捷運與公車等大眾運輸工具，與自動加值、上網加值、帳務等系統整合，加上行動電話購物的小額付款，建置一個近

在今年年底前，能夠在台北的捷運站內開始運行。遠通電收也預計在明年啟用的高速公路電子收費系統服務上，透過近距離無線通訊傳輸(NFC)技術來進行收費動作。遠通電收估計，透過此項收費方式，未來行駛高速公路全線從南到北，將可節省四十五分鐘車程。

儘管目前加入該計畫的國內行動電話業者，以明基為主，但有鑒於i-mode FeliCa 在日本引起的旋風，其他行動電話業者也將順應這股潮流，陸續投入相關投資與開發的工作，在不久的將來，智慧晶片行動電話勢必將掀起行動電話的下一波革命。[51]

另根據日本 FujiSankei Business i.網站報導指出，日本行動通訊業者 NTT DoCoMo 將於 2005 年 12 月 1 日正式推出行動電話刷卡服務「iD」，日後行動電話用戶無需攜帶信用卡，透過行動電話的內建晶片即可刷卡購物。DoCoMo 的「iD」服務係與三井住友信用卡公司合作推出，2006 年春季 DoCoMo 將另推出專屬的信用卡服務，DoCoMo 預估日後信用卡事業的手續費收入即可高達 1,000 億日圓(約 8.5 億美元)。行動電話用戶使用「iD」服務僅需下載軟體，業者將免費為用戶的行動電話增加信用卡功能。用戶購物時，將行動電話往讀卡機一刷，即可支付 1 萬日圓以下的小額帳款。而超過 1 萬日圓的帳款則須經過鍵入密碼，確認為當事人的認證作業。三井住友信用卡公司目前正積極在便利商店、家電量販店等處設置讀卡機，預計 1 年後普及的店家數將達 10 萬家。DoCoMo 先前推出的電子錢包服務，至 2005 年 11 月 6 日止，用戶數已突破 700 萬戶[52]

端行動交易的新營運模式，藉以帶動台灣行動商務應用的風潮。

[51]來源：台灣區電子電機同業公會網站
http://www.teema.org.tw/publish/moreinfo.asp?autono=2639

[52] 企業 IT 新聞，DoCoMo 12 月推行動電話刷卡服務「iD」 透過行動電話內建晶片即可刷卡購物，
http://office.digitimes.com.tw/ShowNews.aspx?zCatId=163&zNotesDocId=68E8CE5B6E2E8C88482570B500435966，2005.11.11 。

政府於「數位台灣挑戰 2008 國家發展計畫」之 e 化交通的規劃已明確揭示朝整合國內交通 IC 智慧卡應用之方向發展。IC 智慧卡(又稱儲值卡小額消費)的應用，隨著晶片卡的技術發展而有不同的商業模式出現，初期以企業應用為多，包括：零售業或百貨業的禮券功能儲值卡，台灣過去幾年也出現許多與校園卡結合的應用模式，其卡片加值或消費之操作方式多為接觸式作業。目前全球儲值卡小額消費應用最多最廣的領域，當屬非接觸式的交通電子票證，隨著交通建設之發展，交通票證儲值卡幾乎成為人們日常生活中不可或缺的一張卡片，國內的台北捷運、高速公路、高速鐵路及高雄捷運等皆引領趨勢。然而，隨著發卡單位增加，消費者必須購買個別儲值卡，多卡不但攜帶麻煩，也常因商店搬遷、企業關閉、或遺失卡片，而造成消費者權益受損之情形，因此有了多功能儲值卡的興起。多功能的異業儲值卡係指一張儲值卡即可滿足消費者跨產業、跨區之需求，同時卡片可使用於接觸式[53]與非接觸式[54]設備。

就現行支付商業模式大約可分為下列幾類，說明如下：

(一) 國內市場

1、交通 IC 智慧卡(單一產業使用)

目前台灣交通運輸上使用 IC 智慧卡付費將趨於多元化，倘若無法整合，未來民眾搭乘各種運具從北到南，恐怕要換上許多卡片才能

[53] 接觸式指讀卡機必須接觸卡片，並利用接觸面由讀卡機提供讀寫動作所需的電源與時脈訊號，讀取卡片資料。接觸式的卡片讀寫方式速度較慢，且如果卡片接觸面受到污染，可能會影響資料的讀寫，這是接觸式卡片的一項缺點。不過接觸式的卡片通常具有較高的正確性。目前國際標準組織針對接觸式晶片卡制定的標準爲 ISO/IEC 7816。

[54] 非接觸式卡片除了晶片之外，還包含一個隱藏的天線，通常圍繞在卡片的周圍並與晶片連接。利用讀卡機所發射出的電磁波，即可與卡片進行無線傳輸，達到讀寫卡片的目的。利用這種方式，讀卡機不需要與卡片接觸，僅需維持在數公分的感應距離之內，就能夠完成驗票的程序。非接觸式的卡片具有處理快速的優點，且因爲晶片隱藏在卡片當中，即使卡片表面受到污染，仍舊不會影響其正常功能。國際標準組織 ISO/IEC 對於非接觸式的卡片亦訂有多項標準，其中 ISO/IEC 14443 是廣泛用於交通票證的非接觸式卡片標準.。

到達目的地，其更凸顯票證整合的迫切性。全世界的交通票證系統之發展趨勢目前均朝電子錢包方向設計，而交通部也於民國 92 年 8 月公佈新版「電子票證系統之多功能 IC 智慧卡規劃書」，希望能達成交通一卡通的便利。然國內限於金融法規限制，暫時無法發展；不過由技術層面來看，目前國內發行之交通卡幾乎都是非接觸式智慧卡(除了 Mondex 之外)，因此未來台灣在運用票證技術整合上已具基礎，只要相關法令通過，實現「一卡行遍天下」的理想將指日可待。

以下為國內幾個大型交通電子票證系統之介紹：

A. 悠遊卡[55]

大台北地區的交通 IC 卡「悠遊卡」於民國 91 年發行迄今，已超過 500 萬之發卡量。卡片可使用於台北捷運系統、大台北地區之公車以及多處公有路外停車場，並規劃於民國 94 年底與銀行合作發行聯名電子現金儲值卡，使悠遊卡的應用範圍進一步拓展至跨業小額消費應用。

B. 台中市公車電子票證系統

台中市公車電子票證已於民國 93 年 8 月完成整體系統的整合與試運轉工作，並且命名為「台中 e 卡通」，正式上線營運。初期使用範圍僅包括台中、仁友、統聯、巨業、全航五家市區的客運業者，共計約 500 台的公車。該電子票證系統主要透過台中市政府及交通部之補助完成建置作業。在政府之相關政策推動下，未來「台中 e 卡通」

[55] 悠遊卡是台灣第一張大型交通 IC 智慧卡，今年二月並已突破五百萬張，這也是目前全球發卡量暫居全球第六的案例。悠遊卡目前應用範圍整合了台北捷運系統、台北市／縣聯營公車(含捷運接駁公車)及台北市公有停車場等三種繳費系統，目前亦正在試辦計程車及路邊停車計時器結合悠遊卡付費，預計將帶給民眾更多便利。使用悠遊卡不僅免除消費者準備零錢及攜帶多種車票的困擾，並可不斷加值，一卡使用多年，避免重複購票的麻煩，更有快速通關節省時間的優點。而預計在年底發行的悠遊聯名卡，將結合信用卡、悠遊卡與電子錢包，延伸小額民生消費的領域。未來悠遊卡也計劃提供更多其他交通、旅遊、民生消費等多樣化的電子消費服務，例如火車、長途客運、電影票、演唱會門票、加油站等。期待在未來突破法令的限制，真正落實「一卡在手，悠遊自在」的理想。

將協助中部其他縣市(台中縣、彰化縣、南投縣)之客運業者，整合建置公車電子票證系統。

C. 南部七縣市交通運輸卡

南部地區的「南台灣交通卡」將結合高雄市公車、高雄客運、屏東客運和旗津-鼓山渡輪的付費功能。未來將結合 Mondex 電子現金儲值卡，採取交通票證與小額消費結合的做法，提供用路人更多便利性。

D. 台灣高鐵電子票證系統

台灣高鐵規劃採用 IC 智慧卡與磁卡並行的電子化票證系統，將由台新銀行、台北富邦銀行及交通銀行進行收單作業，在票證種類部分，高鐵的票證將分為儲值使用的非接觸式 IC 智慧卡、單次使用的磁卡、結合旅遊行程的套票，未來亦可視需要發行紀念票等，和台北捷運系統的票證類似。台灣高鐵亦規劃以金融卡和信用卡的購票授權系統，讓旅客可利用金融卡或信用卡付款。

E. 高速公路電子收費卡

遠通電收[56]與銀行進行異業結盟，共同合作辦理聯名發卡業務。遠通電收的卡片規劃有兩種，即電子收費卡及 e 通卡，e 通卡將於次節電子錢包(現金儲值卡)中加以說明，高速公路電子收費卡，由遠通電收公司發行，屬於 Combi 卡，同時具有接觸式及非接觸式介面，單一功能，金額統一存放於非接觸介面，加值經由接觸式介面，經過高速公路扣款時，透過非接觸式介面，用於高速公路電子收費扣款，消費者可至特約商店購買、加值使用。

[56] 遠通電收公司接受國道高速公路局委託配合推動高速公路電子收費計畫，遠通電收公司由「遠傳」、「東元」、「精業」、「神通」四家公司組成，參考國外營運經驗並引進國外相關技術，將爲台灣地區用路人提供全新的高速公路電子收費服務。 根據遠通電收公司規劃，高速公路計次電子收費系統建置時間預定於今年底全部建置完成，並立即於明年初開始營運。將來高速公路電子收費全面營運之後，從北到南將可節省四十五分鐘的車程，大幅舒緩交通狀況。

2、電子錢包[57](現金儲值卡，得跨業使用)

A. 國外主要的電子錢包標準

目前世界上開放式電子錢包標準主要有四種：Visa Cash, Mondex, Proton 和沒有投入實際應用的 CEPS 。

(a) Visa Cash

Visa Cash 電子錢包卡有三種類型：一次性 Visa Cash 電子錢包卡、可儲值的專用 Visa Cash 電子錢包卡，以及與其他應用共存於同一張銀行卡上的電子錢包卡。從誕生開始，Visa Cash 就一直在不斷地擴展其運用和市場，1999 年在英國里茲也進行了通過 GSM 網路，向 Visa Cash 電子錢包儲值的試驗。Visa Cash 同時也是美國 GSA 組織的多應用雙介面智慧卡專案中的一個應用。在西班牙的馬德里和巴塞隆納，Visa Cash 首次以非接觸的方式用於公共交通電子車票，如今，Visa Cash 電子錢包在西班牙可用於停車、打電話等。已擁有五千萬張電子錢包卡的西班牙是目前全球為數不多的幾個電子錢包應用較為成功的國家之一[58]。

(b) Mondex

[57]電子錢包有兩種概念：一是純粹的軟體，主要用於網上消費、帳戶管理， 這類軟體通常與銀行帳戶或銀行卡帳戶是連接在一起的。二是小額支付的智慧儲值卡，持卡人預先在卡中存入一定的金額，交易時直接從儲值帳戶中扣除交易金額。本文研究的電子錢包是後者，即以智慧卡爲介質，能在多個領域支付的儲值卡。 通常情況下，電子錢包主要用於小額支付領域，所以電子錢包經常被理解成小額支付卡的代名詞。由於電子錢包不是法定貨幣，其使用的範圍與發卡機構的行銷手段及受理環境的建設密切相關，大面積推廣牽涉到更多的利益平衡，因此開放度有限，一般在小範圍、相對封閉的環境中應用比較成功。這一點在一些小的國家和地區顯得特別明顯，如香港、比利時。參見電子錢包應用與發展研究，
http://event.chinaunionpay.com/pages/showArticle.asp?CatID=2&SubCatID=4&ContentID=1009(last visited on 2005.11.25)

[58] Visa Cash 電子錢包目前在阿根廷、澳大利亞、巴西、加拿大、哥倫比亞、德國、香港、愛爾蘭、以色列、義大利、日本、墨西哥、挪威、波多黎各、俄羅斯、西班牙、臺灣、英國、美國等許多國家和地區得到應用。跟 Mondex 一樣，到目前爲止 Visa Cash 在很多國家和地區的應用是不成功的，例如香港、臺灣，目前都差不多已經停止使用。 見前註。

Mondex 是一種靈活的電子現金，它最大的特點是可以方便地實現卡與卡之間資金無追蹤地劃撥，從而充分保證持卡人的支付隱私。這也是 Mondex 電子現金最有爭議的地方。一些人認為銀行無法追蹤審計每筆交易，將提供犯罪者進行非法資金劃撥的機會；而且由於沒有銀行的審計追蹤，對安全性的技術實現要求也比較高。Mondex 與國際通用電子錢包規範 CEPS 協定不相容，但交易費用比較低。

(c) Proton

Proton 最初是由比利時的 Banksys (比利時全國的支付系統運營商) 開發，各家銀行發行的，由 Proton World 負責其發展。它與 Mondex 電子錢包最大的區別是每筆交易都可以被追蹤審計，目前大約有兩 千萬張 Proton 電子錢包在流通中，Proton 應用的地方主要是比利時，電子錢包可以在比利時的任何一台 ATM 上儲值。持卡人使用電子錢包之前，需要到銀行申請開通。商戶大約支付交易額的 0.7% 的交易費。2002 年，由於在歐洲推廣歐元，電子錢包的使用大幅上升，主要原因是比利時人不習慣歐元的硬幣，所以他們轉為使用電子錢包，Proton 電子錢包與 PC 機相連接的集成 Proton 技術的智慧卡讀卡器，提供了 PIN 碼校驗和交易金額確認的功能。用戶通過讀卡器附帶的 PIN 碼輸入小鍵盤所輸入的 PIN 碼將直接與智慧卡上存儲的 PIN 碼進行校驗，PIN 碼不會在網路上傳輸，也不會被 PC 機讀取，增強了持卡人進行網上支付的安全。在歐洲，Proton 是目前使用最廣泛的電子錢包。除了比利時以外，荷蘭、瑞典、瑞士都在使用，主要是因為存在像 banksys 這樣的銀行組織負責銀行間的合作和清算，但儘管如此，Proton 依然處於虧損狀態[59]。

[59] 見前註。

(d) CEPS (Common Electronic Purse Standard)

雖然，大部分的電子錢包專案在小範圍、相對封閉的環境中應用比較成功。但是如果這種智慧卡越過邊界，在更大範圍內使用，那麼電子錢包就會發展更快。例如，如果電子錢包能在整個歐元區使用，那麼單一貨幣對歐洲支付體系的促進作用將更加有力。1997 年，歐洲議會制定銀行標準時就提出了這個問題。ECBS 意識到不同的電子錢包方案需要一個統一的規範和標準，因此選出了一些電子錢包共有的功能，在其基礎上推出了通用電子錢包規範(CEPS)。CEPS 使用公鑰驗證和對稱密鑰加密，類似於 EMV 信用卡/付款卡。底層的電氣特性、相關協定和應用選擇功能與 EMV 一樣，但是應用功能(裝載、支付、退款、查驗資金平衡等等)是 CEPS 定義的。雖然現在完備的 CEPS 實現方案很少，但是，大部分電子錢包發行商都表示了對 CEPS 的支持。Visa Cash 在新標準中，已經符合 CEPS 的標準。 Proton World 也表示 Proton 最終將會被 CEPS 應用方案取代。

B. 目前國內有關電子錢包之應用

(a) Mondex 卡[60]

目前國內市場現有具跨業應用之 IC 智慧卡電子錢，首推萬碁公司推行之 Mondex 卡。為接觸式 IC 智慧卡，未來將配合 PayPass 功能，與南部七縣市交通運輸卡整合。Mondex 目前鎖定北部地區為發展範

[60] Mondex 現金儲值卡是一張隨身攜帶的電子錢包。僅需儲值在晶片內，就可直接插卡使用，使用時不需簽名。除了免找零、縮短購物等候時間的優點外，Mondex 卡可以循環儲值，當卡內儲值款項用完時，消費者隨時可自其信用卡帳戶中，將款項下載至 Mondex 晶片卡使用。此外，Mondex 附有鎖卡功能，只要消費者在讀卡機設備設定密碼，即可以密碼保護用戶的 Mondex 加值金不被盜用。民眾可至全省貼有 Mondex 標誌之特約商店消費。可以使用 Mondex 卡坐計程車、到便利商店買報紙、購買自動販賣機的飲料、簽樂透彩、買漢堡、喝咖啡、吃遍美食街，也可以透過 PC 讀卡機(PCSC 規格)及具有連線功能的電腦連上網路，使用 Mondex 進行線上購物、購買遊戲點數。摘錄自台北國際商銀-三合一晶片卡，http://www.ibtpe.com.tw/creditcardnw/mondex/help.htm 最後瀏覽日期:2005/11/16

圍，配合晶片信用卡之發行，目前發卡量超過 50 萬張。應用範圍包括電影院、計程車、便利商店及樂透彩等。

(b) 銀行 e 通聯名卡及 e 通卡

銀行 e 通聯名卡及 e 通卡均屬於 Combi 卡，金額統一存放於非接觸介面，加值經由接觸式介面，扣款可透過接觸式介面及非接觸式介面。為增加持卡人使用上之便利，並擴展 IC 智慧卡功能，以創造卡片應用之最大效益，遠通電收規劃與銀行共同發行「電子錢包」(現金儲值卡)將高速公路電子收費業務利用銀行「電子錢包」(現金儲值卡)進行扣款，並依據持卡人消費習慣與可承受風險之需求，規劃下列兩種類型：

1. 銀行 e 通聯名卡：遠通電收與銀行共同發行之聯名信用卡，具有信用卡及 e 通卡電子錢包(現金儲值卡)功能。
2. e 通卡：僅具有 e 通卡電子錢包(現金儲值卡)）功能。

依財政部「銀行發行現金儲值卡許可及管理辦法」第七條之解釋函規定，客戶持現金至特約商店進行加值，形同特約商店代替銀行收受存款，將與銀行法第二十九條有關非銀行不得經營收受存款之規定不符，因此 e 通聯名卡及 e 通卡於特約商店須以信用卡進行加值作業，而 e 通卡係依附於 e 通聯名卡下，故其加值須連結至 e 通聯名卡之信用卡帳戶。

3、一般企業儲值卡(單一產業使用)

市場上各企業自行發行之企業儲值卡種類繁多，而目前以 7-ELEVEN 為最成功之模式。7-ELEVEN 於民國 93 年底發行「i-Cash」，短短數月間發卡量已超過一百萬張。究其成功之主要原因，在於便利商店為小額消費之最重要應用通路，而 7-ELEVEN 掌握三千多點之消費通路，搭配其各項促銷商品後，成功吸引消費者買

卡使用。然而「i-Cash」畢竟仍是無法跨業應用，在其他便利商店聯合與銀行發行「電子錢包」(現金儲值卡)後，可能受到嚴重影響。

(二) 大陸市場及其他國家應用

1、香港八達通卡(Octopus)[61](現金儲值卡，得跨業使用)）

八達通卡是採用日本 SONY 所製造的智慧卡 FeliCa，它的應用範圍最初包括交通運輸方面的地鐵、巴士、渡輪、鐵路、停車場等，在 2000 年獲得香港金融管理局認可為「接受存款公司」後，擴展至多種小額付費的應用，成為真正得跨產業使用的「電子錢包」(現金儲值卡)，此為非銀行開放發行「電子錢包」(現金儲值卡)的案例。

2、上海公共交通卡(單一產業使用)

上海公共交通卡股份有限公司是由上海市城市建設投資開發總公司、上海市地鐵總公司、上海巴士實業股份有限公司、上海市輪渡公司、上海强生集團有限公司等 10 家單位共同發起组建，於 1999 年五月正式成立，負責建置涵蓋上海全市公共交通業務的卡片付費與清算系統。截至 2004 年 2 月為止，上海公交卡發卡量已超過一千萬張，約佔居民人口的三分之二。而卡片的應用範圍除了大眾交通運輸之外，也擴展至其他領域。為方便市民減少卡片使用數量，上海公共交通卡公司於 2003 年推出了將公共交通卡用於住宅區門禁系統的試辦計畫，除了公交卡原有功能外，並提供住宅開發商用於住宅區刷卡開門。在區域整合方面，公交卡除可用於上海地區之外，同時可以在無錫、蘇州兩地使用。

3、法國的電子錢包計畫

[61]八達通卡是由香港地鐵公司邀集其他四家運輸業者所籌組，統籌整體系統的設計審核、計劃管制、合約管理和系統營運的工作，系統於 1997 年正式營運，至 2003 年底的發卡量已經超過一千萬張，每天平均交易量約八百萬筆，交易金額達五千四百萬港幣。

法國人是將智慧卡應用於銀行卡的先驅，到目前為止，推出了的電子錢包試驗專案主要有： Modeus, Moneo 和 Mondex。Modeus 是一種雙介面卡，它在一張卡上集成了電子錢包、公交電子車票和其他應用，由法國的四家金融組織和兩家交通機構共同運行。Modeus 的非接觸介面的電子車票用於乘坐地鐵、輕軌和公共巴士，而其接觸介面的電子錢包將可以在車站附近的商店或公共電話亭使用，Modeus 還可以用於高速公路、停車場以及市政設施的收費。Moneo 是一張純銀行應用的電子錢包卡，它的特點是將 GeldKarte 電子錢包與已經在法國得到廣泛應用的 CB 銀行卡結合在一起。GeldKarte 電子錢包由德國的銀行組織 ZKA 開發，目前在德國已發行 5,000 萬張 GeldKarte 卡，GeldKarte 卡結合了信用卡功能和電子錢包功能，但其電子錢包功能卻沒有得到廣泛的使用。還有就是上面提到的 Mondex 電子現金。1998 年，法國的 Credit Mutuel 銀行率先與國際組織簽署協定，在法國發展 Mondex。Credit Mutuel 銀行是第一家推出以歐元為主的 Mondex 電子現金的銀行。在法國有近五千家分支機構，1,200 萬用戶，是法國最大的收單行和第二大發卡銀行，Mondex 電子錢包除了可以在傳統的零售商店使用，還用於網上支付。法國 CB 銀行卡組織的下屬機構 SFPMEI 專門負責法國電子錢包的試驗專案。其長遠目標是實現這三種電子錢包的統一。法國是 CEPS 的積極支持者，所以，最後法國電子錢包的統一標準必將是 CEPS 相容的。

綜上所述，針對消費者小額消費之普遍與使用塑膠貨幣之消費習慣，現今台灣之企業，確有發行跨業「電子錢包」(現金儲值卡)之需求，惟目前礙於銀行法及財政部「銀行發行現金儲值卡許可及管理辦法」之規定，非銀行業之其他企業，縱算其企業達於一定規模或甚至比銀行之規模更大，仍礙於法令限制，不得發行跨業「電子錢包」

(現金儲值卡)，就保護消費者之立場而言，以限制由銀行方得發行，抑或開放一定經濟規模以上之企業加入競爭，並訂定嚴謹的管理機制來管理，何者方是對消費者權益之最佳保障，值得相關主管機關重新思考此一議題。

三、現金儲值卡與行動支付結合

即將 IC 智慧卡(現金儲值卡)置入行動電話之晶片中，結合現金儲值卡與行動支付，使行動電話成為一個支付的工具，由於係使用 IC 智慧卡的技術，有較高的安全標準，對消費者資訊之保護較為周詳，由於現金儲值卡係屬於預付式故對企業而言，呆帳的風險較低，相對的對消費者的保障即比較受重視，故而依「銀行發行現金儲值卡許可及管理辦法」需由銀行方得發行，而要結合此二個新興電子支付機制，依現行法令仍須與銀行為異業結合，甚至仍應以銀行為主，電信業為輔。惟主管機關對於電信業者之各類要求，不論是在對其消費者資訊之保護或對其公司規模之要求，亦有一定程度以上之標準，故而電信業者是否願意於此類商業合作中居於輔助之角色，難免會有一番商業上合作談判之角力。惟若電信業者得與銀行達成一商業合作之模式推出現金儲值卡與行動支付結合之電子支付，對於消費者而言，仍不失為一便利且有保障之付款機制。

若於一行動電話中，同時有現金儲值卡之電子支付工具與另一行動支付工具時，電信業者仍得於消費者為交易行為時，以簡訊之方式通知消費者，讓消費者於交易前以回覆簡訊之方式選擇電子支付工具，並確認交易之成立，如此一來，不但可使消費商店與消費者間就交易行為是否成立之舉證較為容易，相信若電信業者與銀行願意共同

分擔系統建立所需之成本，此一新興的電子支付機制，將可提供消費者對電子支付方式有多樣之選擇。

四、現金儲值卡與信用卡結合

遠通電收為提供其高速公路電子收費之消費者另一個電子付款支付工具(針對可承受風險較高之消費者)，與銀行共同發行ｅ通聯名信用卡(如前述，非銀行不得單獨發行現金儲值卡)，該信用卡同時具有信用卡及ｅ通卡現金儲值卡功能，持卡人得以信用卡消費之方式，直接加值至該信用卡內之ｅ通現金儲值卡，免去因現金儲值卡之加值屬於收受存款之行為，而須至銀行臨櫃加值之不便利。且持卡人至該發行銀行現金儲值卡之特約商消費時，得選擇以現金儲值卡付款，若該特約商店同時亦得以信用卡消費時，持卡人除得選擇以現金儲值卡付款外，亦得選擇以信用卡付款。

五、小結

綜上所述，針對消費者小額消費之普遍與使用塑膠貨幣之消費習慣，現今台灣之企業，確有發行跨業現金儲值卡之需求，惟目前礙於銀行法及財政部「銀行發行現金儲值卡許可及管理辦法」之規定，非銀行業之其他企業，縱算其企業達於一定規模或甚至比銀行之規模更大，仍礙於法令限制，不得發行跨業現金儲值卡。

由前述電子錢包的討論得知，未來電子錢包必將朝向三個面向發展：(1) 標準趨向統一：自從 1999 年 3 月 CEPS 規範發佈，已經有 200 多個金融組織簽訂了許可協定，這些組織來自 30 多個國家地區，代表著超過 1 億多張電子錢包卡的發行量。可見相容性在電子錢包專案中越來越受到重視。雖然，電子錢包的使用往往從一個集中的城市

或行業開始，但如果不同行業和地區都發展自己的電子錢包，通用就成了一個重要問題。統一標準帶來的通用效果使得不同的電子錢包受理終端可以低成本共用，這是電子錢包跨行業、跨地區發展的重要前提。(2) 一卡多用或多功能卡：借鏡香港八達通卡[62]之相關經驗可知，八達通係一政府持股超過百分之五十之公營公司，且其股東主要成員為香港各大交通運輸公司，因交通幾乎係一般消費者每日生活上之必須消費，故其以交通為出發點，整合消費者其他日常生活之小額消費，而發展出一成功的跨業之現金儲值卡[63]。(3) 朝向遠端支付方向發展：電子錢包目前還大多用於面對面的交易場合，如在商戶消費，或乘坐公車。但隨著以網際網路為代表的新經濟發展，越來越多的人們把遠端支付看成電子錢包未來的一個重要發展方向。方興未艾的電子商務向遠端支付應用提出了前所未有的需求。未來的支付應用不僅包括基於網路的線上支付，也必然涉及與金融領域相關的銀行、證券、保險、郵電、醫療、文體娛樂和教育等眾多行業，市場潛力巨大。例如隨選視訊、行動商務、線上遊戲、遠端教育、遠端醫療、遠端諮詢、網上購物、遠端付費等。電子支付將隨著電腦和通信技術的發展，未來將通過網際網路構造更加快捷靈活的電子支付系統。

62八達通收費系統由香港地鐵公司(最大股東，擁有超過 50%股權)、九廣鐵路公司、九龍巴士有限公司(九巴)、城巴有限公司及香港油蔴地小輪船有限公司(油麻地小輪)合資成立的聯俊達有限公司開發和營運。該公司現已改名爲八達通卡有限公司，而油麻地小輪原持有的股份已轉由新世界第一巴士服務有限公司(新巴)和新世界第一渡輪服務有限公司(新渡輪)持有。雖然這是商業業務，但是香港政府卻是八達通卡有限公司的大股東，因爲香港政府擁有地鐵公司四分之三和九廣鐵路公司 100%的股份，參見維基百科，自由的百科全書網站，
http://zh.wikipedia.org/wiki/%E5%85%AB%E9%81%94%E9%80%9A，最後瀏覽日，2005/11/19。

63目前基於八達通卡的服務供應商有 40 多家，市民可以用八達通卡在 7-11 便利店消費，可以用它打公用電話，可以用它在飲料店買可樂，可以用它來付費停車，甚至有些學校的餐廳和商店也接受八達通卡，學生可以用它就餐或購買學習用品。目前有 7000 萬張八達通卡在使用中，每天約發生 600 萬筆交易，日交易量達 500 萬美元。

肆、小額付費機制面臨的問題

一、使用者的身份確認

傳統交易中支付者對現金的持有或銀行印鑑的保有，表彰其為金錢權利之所有權人，而實際的現金交付行為和經簽字確認的對票據的背書，則具有對支付行為的不可否認性。而對於小額電子支付，支付雙方並不見面，支付行為通過網際網路等遠端通訊手段實現，這就給對資金帳戶的確認和保證支付行為的不可否認性帶來一定的困難。

二、支付仲介的法律地位

在電子交易中一些不同形式的支付仲介孕育而生。這些支付仲介的存在於實務上有其必要性：一方面，支付仲介就不相識的支付雙方提供了具有相對可信性的第三方保障；另一方面，支付仲介積累眾多的小額支付，產生規模效應，從而在總體上降低了支付成本。但支付仲介也存在其法律地位、對電子交易行為擔保責任等等法律問題。

三、對支付行為的行政監管

電子交易中的支付行為在本質上是一種私法行為，但同時，此等私法行為不可避免的涉及公法領域，受制於一定的公共秩序和國家政府的監控，於是產生了諸如稅賦徵收和反洗錢等法律問題。

(一) 對線上交易的稅收課徵

通常交易必須交納一定的稅，這些稅收既可以是國家財政的來源(如：增值稅)，也可以產生保護國內經濟秩序的作用(如：關稅)。稅收徵收的依據，一般是以紙張形式存在的發票(雖然也可能使用其他材料)。如果小額電子支付在網際網路或其他遠端通訊系統中進行，那麼發票也就名正言順地變成了電子形式。這種電子發票對稅徵的益處是：一旦支付系統與稅務徵收系統連線，那麼任何小額電子支付行為將都處於稅收監管之下。

(二) 支付行為中對資金流的控制

大額的支付行為往往經銀行途徑，亦可通過銀行系統跟蹤資金的流向。而目前世界上主要的小額電子支付系統(如：Paypal)是游離在銀行系統之外的，難以跟蹤其內部資金流向(數千萬的用戶的支付行為在其內部結算化解)。這就造成國家對資金流向控制的困難，也讓犯罪分子的洗錢行為帶來可乘之機。這一方面的技術措施和法律規範還尚待研討。

伍、消費者觀點論小額付費機制

在國內信用卡(Credit Card)、儲值卡(Stored Value Card)、預付卡(Pre-paid Card)或金融(扣帳卡)(Debit Card)，此類用來做為小額支付之工具，隨著利用率及普及率的升高，發生使用爭議的案件亦時有所聞，而成為消費者權益保障的重要議題。

一、 權利受損之態樣

此類電子化小額支付工具，之所以使大眾感覺消費者權益有受到侵害的疑慮，可歸納為下列幾項原因：

(一) 客戶在申用時未能詳細閱讀約定條款或使用規則，而金融機構則多以交付法令要求的文件代替具體說明。

(二) 交易筆數頻繁，但金額小，且交易時間短暫，故客戶較少保存交易記錄或證明。

(三) 處理交易之一方為客戶個人，另一方為商家的最基層服務人員，或甚至為無人的自動化服務設備，以致一旦爭議發生當時未能即時處理或保全必要證據。

(四) 金融機構自身系統安全及保密措施偶有疏失，造成資訊安全及客戶隱私受損之問題，會造成媒體及民意代表高度報導及重視。

(五) 由於電子化小額支付工具所針對的是額度較小之交易，是故，諸如預付卡及儲值卡並未有身分認明之功能，也就是說，這類支付工具大多數不具有識別性，當卡片遺失或是被竊，消費者只能自認倒楣。這類不具有身份辨識的支付工具或許便於交易，但也引發其他問題，像是支付工具因被竊或遺失而遭他人使用，這些都會使消費者權益處於一種不可回復之狀態。

為降低使用小額付款工具之風險及對消費者權益之負面影響，主管機關已責成金融機構在今年內要將信用卡及金融卡全面晶片化，利用晶片(chips)的大量儲存及運算功能，應可使儲存在晶片中之個人資料及交易記錄，受到較目前磁條卡更好的加密機制所保護，而可減少個人資料遭盜用、交易被冒用等風險。相對的，配套法令及交易規範亦應該配合修訂，方可在技術面及法令規章面，均可建構出一個安全交易的環境及制度。

二、 現行法令規範

由於我國並無針對小額電子支付的立法，如美國的聯邦電子資金移轉法(Electronic Fund Transfer Act)，而我國僅有在刑法中分則針對偽、變造信用卡、金融卡、儲值卡等支付工具之行為，及將不正確指令輸入電腦或其相關設備等行為分別單獨之罪名及刑罰(刑法第 201-1 條及刑法第 339-3 條)。此外，相關規範則是以法規命令，定型化契約範本，及業者自律公約的方式行之，茲分述之：

1、法規命令

金管會銀行局(前身為財政部「金融局」)基於銀行法第 47-1 條及第 42-1 條之授權，分別對信用卡業務制定「信用卡業務機構管理辦

法」[64]，對現金儲值卡業務制定「銀行發行現金儲值卡許可及管理辦法」[65]。另外，對於利用自動化設備提供遠端(即非臨櫃)之付款、轉帳、提款等交易，另制定「金融機構辦理電子銀行業務安全控管作業基準」[66]作為銀行電子銀行業務之最基本安控標準。最近則針對現金卡此類小額借款之工具，採用對信用卡業務類似之管理標準，制定「金融機構辦理現金卡業務應注意事項草案」[67]。

2、定型化契約範本

主管機關責成銀行公會提出保障持卡人權益為出發點之「信用卡定型化契約範本」[68]，供所有信用卡業者持用，業者如要修改或變更條款，則提出之內容不得低於上述定型化契約範本對消費者的保障。相同模式也採用在電子銀行業務，銀行公會提出「個人電腦銀行業務及網路銀行業務定型化契約範本」[69]，各家銀行在申請開辦電子銀行業務前均應備置依該範本所制作之契約條款。此外，行政院消費者保護委員會依消費者保護法第 17 條之規定，請主管機關金管會銀行局提出「信用卡定型化契約應記載及不得記載事項」，亦屬之。

3、自律公約

銀行公會下設信用卡業務委員會，全體信用卡發卡機構(不以銀行為限)均參與並共同制訂關於行銷、催收方面之自律公約[70]。另外銀行公會授信業務委員會也針對現金卡的行銷等業務制定自律公約，責成全部發行現金卡的金融機構得以遵行。

---

[64] 中華民國 92 年 10 月 7 日報 92)台財融(四)字第 0924000888 號令修正「信用卡業務管理辦法」，並修正名稱爲「信用卡業務機構管理辦法」。詳參附錄一。

[65] 財政部於民國 90 年 10 月公布。詳參附錄二。

[66] 於 2000 年 8 月中華民國銀行公會報請財政部核定。詳參附錄三。

[67] 詳參附錄四。

[68] 詳參附錄五。

[69] 詳參附錄六。

[70]「中華民國銀行商業同業公會全國聯合會信用卡業務委員會所屬機構辦理信用卡業務自律公約」，財政部八十九年八月三十日台財融第 89747200 號函准予備查。

三 、法令規範之檢討

1、 規範之一致性

上述法令規範之目的均在要求銀行應建立安全的付款機制，並將交易風險大部份由銀行負擔，以保障客戶的權利。此種精神雖可見於上述法令規範，但由於並無一完整的立法(例如：美、英、德、日等國均有「消費信用法」或「消費信用保護法」)，而由個別主管機關基於職權個別發布，以致於實務上曾發生銀行局認可信用卡定型化契約範本內容，但行政院消費者保護委員會有不同意見而需修正之案例，在具體案例中又偶有法院仍會認為「違反平等互惠原則」而應無效的情形。例如：定型化契約範本中的信用卡遺失被竊時，持卡人應否負擔一定時期，或一定金額之損失？以促使持卡人提高注意；未成年之副卡持卡人是否應對正卡持卡人之信用卡負帳應負連帶責任；以及特約商店不能提供服務之損失，究竟由持卡人、發卡行或收單行負擔？

上述問題，過去幾年來，都曾因發生幾件個案受到大眾關注，或法院採取不同見解，以致使用信用卡定型化契約範本經歷多次修改，迄今尚不能預知未來是否仍有修正之可能及必要？使發卡機構與客戶間，權利義務及風險分擔處於不確定的狀態。此點在有消費信用立法的國家因法律條文已有明文規定，故行政機關或法院之解釋不會偏離或超越法律，使法律的規範功能可充份及穩定發揮，而不致於會因不同主管機關因不同立場採不同解釋，造成規範內容不確定的現象。

2、電子銀行交易風險分擔機制亟待建立

「個人電腦銀行業務及網路銀行業務服務定型化契約範本」雖為銀行公會所提範本，並經銀行採用，惟其中許多重要條文，行政院消

費者保護委員會認為對客戶權益保障仍屬不周而請銀行局重新研究，再次造成該「範本」未來仍有大幅變動，銀行應配合修正之可能。

消保會請銀行局再行研議的問題，主要在於交易風險的分擔及舉證責任。原範本第 12 條將電腦駭客入侵造成損失雖規定由銀行負責，但卻要求客戶負舉證責任。範本第 14 條約定「雙方同意依本契約傳送或接收電子訊息，因可歸責於當事人一方之事由，致有遲延、遺漏或錯誤之情事，而致他方當事人受有損害時，該當事人僅就他人之積極損害(不包含所失利益)及其利息負賠償責任。」根據該條之解釋結果，則將來網路交易中若發生可歸責於擬連結之銀行或跨行機構之事由，以致擬進行之交易不能完成，將該事由將被認定為不可歸責於銀行之事由，則依據範本 14 條客戶僅得向該等機構求償，而無法向銀行主張損害賠償。

此等規定相較於信用卡定型化契約範本，確實對消費者較不利，而有商榷的餘地。惟為何同樣由銀行公會提出之範本，但對於第三人之行為造成交易損失風險的規定，信用卡定型化契約與電子銀行定型化契約中對於風險分擔及責任卻不盡相同，實值深思。

信用卡交易，係在一個支付體系(例如：VISA, MasterCard)所制定的交易授權(authorization)，交換(clearing)及清算(settlement)的相關規則下進行，交易中涉及的風險，例如：第三人詐欺、冒用、特約商店詐欺、或發卡、收單機構倒閉等，均已明確規定責任歸屬及不能歸屬時損失分擔的機制。由於參與此種支付體系的機構均已明確得知其責任及風險，而可加以評量，所以有能力在處理與客戶間法律關係及爭議時，負擔較多損失，因損失發生之可能性及範圍，均可客觀量化而為可控制之損失及風險。

反觀目前經由網際網路建構的網路銀行系統，如要進行一筆跨行小額支付，其交易流程至少會經過二家銀行的系統(接受客戶指示啟動交易之銀行及收到指示進行轉出或轉入之銀行))及專責處理跨行交易資訊的財金資訊公司，電子訊息會經由網際網路至財金資訊公司之加值網路，傳遞至銀行專屬網路。由於沒有任一家銀行可以全程控制上述單位及網路的全部風險，在尚無一套完整而合理的風險分擔規則之前，銀行對於承擔的風險及損失難以量化評估，於是在處理與客戶間風險分擔的條款時，將舉證責任轉由客戶負擔，把可歸責銀行事由縮限，對客戶而言並不公平。

欲根本解決此一問題，應是比照國際信用卡組織建立的清算規則，由銀行及財金資訊公司共同建立一套明確的交易風險分擔規定，使銀行可瞭解其承擔的風險後，由客戶直接往來之銀行先行承擔駭客行為，或其他第三機構應負責事項所造成之損失後，再由該銀行依上述銀行間風險分擔規定，進行內部求償，應為較合理的風險分擔機制[71]。

3、監理方式的商榷

目前對小額支付的管理法規，皆採取選擇性機構的管理方式，例如：「銀行發行現金儲值卡許可及管理辦法」管理對象限於銀行，而不適用於百貨業或異業務盟發行的電子式禮券或儲值卡。「信用卡業務機構管理辦法」，僅適用於銀行及專案發卡公司，而不適用於百貨公司發行的卡片及店內卡(private label card)。於 2005 年 4 月 29 日公佈之「金融機構辦理現金卡業務應注意事項草案」亦僅適用於銀行，而不及於民間小額借貨業者，或擬議中之「融資公司管理條例」之融資公司。

[71] 林繼恆著「信用卡業務及法務之理論與實務」增修訂二版，頁 131 至 136。

上述情形，造成個別法規中提供對消費者權益的保障，僅及於受該法令規範機構往來之消費者；然而，非受該法令規範之機構所提供之小額付款服務，更應受到規範以保障弱勢消費者的權益，但卻因非各該法令所規範之機構，反而使消費者不能得到合理保障。

美、英等國對此種小額支付或小額信用之管理，以消費信用法或消費信用保護法對消費信用之行為加以管理，而非僅對特定身分之機構進行管理，如此方可週延保障消費者權益，此點實可供我國借鏡[72]。

[72] 林繼恆，小額支付的法律關係，財金資訊股份有限公司，http://www2.fisc.com.tw/news/MAZ/39/p3-3a.asp(last visited on 2005.09.10)

第四章　國外相關立法例

壹、國際清算銀行就有關電子貨幣、網路及行動付款相關調查

近年來因科技進步與金融市場之發展，發若出干新型支付工具。不論是國內或跨國之零售業，使用此等新型支付工具之交易數量及金額均日益增加。電子貨幣作為現金或小額付款之可能替代品，e-money 或 Electronic money 引發各中央銀行就其可能涉及中央銀行之收入、應採行之貨幣政策、對支付系統之管理等政策上爭論。針對此等政策爭論，G10 集團國家的中央銀行總裁於 1996 年，公佈其密切觀察電子貨幣及產品發展之意圖，並於必要時採取適當之措施。自 1996 年來，國際清算銀行(Bank for International Settlement, BIS)在支付及清算系統委員會(CPSS)之合作與協助下，已定期就全球之電子貨幣發展進行調查，以便協助各國之中央銀行。此等調查每年進行兩次。相對於電子貨幣，近年來以網路與行動電話方式付款急速增加，支付及清算系統委員會於 2002 年底在會員國發動一次調查。支付及清算系統委員會認為，網路與行動付款所涉及之央行政策爭論，與電子貨幣所引發之爭論相似，有必要在公共調查時一併列入。2004 年 3 月國際清算銀行支付及清算系統委員會針對電子貨幣、網路及行動付款等新支付方式做出調查報告[73]。該調查包含兩種類型之支付產品。第一類包括可儲值之電子貨幣(electronic money)，其形式包括儲值卡(stored value cards)及儲存於電腦記憶體中的電子代幣(electronic tokens)。此類電子貨幣須與可進入客戶帳戶之支付工具區分。第二類則包括網路與行動付款(mobile payment)，其定義主要依據付款指示(payment instruction) 進入付款系統之管道。

[73] 原文請詳參附件。

1、電子貨幣

於該調查中，電子貨幣延續以往之定義[74]，係一儲值或預付之產品，於消費者所持有之電子設備中，儲存著可供消費者多用途使用之資金或價值紀錄。此一定義包括預付卡(有時稱為電子錢包)以及供電腦網路使用之預付軟體產品(有時稱為電子現金，digital cash)。於卡片類產品，預付價值一般儲存於附著於卡片上的微處理機晶片(microprocessor chip) --「智慧卡 (smartcard)」。另一方面，網路類產品則使用安裝於個人電腦內之特殊軟體儲值。將價值載入設備之過程，類似於從自動櫃員機中領取現金，而產品之使用則是透過將價值轉入商家之電子工具以購買商品。

本問卷調查請各國中央銀行就若干關於電子貨幣之政策爭點提出意見：

(1) 就電子金錢對貨幣政策與鑄幣稅收入方面，雖然短期間內電子貨幣對貨幣政策之施行不會產生重大影響，但中央銀行均抱持著須嚴密監控其發展的態度[75]。目前為止，並無中央銀行指出因廣泛採用電子貨幣致銀行票據價值貶損而對其資產負債表產生之負面影響。歐洲中央銀行(ECB)認為如有必要時，各國中央銀行可要求電子貨幣發行者維持最低準備金或自己發行電子貨幣，以維持其資產負債表之規模。如該調查報告所示，因電子交易之平均金額甚低，且卡片可儲存之最高金額亦非常小，故電子貨幣之浮動貨幣仍非常低。受調查之中

[74] In Article 1 of European Parliament and Council Directive 2000/46/EC (JU L 275 of 27 October 2000, pp 39-43) 將電子貨幣定義爲：「electronic money shall mean monetary value as represented by a claim on the issuer which is: (i) stored on an electronic device; (ii) issued on receipt of funds of an amount not less in value than the monetary value issued; (iii) accepted as means of payment by undertakings other than the issuer.」

[75]美國聯邦儲備銀行目前並於法律授權可要求非存款機構就其發行之電子貨幣結餘提出報告。英國之銀行就其所發行之電子貨幣蒐集部分資料，但芬蘭除一般銀行資料外，還向非自存款扣款之信用卡機構蒐集資料。

央銀行亦認為因電子貨幣而降低之鑄幣稅收入無關緊要，並無採取特殊政策以應對。受調查之中央銀行並無自己發行電子貨幣之計畫。

(2) 在一般法律爭議方面，發行電子貨幣產生監督發行者、監督付款系統、消費者及資料保護、與執行法律等問題。在歐洲，針對存款機構及新興信用機構(稱為電子貨幣機構，ELMIs)發行電子貨幣之完整、和諧之法規範架構由二個歐盟指令所規定：European Parliament and Council Directive 2000/46/EC[76]就電子貨幣機構之業務採取及尋求謹慎之監督，European Parliament and Council Directive 2000/28/EC 就原 2000/12/EC 關於採取及尋求信用機構業務之指令進行修正。歐盟各國之中央銀行表示其國內之法規已與此二歐盟指令相符。近來有香港及馬來西亞就電子貨幣進行修法，韓國、馬拉威及馬來西亞則尚在考慮中。部分國家就電子貨幣之發行另行頒佈法規[77]。

(3) 相關安全爭議方面，國際清算銀行於 1996 年 8 月出版之電子貨幣安全報告，主要強調電子貨幣產品之設計特徵及功能面，並分析此等產品之特定風險。歐洲中央銀行 (ECB) 於 2003 年 5 月的電子貨幣系統安全指標報告，則提供風險/威脅分析以及電子貨幣為避免此等風險/威脅所應符合之安全指標。此份報告可作為歐盟國家中央銀行監督電子貨幣之參考。香港貨幣主管機關(Hong Kong Monetary Authority, HKMA) 則要求申請主管機關授權發行多用途之儲值卡(multipurpose stored value cards, MPCs)時，須完成一份關於安全之問卷調查，以符合其要求之安全標準。新加坡貨幣主管機關評估發行銀

[76] 歐盟電子錢指令(E-Money Directive, Directive 2000/46/EC)中，電子錢(E-Money)的定義爲(1)將貨幣價值(monetary value)儲存於電子裝置中；(2)儲存於電子裝置的貨幣價值，不得少於消費找利用傳統通貨所購買的價值；(3)得作爲一種支付工具，而爲發行者和持卡者以外的第三人所接受。就發行機構而論，該指令的定義涵蓋傳統的信用機構(credit institutions)及電子錢機構(electronic money institution)。See http://europa.eu.int/comm/internal_market/bank/e-money/index_en.htm

[77] 例如臺灣。

行是否採行健全之安全制度以避免仿冒與詐欺時，亦採行近似之措施。於評估支付系統之運作與技術安全特徵時，奧地利中央銀行由技術團體協助，墨西哥則組成特別工作小組。

(4) 在電子貨幣發行方面，歐盟法規架構下，僅存款機構及經授權之電子貨幣機構得發行電子貨幣。所有歐盟會員國已將相關之歐盟指令移入其內國法規。在香港，以發行多用途儲值卡為主要事業者，依銀行法規就發行多用途儲值卡之目的，與經取得執照之銀行一同被視為接受存款之公司。在印度、墨西哥、奈及利亞、新加坡與臺灣，僅銀行得發行電子貨幣；加拿大、馬來西亞、瑞士與美國則未就發行電子貨幣之機構進行限制。若干國家如玻利維亞、泰國及委內瑞拉，相關政策仍定或審議當中。

(5) 在管理議題方面，多數中央銀行就其國內之支付系統具有管理功能，並就電子貨幣之發展進行觀察與分析，包括資料之蒐集、定期與發行者進行會議。其他情況則採取廣泛之活動以研究經營者與產品之組織、法律、行政與安全特徵。歐盟系統就電子貨幣之安全科技標準之設立與評估方法已建立一套和諧之措施[78]。在香港，則建議採取自律措施，由業界自行擬定執業標準並自行監督是否符合該標準，而 HKWA 僅就此等自律措施之施行進行概要性管理。

(6) 在監督議題上，前述的兩個歐盟指令就歐盟內之電子貨幣機構業務之謹慎監督，提供一個完善的規範架構。印度、奈及利亞與新加坡透過立法由中央銀行將電子貨幣之發行者限制在銀行。美國之聯邦銀行正更新銀行之審查程序以包含電子貨幣之發展及其相關之風險。迦納、韓國及泰國之中央銀行已提出法律修正案，以賦予中央銀

[78] See Report on Electronic Money, ECB, August 1998 and Electronic Money System Security Objectives, ECB, May 2003.

行特殊之監督資格。某些銀行，如墨西哥與瑞士，並未就電子貨幣公佈任何特殊法規。

(7) 在法律執行面，許多電子貨幣之安全特徵，包括卡片所得儲存金額設有上限等，使其較不受洗錢者以及其他犯罪者之青睞。關於洗錢之法規範亦適用於電子貨幣，因其亦為信用機構(credit institute)，且在許多國家信用機構係唯一之電子貨幣發行者。作為中央銀行管理功能之一部分，中央銀行著重研究電子貨幣之特徵，以確保其範圍不會擴大成為可能之犯罪工具。部分被堅持採行之措施包括：保留查帳存底(audit trail)、確定客戶身份、發卡僅限於信用機構之帳戶持有人等。調查顯示電子貨幣之跨國界使用尚未普及。雖然歐盟依關於電子貨幣謹慎監督之指令採行「單一證照(single passport)」，意即任何歐盟國之授權機關或監督機關得於其他國家提供服務，包括發行電子貨幣，但現存之電子貨幣產品仍未發展至跨國界階段。

2、在網路與行動付款方面

與電子貨幣相比，近年來網路及行動付款發展得非常急速，且已在電子零售付款中占有相當重要之一席之地。目前，將資訊與通訊科技結合以符合消費者需要之發展快速增加。網路付款可使用傳統的轉帳卡或信用卡或電子錢包工具。針對轉帳或信用卡交易，商家亦提供消費者非實體發票，使消費者可透過「電子化帳單及線上付款機制(electronic bill presentment and payment, EBPP)」付款[79]。而卡對卡交易之 P2P (person-to-person)資金移轉服務，已即將由 MasterCard 及 Visa 及公司引至全球。

行動付款則可以語音(voice access)、短訊(short messaging service, SMS)或無線上網(wireless application protocol, WAP)等網路通道完

[79] 目前有澳洲、奧地利、哥倫比亞、瑞典及瑞士使用 EBPP，正在考慮使用的有比利時。

成。無線上網科技使得行動電話之持有人可登記取得服務，以進入其銀行網站取得銀行服務。目前已使用之兩種商業模式為：從預付款中扣款或稍後與行動電話帳單一起繳付。某些產品以行動電話作為從既存付款工具(例如銀行帳戶或付款卡)開始及驗證交易之管道[80]。其他行動付款方式讓消費者得以儲存於行動電話之預付額付款，或將購買之商品/服務列於消費者的帳單中(pay ex post)。付款之身份驗證則以輸入密碼(個人身份號碼)為之。

調查顯示各國中央銀行一致認為，網路與行動付款之數量與金額對零售付款市場尚不具重要影響，故對中央銀行之重大政策議題未產生衝擊。然而，中央銀行仍就其法律、管理及安全層面進行檢視。若干國家之既存法規已就網路與行動付款為法律規範。若無特別法規時，則適用既存法規。而就網路與行動付款特別新立法或修正法規之國家有澳洲、玻利維亞、保加利亞、捷克、希臘、印度、日本、立陶宛、菲律賓、南非、臺灣及委內瑞拉。歐盟就網路與行動付款及一般電子商務之立法架構包括若干指令[81]。法律架構通常處理使用者與發行者間之權利與義務，消費者保護規定及電子簽章，少數則定有詐欺之罰則。

由於網路與行動付款交易之數量與金額仍甚低，中央銀行並未就此類付款之提出特殊管理議題。但考慮付款安全與效率之重要性，中央銀行就網路與行動付款之發展保持關注，以盡其一般之管理義務。網路與行動付款之安全議題均涉及避免濫用及防止未經授權使用者之詐欺。以網路或行動電話直接進入銀行帳戶之情形，需要高等級之

[80] 例如英國的 Vodafone m-pay card system 讓使用者可以自預先登記之付款卡中直接付款。

[81] The E-commerce Directive (Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market), the E-money Directive (Directive 2000/46/EC on the taking-up, pursuit and prudential supervision of the business of electronic money institute) and E-signature Directive (Directive 1999/93/EC on a Community framework for electronic signatures). For more details, see the ECB chapter.

安全措施。目前有不同措施，包括以網路為主的加密科技以及使用行動電話輸入密碼等。於 2005 年年底，全球將引進 EMV (Eurocard, MasterCard, Visa)標準，屆時信用卡及轉帳卡上都將加裝晶片，藉由密碼程序(cryptographic procedures)大幅提高在網路上使用信用卡之安全性，能有效避免偽造或變更。然而，部分國家於調查中指出，跨國電子付款之使用與發展，在安全標準上有再加強之空間。歐盟國家的中央銀行於評估整體電子付款與線上交易之安全時，考慮若干因素，例如普及性、身份認證/授權、完善、不可否認性(non-repudiation)與機密性。

貳、美國財政部貨幣金融局(OCC)為因應電子金融服務及行動付款近期提出之公告

一、 OCC Bulletin 2005-13

美國財政部貨幣金融局(OCC)、美國聯邦儲備委員會(FRB)、美國聯盟存款保險機構(FDIC)以及儲蓄監督局(OTS) 聯合發佈隨函所附之「未經授權取得客戶資訊之回應計畫及客戶通知之跨機構指導原則(Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice)」。本指導原則亦公佈於 2005 年 3 月 29 日之聯邦公告(Federal Registry)，並自公告之日起生效。

本指導原則解釋「建立資訊安全標準之跨機構指導原則[82] (Security Guidelines, 安全指導原則)」並說明各金融機構應針對未經授權取得該機構或其服務提供者所保存之客戶資料，實施應變計畫。

[82] This guidance will be published in the Code of Federal Regulations as a supplement to the Security Guidelines that are codified at 12 CFR 30, Appendix B. The Security Guidelines were formerly known as the "Interagency Guidelines Establishing Safeguards for Customer Information.

此一指導原則敘述應變計畫應包含之項目，如通知客戶關於其敏感(sensitive)資料遭未授權之人取得之程序。

本指導原則規定：「當金融機構知悉有未經授權取得客戶敏感資料之情事時，該機構應立即進行合理之調查，以決定該資料是有可能已被使用，或即將被使用。」若該機構認為不當使用客戶資料之情事已發生或可能發生，該機構應立即通知可能受影響之客戶。然若執法機構認為通知客可能妨礙對犯罪活動之調查，且以書面請求金融機夠暫緩通知客戶時，金融機構得延緩通知受影響之客戶。

客戶敏感(sensitive)資料，係指客戶之姓名、地址、或電話號碼，以及客戶之社會安全號碼(social security number)、駕照號碼、帳號、信用卡或轉帳卡號碼、或個人識別碼或進入帳戶之密碼。客戶敏感(sensitive)資料亦包括任何可能讓第三人透過網路進入客戶帳戶之資訊，例如使用者姓名及密碼或密碼與帳戶號碼。

本指導原則規定金融機構與各服務提供者之契約，應要求服務提供者就未經授權取得該金融機構之客戶資料之情事，採取適當之行動，包括發生此等情事時，立即通知金融機構，使金融機構得立即執行其應變計畫等。

本指導計畫亦規定，不論金融機構是否通知客戶，金融機構須通知其主要聯邦主管機關負責客戶敏感資料之部門。全國性銀行應通知其監督機關(supervisory office)。

當評估全國性銀行依「安全指導原則」建立之資訊安全計畫是否充分時，美國財政部金融局將考慮該銀行是否已依本指導原則建立並實施應變計畫。美國財政部金融局亦就相關之環境，考量各銀行是否依誠信建立與本指導原則相符合之應變計畫。美國財政部金融局得將

未依本指導原則建立應變計畫之銀行，視為違反安全指導原則，並構成聯邦法規第 12 篇第 1818 條之不安全與不健全執業。

二、 OCC Advisory Letter 2003-10

(一) 背景與目的

美國財政部金融局有鑑於新興網路標準(networking standards) 與仰賴未經授權之無線電頻率(unlicensed radio frequency)之產品，引起越來越多全國性銀行思考如何藉此等先進科技獲利；且全國性銀行可利用無線科技，以低成本且易於安裝之設備，建構區域網路(local-area-works)及個人網路 (personal-area-networks)。故美國財政部貨幣金融局於 2003 年第 10 號行政函令(Advisory Letter)中，就無線網路之風險管理(Risk Management of Wireless Networks)提出若干指導原則，供全國性銀行就保護公司資產、客戶機密資訊、達成服務水準需求、維持營運安全與健全，並確保符合法定安全期待之參考。

(二) 使用無線網路之潛在風險

視銀行運用科技之方式，無線網路對銀行造成風險之方式亦有不同。因無線網路標準持續不斷地產生與進化，使用者面臨如何取得必要專門技術與知識、以及是否及早採取新研發之標準，或等候已驗證之標準等挑戰。若銀行未能即時跟上變化中的標準，則可能面臨策略與信譽危機。銀行減低此等風險之能力，取決於

- 董事會與管理階層之有效監督；
- 與執行、管理無線網路計畫相關之有效管理策略與程序；
- 跟上科技發展之能力；
- 網路的可靠性與容量；
- 充足的商業持續發展計畫；

- 有效的銀行安全計畫；以及
- 對不良事件採行之監測活動與為降低風險採行之額外步驟。

有兩項與安全有關之挑戰，值得特別提出：無線網路的廣播特性與初級薄弱的加密標準。無線電波能穿越牆壁及門窗，因此無線網路能將數據資料傳播予該地區任何持有適當截取設備之人。此點為無線網路與有線網路之最大差別，並將使銀行暴露於重大之交易與信譽風險。此外，初期保護資料數據傳輸之加密標準「有線等效隱私(Wired Equivalent Privacy, WEP)」是出名的脆弱。不僅專家已破解 WEP 安全標準，且利用 WEP 脆弱特性之工具已問世。不受控制之傳播加上薄弱的加密標準，使得未經授權進入系統取得資訊之情事相當容易發生。也因此，有效的安全與高品質的風險管理日形重要。

(三) 風險管理之考量因素

美國財政部金融局意欲確保銀行董事會與管理階層對無線網路之有效監督，以及適切地控管因使用無線網路造成之風險層級。故就降低與控制因使用無線網路所伴隨之風險所涉及之安全、計畫管理及執行等重要因素進行討論。該行政函令之附件，則重點提示國家標準和科技機構(National Institute of Standards and Technology, NIST) 所提出，有關有效管理無線網路之風險管理建議。其中的關鍵措施包括：

- 於使用無線網路前，應先具備安全風險評估、合適的政策及充分的內部控制。
- 安全措施應保護銀行之網路及無線設備免於未經授權之進入、截取傳輸資料、揭露機密客戶資訊及其他漏洞威脅。
- 針對無線網路之安全測試計畫。
- 應針對服務水準協議之表現水準進行監督，以確保無線解決方案

之有效性。

- 於決定計畫是否成功時，執行及維護網路之擁有權總成本 (total cost of ownership) 或投資報酬率目標，包括增加之安全成本 (例如身份驗證、監控、更新、測試)，亦應一併考量。

(四) 無線網路安全

美國聯邦財政機構檢測委員會(The Federal Financial Institutions Examination Council)在 2002 年 12 月出版之「IT 審查手冊–資訊安全小冊 (IT Examination Handbook – Information Security Booklet)」中，略述銀行安全計畫中關於風險管理之程序。此一程序指出幾項關鍵步驟：風險評估、策略、控制、測試、監督及更新。因使用新科技可能致使現存之安全計畫失效，故在啟動新系統前(例如無線網路)，銀行董事會及管理階層須更新銀行之安全計畫，此點甚為重要。未更新計畫可能違反法令有關保護客護資訊之規定。[83]

1、施行使用者政策與程序

施行有效之無線網路安裝、使用政策與程序，以加強系統安全之重要性。因無線網路接入點相當容易設置，故無線政策通常限制銀行員工未經事前許可，建立自己的無線網路。未經授權之無線網路可能造成銀行網路安全與完整之高度風險。此外，有效之政策與程序將鼓勵銀行員工使用經核准之無線網路，並就不正常之網路活動提出通報。

2、指出可取得之資訊

[83] See OCC Bulletin 2001-8, "Guidelines Establishing Standards to Safeguard Customer Information." The guidelines mandate that banks protect certain customer information and amend its information security program before implementing systems. This requirement would apply to a bank adopting wireless network technology.

銀行應將明確指出可透過無線網路取得之資訊種類 (即已傳輸且可透過網路取得之數據資料)，以確保風險評估之正確性及安全計畫之合理性。

3、指出無線網路接入點

保持一份經許可且已佈署之無線網路解決方案[84]及網路接入點清單，以達成有效之計畫管理，此點甚為重要。此份清單將增強管理階層管理與更新設備設定、採用升級設備與修正程式、及管理網路與設備安全之能力。明確地指出無線網路與設備之系統建置圖(system architecture diagrams)亦有助於風險評估與安全測試之持續進行。

4、控制廣播區域

無線網路信號之廣播特性意指任何持有適當設備之人，皆得調準頻道、接收訊號，增加未經授權進入系統取得資訊之可能性。然而，此等威脅得藉由不同之科技予以降低，例如策略性的佈署網路接入點(例如建物的中央)，以強低廣播訊號之強度至最低需求強度，或不使用時將設備關閉等。方向性天線、訊號隔離及對無線網路接入點之實體保護等，均有助於控制廣播區域及避免未授權進入。

5、數據資料之加密

[84]無線區域網路 (WLAN) 之安全政策應考慮下列需求：

- 明確指出誰得使用無線區域網路科技；
- 明確指出網際網路之使用是否爲必需；
- 敘述誰可安裝網路接入點及其他無線設備；
- 提供網路接入點之地點與具體保護之限制；
- 敘述經由無線連接傳輸之資訊種類；
- 敘述於何種情形得允許使用無線設備；
- 界定網路接入點之安全設定標準；
- 敘述無線設備使用之限制，例如地點；
- 敘述網路接入點軟硬體之設定；
- 提供無線設備失竊申報與安全意外事故之指導原則；
- 提供使用加密與其他安全軟體之指導原則；
- 界定頻率及安全評估之範圍。

無線傳輸之加密可避免未經授權進入系統、使用設備或取得資訊。「有線等效隱私加密(WEP encryption)」提供一個安全層級以遏阻未經授權之進入，但此一加密措施被視為是相當脆弱之安全措施。較佳之解決方式是使用「端對端加密 (end-to-end security)」以維護數據資料完整性，並保護機密資訊之傳輸。一般而言，不論使用何種傳輸方式，端對端加密措施可自始至終保護資訊。例如使用虛擬私人網路(virtual private network, VPN)增加另一保護層級，以增強安全性。新興的電子電氣工程師協會(IEEE)標準則致力於提供另一種較強之加密，以彌補既存無線加密協定之缺失。簡言之，銀行使用之安全措施應與其管理階層之風險評估相呼應。

6、保持身份驗證控制

使用者與設備之驗証控制必需能保護系統之機密性與完整性，且降低使用無線網路伴隨之風險。使用者僅使用密碼作為身份認證，可能造成未經授權之第三人以猜測密碼或竊聽無線電波之方式，進入系統。因不確定使用者所在之具體位置，無線網路標準之薄弱以及無線通訊之廣播性質，此等風險可能需要較先進之科技，例如以記號為基礎(token-base)或以電子憑證為基礎的解決方案。新興之 IEEE 標準亦協助設備驗證之新科技(例如 Wi-Fi Protected Access or WPA)、增加安全性。

7、避免攻擊

無線網路與設備經常遭受跨國性的攻擊。防火牆、入侵偵查系統及防毒工具等皆能保護系統及設備免於攻擊。此外，於下班時間停止無線網路亦是一種保護措施。同時，限制實體接觸無線網路接入點，亦是避免故意或過失更改系統設定之重要措施。

8、監督脆弱之系統

有效的管理計畫應包括網路安全系統之持續監督、認證與軟體升級。積極監督系統之不正常活動可降低損害。

9、完成安全測試

日常安全測試計畫應包括無線網路系統，以確保銀行內運作之無線系統與裝置運作正常，且係銀行所授權者。

(五) 計畫管理實務

科技計畫管理之程序須考量無線網路科技及標準之快速進化。當新標準與產品問市時，採用早期標準與產品之銀行須取得必要之科技專業知識與技術，且須從本益比上考慮及評估繼續採行現行標準與產品以求穩定，或使用新標準與產品以求效率。

1、完成審查評鑑 (Due Diligence)

專案外包(outsourcing)可提供無線網路安裝、維修及測試所需之專門知識與技術。當專案外包無線網路時，因潛在之安全威脅，採取適當且充分之審查評鑑至為必要。

2、分析本益比

採用擁有權總成本(total cost of ownership)或投資報酬率目標等方式評量無線網路之成本與利潤，有助於總體計畫之管理。此等分析方式考慮預期利益，例如較低之設置成本、增加員工之生產力、擴張產品及服務、以即提供更佳之客戶服務。成本包括佈署及維護無線網路、取得軟硬體、增強身份認證條件、數據資料傳輸安全、例行維修、未符合服務水準合約要求、產品生命週期縮短及升級週級及獲得專門知識技術等所生之費用。

3、無線網路表現

預期網路容量　數據資料傳輸率以網路傳輸量視銀行採用之標準而有不同。典型之高傳輸率並不意味網路具備即時傳輸所需之傳輸量。因此，具體指出無線網路發展過程中之表現需求，即數據資料傳輸之種類與數量，是十分重要的。

4、瞭解網路可得性

網路可得性取決於未經授權之頻率，亦即某些頻率或許現在可使用，但不表示未來亦一定可使用。若銀行之無線網路發生與其他網路、設備或器具(例如微波爐、無線電話)相互干擾之問題時，銀行負有義務指出問題爭點並採取適當行動以達成其商業目標。

(六) 結論

無線網路提供全國性銀行另一種系統發展，但需要董事會與管理階層之監督。有效的無線網路管理包括維持充分之安全、確保適當的計畫管理及達成表現目標。美國財政部金融局要求董事會與管理階層在執行無線網路前先更新銀行之安全計畫，並監督安全計畫，以確保銀行具備有效之風險管理措施。本行政函令所提供之指導可幫助全國性銀行以更安全及健全之方式使用無線網路。

三、 OCC Bulletin 2005-24

(一) 背景與目的

網址偽裝(Website Spoofing)是指以詐欺方式，製作出一個完全相同或十分近似之詐欺網站，例如銀行網站。客戶通常是經由隨意寄發之詐欺電子郵件(phishing schemes)或網釣技術(pharming techniques)，被導引至詐欺網站，並被誘使提供資訊，例如網路銀行之使用者名稱與帳號、信用卡資料、或其他犯罪者得使用客戶帳號以進行詐欺或竊取客戶身份之資訊。網址偽裝致使銀行暴露於策略、營

運與信譽之高度風險，並危及銀行客戶之隱私，且使得銀行於客和暴露於金融詐欺之風險中。

美國財政部貨幣金融局(OCC) 2004 年第 24 號公告旨在提供銀行處理網址偽裝事件之指導原則。本公告著重銀行於發現網址偽裝事件時，為降低其自身及其客戶所受損害，得採行之措施。並明確指出銀行得向執法機關提供何種資訊，以協助不法活動之偵察。本公告並就美國財政部貨幣金融局於 2003 年 9 月 12 日出版之第 11 號關於「客戶身份竊盜:與電子郵件相關之詐欺威脅」之警告函，作進一步之說明。

(二) 應付網址偽裝之程序

銀行可透過執行本公告之身份確認與回應程序，以降低網址偽裝之風險。亦可透過指定並訓練特定員工負責針對此類事件作出必要且有效之回應，以降低網址偽裝帶來之衝擊。若銀行之網際網路活動採用專案外包方式，銀行可於契約中特別強調關於偵測、回報網址偽裝事件之程序，使其技術服務提供者回應此等事件之程序與銀行之內部程序相結合。

銀行得就網址偽裝事件事先與 FBI 及當地執法系統進行聯繫，以增強銀行應變程序之有效性。聯繫之對象應包括負責偵察電腦安全事件之適當部門與人員。有效的應變程序應包括尋求執法人員協助之適當時機，並就資訊之性質與種類、銀行可使用之資源以及執法機構迅速回應以保障銀行及客戶能力，進行記錄。此外，銀行可利用客戶教育計畫以降低此等網址偽裝之風險。教育內容應解釋與網路有關之各種詐騙手段，包括使用詐欺電子郵件以及網址偽裝等。且因此等詐欺

可能利用網站瀏覽器或作業系統之漏洞，銀行應考慮提醒其客戶安全地使用電腦的重要性。

(三) 偵測及資訊收集

銀行可透過監控銀行內部可得之資訊與搜查網路上非法或不當使用銀行之名稱與商標，增加其偵查網址偽裝之能力。以下為網址偽裝之警示清單：(1) 銀行伺服器在接獲電子郵件相關訊息時，由於此等電子郵件並非銀行寄發。某些情形，此等電子郵件可能包含詐欺網站之連結；(2) 檢視網站伺服器紀錄可能會發現可疑的連結網址，顯示銀行之網站已被複製或有其他不法活動正在進行；(3) 客戶撥打至客服中心或其他銀行服務人員之數量增加，或客戶直接呈報網址偽裝活動。

銀行亦得藉由在網際網路上檢索與銀行身份有關之資訊，例如公司名稱或銀行，以偵查網址偽裝。銀行得使用既有之搜尋器或其他工具，以監控網站、公佈欄、新聞、聊天室以及其他論壇，以確認特別公司或銀行名稱之使用。此等檢索可能會揭露近來與銀行名稱相近似之網域名稱註冊。銀行可自己進行此等監控，或與第三者締約，由第三者提供監控服務。銀行可提供網站連結或聯絡電話，鼓勵客戶提報網釣或其他詐欺活動。銀行亦可訓練客服人員確認並提報因網址偽裝所產生之客戶申訴電話。

若銀行確認其為網址偽裝事故之攻擊對象時，銀行應收集關於此事故之相關資訊，以便作出適當之回應。收集之相關資訊有助銀行確認並關閉詐欺網站，決定客戶資訊是否已外洩，並協助執法機關進行偵察。有時，銀行應尋求技術人員之協助，以取得此等資訊。以下為銀行應搜集之資料清單：

- 銀行得知其成為偽裝網址對象之方式 (例如透過網站、傳真、電話等管道取得)；
- 誘使客戶進入偽裝網站之電子郵件複本或其他溝通方式之文件影本；
- 偽裝網站的 IP address，其與該 IP address 有關之公司；
- 偽裝網站的網址及網域註冊資料；
- 偽裝網站 IP address 之地理位置 (市、州及國家)。

(四) 偽裝網址事故之應變

為有效回應偽裝網址事故，銀行管理階層應建立一套有組織且一致之措施。此等措施應包括關閉詐欺網站、取得詐欺網站內之身份資料以保護客戶，並保留任何可能有助於執法機關進行偵查之證據。銀行得採取下列步驟，以癱瘓詐欺網站並取回客戶資訊。採行部分步驟前，應先徵詢律師之意見：

- 立即與負責詐欺網站之 ISP 業者溝通 (包括以書面方式)，要求 ISP 業者關避該網站；
- 立即與任何與詐欺網站有關之網域名稱註冊者溝通，並要求取消該網域名稱之註冊；
- 向美國聯邦地方法院依「數位千禧年著作權法案 (Digital Millennium Copyright Act)」取得傳票，要求 ISP 明確指出詐欺網站之所有人，並取回客戶資訊；
- 與執法人員配合；以及
- 使用其他現存機制以呈報可疑之網址偽裝活動。

下列為其他銀行回應網址詐欺事故可採取之行動及法律文件：

- 銀行得致函予網域名稱註冊者，要求立即停止其不當使用銀行名稱與商標之行為；
- 若上述信函未發揮作用，銀行得依「統一網域名稱爭議解決程序(Uniform Domain Name Dispute Resolution Process, UDRP)」與不當使用銀行名稱與商標者進行協商。銀行得依 UDRP 要求網域名稱使用者停止偽裝網址之行為；以及
- 銀行可依「反網路侵佔消費者保護法(Anti-Cybersquatting Consumer Protection Act, ACCPA)」取得其他救濟。此法允許銀行立即依美國商標法 (Lanham Act) 第 43 條第(d)項採取行動。特別是，ACCPA 提供立即之禁制救濟，銀行毋須證明兩造之商品或服務相近似或混淆消費者

(五) 與美國財政部金融局及執法機構聯繫

若銀行成為網址偽裝事件之對象，應立即通知美國財政部貨幣金融局，並向 FBI 及其他適當之州或地方執法機關通報。銀行亦可上網向網路詐欺申訴中心(Internet Fraud Complaint Cente) 提出申訴：http://www.ifccfbi.gov。

為使執法機關就網址偽裝事件作出有效回應，銀行應依本公告提供必需之資訊以確認及關閉該詐欺網站，並逮補罪犯。此外，銀行亦可利用其他非正式之機制，通報並厄止此等詐騙事故。例如 “Digital Phishnet” (http://www.digitalphishnet.com/)，或以電子郵件通知聯邦貿易委員會 (FTC) spam@uce.gov

參、美國及香港有關儲值卡發行的規定

一、美國統一資金服務法案(Money Service Business Act, UMSA)

2000 年 8 月美國聯邦統一法制訂委員會(The National Conference of Commisssioners on Uniform State Laws, NCCUSL)通過了「統一資金服務法」[85]，針對網路金融的付款機制，該法除規定發行儲值卡的發卡人必須依法取得執照外，亦提出以下幾項重點的指標[86]：(1)「貨幣價值(monetary value)」的定義；(2)「儲值(stored value)」的定義；(3)「資金轉移(money transmission)」的定義。

(1) 貨幣價值方面，該法認為無論貨幣是否可以贖回，只要有兩方以上的大多數人的進行該貨幣的交換(a larger group than the two parties to the change)，即具貨幣價值。在該定義中，有關購物禮券(gift certificate)及其他付款機制(如學校的電子金融卡)，由於係由單一商家發行，將被排除於定義之外。

(2) 在儲值方面，該法承認以電磁記錄方式呈現的貨幣價值是一種儲值交易的媒介。不過有關單一用途的封閉型(closed-end)儲值系統(例如單純之大眾運輸儲值卡)則非本法規範範圍。換言之，適用範圍僅及於多用途儲值卡(即使用範圍必須擴及發卡人及持卡人以外的第三人)。

(3) 在資金轉移方面，該法包括在美國境內或境外經營(a) 出售或發行付款工具；(b) 出售或發行儲值；以及(c) 收受金錢或具貨幣價值之業務。

二、香港銀行業條例

在香港方面，香港的「銀行業條例」[Bank (Amendment) Ordiance Act 1997]中，對於「儲值卡」的定義有兩部分，第一，銀行業條例排

[85] 該法目前已有 Iowa, U.S. Virgin Islands, Vermont, Washointon 等州透過州法予以適用。
[86] See Jeffrey P. Taft, Mayer Brown & Platt, Uniform Money Services Act Covers Stored Value and Other Internet-Based Payment Mechanisms, August/September 2000, http://www.securitization.net/knowledge/legal/uniform.asp(last visted on 2005.11.20).

除單一用途[87]的儲持卡適用銀行業條例；第二，就多用途的儲值卡而言，發卡人或第三人必須提供一定的商品或服務，包括金錢或與金錢等值者在內。

另針對多用途儲值卡的監管，「銀行業條例」賦予金融管理專員監管多用途儲值卡發行的權力。監管制度的目的，是確保多用途儲值卡計劃及發卡人符合穩健標準。該條例規定：(1) 持牌銀行被視為已獲准發行或促進發行多用途儲值卡；(2) 如屬特別目的公司，而其主要業務是或將會是發行或促進發行多用途儲值卡，則可申請認可為接受存款公司(deposit-taking company)，以便獲批准經營該主要業務；(3) 金融管理專員可宣布某儲值卡或某類儲值卡就本條例而言，不屬於「多用途儲值卡」，以豁免這些儲值卡需要符合批准條件[88]；及(4) 發行單一用途儲值卡無須根據該條例取得批准。

除發卡人外，該條例亦引進「促進人」的概念。根據第 2(11) 條，促進人的定義是指藉由向發卡人提供有值代價而促進多用途儲值卡的發行的人，而該代價的價值決定了該發卡人就多用途儲值卡的定義所指而可承諾的範圍(不論是全部或部分)。這項定義包括創製電子價值並售予其他銀行，以便銀行把價值儲存在所發行的卡上的「創製者」。(這項功能類似發鈔銀行印製鈔票，然後售予其他銀行，以供分發予其客戶)。但就《銀行業條例》而言，向多用途儲值卡發卡人提供輔助服務的人士，例如廣告、收款服務或電子數據網絡設備等，一般不會被視為促進人。在制定這套監管制度時，金融管理專員力求在維持支付系統，以及整個金融體系的穩定，避免窒礙。

[87] 發卡人承諾(包括明示或暗示)，當持卡人提示該卡片時，發卡人會提供商品或服務，但不包括金錢或與金錢等值(money's worth)者。

[88] 目前香港的八達通卡即是經過香港金管局豁免後才發行的多用途儲值卡，所以不受銀行業條例中有關多用途儲值卡的規範。

為了達到上述第一項目標，並且鑑於只有持牌銀行才可直接使用香港的支付系統，因此條例規定只有持牌銀行才可發行用途不受限制，可用以購買任何貨品和服務的多用途儲值卡。這類儲值卡具有「被廣泛接納的購買力」，因此與貨幣非常近似。另一方面，根據第二項目標，非銀行發卡人亦應該有機會申請批准發行用途受到限制的多用途儲值卡[89]。

就行動付款機制，上述有關歐盟、美國及香港等法制，參考資策會科技法律中心 2005 年 11 月份之相關報告，整理表格如下：

圖表 5：行動付款之國外法制研究

	歐盟 (E-Money Directive, Directive 2000/46/EC)	**美國 (Uniform Money Services Act, UMSA)**	**香港 (銀行業條例)**
發行機構	● 傳統的信用機構 (credit institution) ● 電子錢機構 (electronic money institution) (Article 1. 3. (a))	依規定取得執照即得經營	● 依法與得執照、從事銀行業務的銀行 ● 依法取得認可的接受存款公司 (deposit-taking company) ● 被公告排除者
預收金額是否視為收受存款的行為	否	未規定	是
對儲值卡的規範範圍	限於多用途儲值卡 (Article 1. 3. (b).(iii))	限於多用途儲值卡 (Goal & Objects)	限於多用途儲值卡
申請執照的資格限制	電子錢機構於成立時，除非法律另有規定，否則資本額不得少於一百萬歐元。 (Article 4.1))	申請者必須提供擔保金 (SECTION 203)	申請者之股東已繳付的股本總額及其股份溢價帳結餘的總額不得少於二千五百萬港元
營業範圍之限制	● 不得從事授信業 ● 不得兼營與電子錢發行無關之事業 ● 替其他人在電子設備上儲存資料	未規定	須以經營儲值卡業務為主要業務

[89] 參見 多用途儲值卡的監管，
http://www.info.gov.hk/hkma/chi/bank/value_cards/value_cards_b.htm (last visited on 2005.11.20).

	● 電子錢機構不得持有其它事業的股份，除非該事業係從事與電子錢之發行有關之業務 (Article 1.5))		
維持財務的穩定性	● 自有資本比例須高於最近六個月流通在外之電子錢平均總額的 2% ● 應建立良好建全的管理制度、稽核制度及內控制度 (Article 4.2 & 4.3 & 7) ● 設有投資的限制：限定電子錢機構僅能進行流動性佳無風險的投資 (Article 5) ● 主管機關每年要針對上述事項進行兩次以上的查核 (Article 6)	淨值須維持於美金二萬五千元以上，可允許投資額包括現金、定期存款....等，依一般會計原則所計算之市場價值不得低於流通在外之儲值總金額 (SECTION 206)	維持一定比例的流動資產以及一定的準備金；維持良好的會計及內控制度
贖回的規定	依民眾之要求，按面額贖回儲值金額，亦須於契約中詳述贖回的條件，契約中可載營贖回的最低門檻金額，但不得超過十歐元 (Article 3)	未規定	未規定
洗錢防制	配合相關洗錢防制規定 (Money Laundering Regulations 1993)	配合相關洗錢防制規定 (SECTION 606)	未規定
放寬管制	● 主管機關可以依職權對下列電子錢機構減輕它們符合本指令之要求的程度： 1. 電子錢機構發行流通在外的電子錢之總金額在正常情況下不得超過五百萬歐元且未曾超過六百萬歐元者 2. 電子錢之使用僅限於發行機構及其子	未規定	● 申請者必須具有實質的財力、聲譽良好以及能夠以安全健全的方式營運儲值卡系統 ● 持卡人的風險是有限的 ● 卡片的使用僅限於某特定區域 ● 附加性用途的使用相當有限

	公司和發卡人者 3. 電子錢之使用有一定的範圍，限於一定區域，或是使用人與發卡人間有緊密的財務或商業關係 (Article 8)		

肆、行動通訊與位置隱私(Location Privacy)

美國 1996 年電信法(Telecommunications Act of 1996)中與隱私最相關的，就是 Ttitle VII 的第 222 條關於消費者資訊隱私之規定。每家電信傳輸業者有責任保護該電信傳輸業者及其他電信傳送業者、設備製造商、消費者的獨占機密，包含電信傳輸業者轉賣由其他電信傳輸業者所提供的電信服務。在 911 攻擊之後，美國通過「無線通訊與公眾安全法 (Wireless Communications and Public Safety Act of 1999）」，要求所有在美國境內經營行動電話行動電信之業者，必須在行動電話中安裝 GPS，以便定位追蹤。然而消費者消費時，其行動與所在地點亦為其隱私之一部分，如可隨時被定位，亦有隱私遭受侵害之嫌。就此，2001 年通過的「位置隱私保護法 (Location Privacy Protection Act of 2001）」，要求提供無線位置服務的公司於收集位置資訊時，須通報用戶。該法案並禁止未經用戶許可而逕行收集或銷售資訊。

在歐盟立法例部分，1995 年公布的「關於個人資料處理以及此類資料自由流動的個人保護指令(Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data) 」中，即已令要求各成員國應以立法之途徑來管理個人資料，該指令適用於任何有關涉及個人資料之活動，包括蒐集、儲存及發表之行為，且不論是自動或非自動化的資料蒐集方式。

其個人資料定義之範圍則相當寬廣，舉凡足以辨識或可辨識個人身分者皆在內，且不限於文字、圖像、聲音、視像、影訊等。在 2002 年公布的「電子通訊隱私指令[Directive on Privacy and Electronic Communications (2002/58/EC)]」中，亦確立了以電子通訊中傳輸個人資料的隱私保障，應採技術中立(Technology-neutral)的原則。該指令第九條明確要求電信業者提公有關位置服務時，須符合 opt-in consent 之要求。而且客戶須能隨時撤回該同意。

有關與位置有關的行動商務，日本的發展更早於美國及歐盟。1998 年郵政及電信部(Ministry of Posts and Telecommunications)公布了行動通訊個人資料保護辦法(Protection of Personal Data in Telecommunications Business)，對於使用位置資訊的客戶同意，建立了一套清楚的標準：行動通訊業者在未經客戶的同意下，不得將其位置資訊揭露予任何第三人。另外，在 2003 年 5 月通過的個人資料保護法(Personal Data Protection Law)，也確立了 1998 年郵政及電信部的行動通訊個人資料保護辦法對於 opt-in consent 的要求。

在上述三個地區之中，日本對於以位置資訊為基礎的服務活動之發展乃是最蓬勃的。其中一項原因即是因為這些明確且清楚的法律規定，確實地保障了非緊急性的客戶的位置隱私資訊，也不妨礙此類商業服務之發展。由於位置資訊本身的敏感的特性，所以應該以有別於處理「客戶財產網路資訊(Customer Proprietary Network Information, CPNI)」，包括：時間、日期、通話時間、撥打電話號碼。CNPI 的程序及立法來保護這類的資訊。特別是讓消費者能清楚地知道：當他想購買以位置資訊為目標的服務時，對於誰可以獲得此類的資訊或何時這些資訊會被揭露等。而法令在此時即扮演一個重要角色：負責提供一個標準，好讓業者、政府和其他相關的人清楚地知道自己的權利和

義務。通訊業者有很強烈的利益理由來促進這類服務的發展，而政府也有非常強烈的理由來規範這樣資訊的保障。所以這類的立法應達成：消費者如何授權誰得獲取位置資訊的規範：清楚、一致而且是技術中立的目標。

圖表 6：各國有關位置隱私(Location Privacy)保障之立法及議題

	美國相關法案	歐盟相關法案	日本相關法案
技術中立	N/A	在 2002 年公布的 Directive on Privacy and Electronic Communications (2002/58/EC)確立了：在電子通訊中，所傳輸的個人資料的隱私保障，應採技術中立(Technology-neutral)的原則。	N/A
「位置資訊」(Location Information))的意義	美國：電信法 1996(1996 Telecommunications Act) → 又稱為客戶財產網路資訊(Customer Proprietary Network Information, CPNI)，包括：時間、日期、通話時間、撥打電話號碼。 本法除了說明為完成一通電話所需的資訊及為處理帳務所需的資訊外，並無指明客戶同意的形式及 CPNI 如何被獲取。	意義同左列。	意義同左列。
使用位置資訊時之客戶同意	美國：1999 無線通訊及公共安全法(1999 Wireless Communication and Public Safety Act, WCPSA or E911	相較於美國的不明確，歐盟則顯然清楚多了。 在本指令的第 9 條規定中，很明確地要求，	有關與位置有關的行動商務，日本的發展更早於美國及歐盟。 1998 年郵政及電信部(Ministry of Posts and Telecommunications)

	Act)→非因緊急目的而須使用客戶的位置資訊時，須於事前獲得客戶明示且書面之同意(opt-in consent)(註一)，方可為之。 FCC 一直到 1998 年才同意上述 opt-in 的看法。 但在第 10 巡迴上訴法院於 U.S. West v. FCC 的案中，法院認為 opt-in 的規定是限制了通訊業者在憲法第一修正案所得享受的言論自由，但是法院並不認為位置資訊不應被獨立於 CNPI 被處理。 因此 FCC 在 2001 決定 opt-in consent 是不需要的；而且在 2002 年決定，對於一般的 CNPI 的處理，opt-in consent 或 opt-out consent 皆得適用。 這樣的見解在 2003 年時國會法案中有好幾次都被提出來，但都沒有落實成正式的法律。 E911 法特別被指明應適用於行動電話，但至於有無包含其他的無線通訊設備則未被清楚地說明。 各州的情況，華盛頓州對於 CNPI 要求要做到 opt-in；但是華盛頓州的地方法院卻遵循了第十巡迴	在電信有關位置服務的提供中，須要符合 opt-in consent 的要求。而且客戶能隨時撤回該同意。 本指令將 pot-in 的內容、形式，及如何撤回，委由各個會員國自行決定。	公布了行動通訊個人資料保護辦法(Protection of Personal Data in Telecommunications Business)，對於使用位置資訊的客戶同意，建立了一套清楚的標準：行動通訊業者在未經客戶的同意下，不得將其位置資訊揭露予任何第三人。 2003 年 5 月，個人資料保護法(Personal Data Protection Law)被通過，其中確立了 1998 年郵政及電信部的行動通訊個人資料保護辦法對於 opt-in consent 的要求。

	上訴法院的意見而採與華盛頓州不同的見解。 註一：Two kinds of customer consents to use CPNI, “opt-in” means express prior consent to use; “opt-out” means express prior consent not to use.		
執行的成效	各州及聯邦對於此議題的看到是不明確的。 2003 年 9 月，Cellular Telecommunications and Internet Association (CTIA), 提出一個業者自律的規範，稱為客戶規範(Customer Code)。本規範並無提及有關客戶同意的要求，但是要求各業者應遵守自己公司的隱私政策。 由於聯邦及各州對於此議題沒有一個清楚明確的標準，因此有關這部分的立法就變成各州及業者自律規則的綜合體。這樣將會導致美國繼續在這個以提供位置為服務的商業活動領域中的延遲。	這個指令應該在 2003 年 10 月 31 日前被落實到各個會員國，但截至 2003 年為止只有四個會員國採用，分別是：丹麥、瑞典、芬蘭及西班牙，其他國加則是繼續在進行中。 這個指令將會帶領歐盟繼續地發展此類的商業活動。	在三個地區之中，日本對於以位置資訊為基礎的服務活動之發展乃是最蓬勃的。其中一項原因即是因為這些明確且清楚的法律規定，確實地保障了非緊急性的客戶的位置隱私資訊，也不妨礙此類商業服務之發展。

伍、新興的 RFID(Radio Frequency Identification)技術發展

一、RFID 涉及之隱私權問題

RFID (Radio Frequency Identification Chip) 無線頻率辨識系統，係將一個極小的 IC 晶片貼在商品上，然後利用微波射頻技術將 IC 內儲存之辨識資料傳遞至系統端作為追蹤、統計、查核、結帳、存貨控制等用途。 在利用 RFID 讀取技術在讀取價格的同時，RFID 的微型性、適形性、及穿透性等特性，加上主動標籤不可預測的電波可發送產品名稱、購物時間及區域等資訊，有些 RFID 電波發送範圍甚至遠達 15 呎，不僅暴露消費者購買的物品資訊，甚至侵犯消費者其他私領域行為，諸如行程、地點等。不僅如此，若未妥善處理物品上的 RFID，舉凡衣服、食品、汽車甚至垃圾等，都將不經意洩漏個人資訊。就發展中的 RFID 技術，對於個人的私密物品與採購等一般消費情形的隱私權，已足以讓大眾產生疑慮。隨 RFID 技術普及到各層面，未來更可能使用在證照或身分證件[90]等方面，資料曝光的危險性相形更高，隨之而來如駭客或是政府執行的通信監察措施，也都將影響到人民的權益[91]。

在金融消費方面，由於使用 RFID 的廠商可能針對產品行銷提出對特定消費族群的折扣優惠方案，而透過 RFID 的身份辨識，該特定消費族群的「未經公開的資訊(Non-Public Information, NPI)」(例如消費記錄等隱私)，即可能因此而未經金融消費者同意下暴露。另外在洗錢防制方面，透過 RFID 的技術，對於洗錢防制亦可能有新的突破，歐洲中央銀行(European Central Bank, ECB)2003 年曾計畫與 Hitaichi

[90] 日本 2005 年 12 月 22 日宣佈，2006 年 3 月 20 日以後申請的日本護照都將加入 RFID 的辨識。參見 RFID in Japan: RFID Passports in Japan, http://ubiks.net/local/blog/jmt/archives3/004649.html；美國護照更新亦自 2006 年春季起，全面更換成有 RFID 辨識的 e-passport，但是個人資訊並未透過數位簽章技術加密，因爲擔心其他國家在辨識時無法解密。參見 Wired News:American Passpost to get Chipped, http://www.wired.com/news/privacy/0,1848,65412,00.html，最後瀏覽日期:2005/12/26。

[91] 謝穎青、葉志良，RFID 的隱私權保護問題，(2005.05.12) http://taiwan.cnet.com/enterprise/column/0,2000062893,20098981,00.htm 最後瀏覽日期:2005/11/16。

合作開發將 0.4mm X 0.4mm 大小的 RFID chip 加入在銀行的票券上(banknote），用以取代數位浮水印技術(digital watermark)、加速銀行在計算清點的時間及流程、進而追蹤並防制洗錢行為[92]。

目前產品上 RFID 所記載的資訊均可為使用人蒐集，毋需當事人同意，如超市結帳台得藉由 RFID 蒐集到消費者購買產品時之購物品牌、種類、金額、購買地點及日期等資料；惟如門禁資料、追蹤管理等用途，此等紀錄的保存及使用政策，應公告使用人周知，較為妥當。

RFID 記載之資料，如姓名、電話、地址、身分證字號及出生年月日等個人資料，這些資料非經當事人同意，不得記載於 RFID 上。然而以下資訊是否屬於個人資料，則須個案考量：

1.就診紀錄、病史及使用藥物資訊：依多數國外立法例，這些屬於個人資料範疇，非經當事人同意，不得記載於 RFID 上。

2.地點追蹤：如產品位置等，通常並不屬於足以識別該個人之資料，但產品離開消費場所或進入私人場域時，RFID 是否可以持續追蹤並定位，大部分贊成採取否定見解。

3.使用紀錄：如產品或場所使用紀錄等，像大廈管委會設置之門禁管制進出紀錄，或學校圖書館進出或借閱書籍紀錄，是否屬於足資識別該個人之資料，司法實務傾向否定。

4.關於消費者購買產品時，購物品牌、種類、金額、購買地點及日期是否屬於特定人之個人資料？按該資訊通常無法足資識別該個人之資料，但經蒐集整理分析後，或可歸納出個人購物特性及習慣，

[92] CNET News: Radio ID Chips May Track Banknotes，May 22, 2003, http://news.com.com/2100-1017-1009155.html，最後瀏覽日期:2005/12/26。

此類在司法實務上尚有爭議，不過業者為避免爭議，也都開始研發出一些讓消費者走出賣場後 RFID 即失去效用的設計[93]。

RFID 記載資料的所有權，在 RFID 使用區域內應屬 RFID 使用人所有，但於產品移轉所有權時，RFID 記載資料則應屬消費者所有，並有自行刪除 RFID 記載資料的權利；例如 Wal-Mart 就準備廣發手冊告訴消費者，只要結完帳，就可以撕下標籤。除前述情形以外，需視 RFID 之用途及特別約定[94]。

不當的利用 RFID 將會造成隱私權及公民自由權(civil liberties)的侵害，例如：(1) RFID 的標籤將會附著在任何物體上，而消費者渾然不知；(2) 全世界所有的物品都有屬於它自己獨一無二的 ID，透過這個 ID 會連結到購買它的消費者的個人資訊；(3) 大量資料的蒐集；(4) RFID 的閱讀機到處都有，消費者亦無從得知；(5) 消費者的一舉一動將被這些 RFID 的設備「全都錄」等[95]。是故，部分美國隱私權保護相關團體及消費者團體已發起抵制行動，部分團體如 CASPIAN (Consumers Against Supermarket Privacy Invasion and Numbering)等，

---

[93] 爲消除各界對於 RFID 可能侵害隱私權之疑慮，Wal-Mart 已宣稱未來應用 RFID 時，在消費者步出消費場所後即「失去效用」，此外在科技方面的解決方式，業者已大致發展出「選擇取消」(Opt-out)模式、「銷毀」(kill)模式、「休眠」(sleep)模式或「干擾」模式。美國電子隱私資訊中心(Electronic Privacy Information Center, EPIC)於 2004 年 6 月提出一份關於消費者與私人企業使用 RFID 的綱領，建議使用 RFID 技術的私人企業應告知 RFID 的存在，包括在倉庫、展示架或結帳處透過標籤或商標展示等，並合理揭露使消費者了解 RFID 系統及資訊處理的本質。再者，在產品銷售完成前即應關閉 RFID，除非因個人需要，否則使之永久失去效用（a kill-switch）；假如消費者不知有此選擇，即應主動關閉。一旦標籤關閉後，非經消費者同意不得主動重新開啓，否則，消費者可對違反前述 RFID 使用責任與義務的私人企業提出訴訟。此外，RFID 應使用最簡單的可移除方式裝置。參見 Stephen August Weis, Security and Privacy in Radio-Frequency Identification Devices, March 2003, http://theory.lcs.mit.edu/~cis/theses/weis-masters.pdf 最後瀏覽日期:2005/11/16

[94] 謝穎青、葉志良，RFID 的隱私權保護問題，(2005.05.12) http://taiwan.cnet.com/enterprise/column/0,2000062893,20098981,00.htm 最後瀏覽日期:2005/11/16

[95] Privacy Rights Cleaninghouse, http://www.privacyrights.org/ar/RFIDposition.htm, 最後瀏覽日期:2005/11/16

甚至於 2003 年推動「2003 年 RFID 受告知權法案(RFID Right to Know Act of 2003)」，主張多項聯邦法令的修正案，以規範 RFID 之應用[96]。

二、私人企業應用 RFID 之應注意事項私人企業利用 RFID 技術蒐集資訊時，應特別注意以下事項[97]：

1. 企業在藉由 RFID 儲存、記錄或其他蒐集方式取得個人資料前，應告知個人蒐集資訊的目的，並取得個人之同意。
2. 企業不得將 RFID 標籤辨別資訊結合或連結個人資訊，亦不得將個人資訊藉由 RFID 標籤辨別資訊揭露給第三人知悉，或直接透過第三人使用 RFID 標籤來辨別資訊加以辨別該個人。
3. 業者不應要求個人提供非必要的個人資訊。
4. 採取合理措施以確保透過 RFID 蒐集的個人資訊均安全傳送與儲存，並限操作與維護 RFID 系統的人員取得。
5. 確保蒐集的資訊精確、完整並定期更新。
6. 僅將需使用的個人資訊保存。
7. 公告其 RFID 隱私權政策。

三、美國州立法例[98]

在美國有許多州也已經開始對消費者保護的議題進行討論。在 2004 年 2 月，猶他州的眾議院通過 Radio Frequency Identification -

[96] Reuven R. Levary, David Thompson, Kristen Kot and Julie Brothers, RFID, Electronic Eavesdropping and the Law, Existing laws in the United States could be amended to protect consumer privacy, Feb. 14, 2005，
http://www.rfidjournal.com/article/articleview/1401/1/128/，最後瀏覽日期: 2005/11/16

[97] 謝穎青、葉志良，如何解決 RFID 侵害隱私的疑慮？，(2005.05.13)
http://taiwan.cnet.com/enterprise/column/0,2000062893,20098982,00.htm 最後瀏覽日期:2005/11/16

[98] Reuven R. Levary, David Thompson, Kristen Kot and Julie Brothers, RFID, Electronic Eavesdropping and the Law, Existing laws in the United States could be amended to protect consumer privacy, Feb. 14, 2005，
http://www.rfidjournal.com/article/articleview/1401/1/128/，最後瀏覽日期: 2005/11/16

Right to Know Act (H.B. 251)法案，但卻未被參議院所表決通過。相似的法令在加州雖然被參議院通過(March 1, 2004 - the author was California State Senator Debra Bowen)，但卻不被州議會所同意。另外，加州於 2005 年 2 月 22 日由參議員 Joe Simitian 提出的「身份資訊保護法(Identity Information Protection Act of 2005)」，主要也是在限制這個備受爭議的 RFID 晶片的使用。如果加州完成此一法令的通過，則該法令將成為限制 RFID 晶片的使用的濫觴。此法令目前是懸而未決的，而其將禁止州及地方政府機關核發載有 RFID 的身分證明文件[99]，例如：學生證、駕照、醫療卡及州政府的員工卡。但是，此一法令允許使用 RFID 設備於監獄、醫院、公立醫療院所及收費站。另外，在南達科達州也正考慮訂立一個禁止將 RFID 晶片植入人體的法令；而羅德島州，則正在審視一個禁止用 RFID 技術來追蹤受僱人、學生或顧客的立法提案。

四、美國聯邦立法例

未來「聯邦電子通訊隱私法(The Federal Electronic Communication Privacy Act，ECPA)」，之部分內容可以直接或於進行修改後解決上述所提及的消費者隱私保護的問題。此法令第三章對於下列的行為均視為不合法：竊聽、以其他形式進行的電子竊聽、竊聽裝置及電子竊聽設備的持有、以違法的竊聽方式所獲取的資訊的使用或揭露。雖然竊聽不完全等同於 RFID 技術，但是兩者之間有很高的相似程度，因此 RFID 之使用亦會受到本法令有關電子類別的限制規定之拘束。「竊聽法(The Wiretap Act , 18 U.S.C § 2701)」，本法指出，在未經授權

[99] State Bill to Limit RFID by Kim Zetter, 02:00 AM Apr. 29, 2005 PT，http://www.wired.com/news/privacy/0,1848,67382,00.html,最後瀏覽日期: 2005/11/16

的情況下，故意地使用電子通訊是構成違反刑事法且要負擔拘役或罰金等刑罰。

五、「公平資訊原則」(Principles of Fair Information Practice)

RFID 不只可以追蹤產品及個人的行蹤，也可以蒐集個人的資訊。對此，聯邦貿易委員會(Federal Trade Commission, FTC)的「公平資訊原則(Principles of Fair Information Practice)」，就負責扮演一個非常重要的角色。在這個原則當中，FTC 要求有關個人資訊及地址的蒐集及使用，應符合公平而且要達到以下所列五個隱私保護的原則：

1. 資訊蒐集的通知及知悉；
2. 使用資訊方式的選擇及同意；
3. 個人資訊的接近使用權；
4. 被蒐集的資訊的完整性及安全性；
5. 上述原則的落實。

就因為 RFID 技術可以用來當成是行銷的利器、追蹤的工具和蒐集資料的方法，所以這些原則在此就扮演了積極的角色，在解決這些因為推展 RFID 技術時所可能面臨到的問題。

六、小結

當 RFID 技術極快速地成為零售商所採用的產品管理工具時，也將會對全世界的生產及營運管理模式產生變革。然而，這個技術卻伴隨著侵犯消費者隱私的風險。人們也許會在不知情的狀況下被企業或政府所監控而且個人的自由也會受到侵害。為了保護消費者的隱私權，提倡這項技術的團體也積極呼籲以公平且直接的方式來使用這項

新技術。各州試圖藉由保留消費者保護團體的需求來制定相應的法令來管制使用 RFID 的產業。

伴隨著 RFID 技術大量地被運用在各產業裡，法律議題也不斷地發生。隱私權的定義最後則會影響到科技型的犯罪的定義。當 RFID 技術很有可能產生新型態的竊盜、黑函等犯罪時，也同時會有新型態的犯罪預防工具的出現。雖然法律總是不可避免地跟在科技的後面，但是總是趕得上的。而且將會負責指導 RFID 技術的生產者及使用者。

第五章　電子金融服務與付款機制所引發之議題

壹、問題之提出與因應

一、錯帳

1、我國法制現況

金融電子化造就電子支付系統(ELECTRONIC PAYMENT)的蓬勃發展，相對地產生了傳統金融服務經由臨櫃、現金交易方式不曾存在的許多問題，錯帳(BILLING ERROR)即為其一。我國金融法規中針對發生錯帳情形僅有在「信用卡定型化契約範本」第十一條及第十三條規定中，針對暫停支付機制與帳單疑義設有規範，原則上係就有關商品或服務之品質、數量、金額，或與委託辦理預借現金機構取得金錢之金額的爭議處理，並不得作為拒付款項的法律根據，僅在例外情形賦予質疑當期應付費用明細的持卡人，得對於發卡銀行提出附有相關證明文件的通知，或請發卡銀行向收單機構調閱簽帳單或退款單，請求銀行就該筆交易依各信用卡機構之作業規定，向收單機構或特約商店、辦理預借現金等機構主張扣款，並得就該筆交易主張暫停付款。若未依規定提出上開請求，則推定當期明細為正確。

觀此規定，似對於金融服務終端消費者過於嚴苛，亦無法涵蓋其他電子資金移轉錯帳之權益保護，在法源位階上並非無瑕，對使用電子支付方式之人保護仍嫌不足，使相對弱勢的金融消費族群暴露於錯帳風險之中，間接地亦增加了使用電子支付服務的金融處理成本。

2、美國立法例

一般來說，美國法針對電子資金移轉或信用卡交易發生錯誤時，設有下述規範以資保障[100]：

[100] 此處所指 EFTA 與 TILA 兩部法典在本文探討的四大問題上規範有所出入，其可能造

A. 電子資金移轉法 Electronic Fund Transfer Act (EFTA, EFTA/E)

Electronic Fund Transfer Act (EFTA)，電子資金移轉法中針對「電子資金移轉」定義[101]為包括但不限於經由電子終端機、電話設備、電腦或磁帶，以命令、指示或授權金融機構於帳戶中扣款或入帳，或使用網路、銷售點交易、自動櫃員機、直接提存提資金及電話等方式移轉資金。但排除以支票、匯票或其他類似文書所為的資金移轉。

美國電子資金移轉法主要規範消費性電子資金移轉，至於一般消費者使用電子資金移轉交易之規範則主要設於此法所授權經由聯邦準備理事會(FRB)制訂之各種行政規則中；目的在建立電子資金移轉系統參與者相關權利義務關係與責任的基本規範架構，避免銀行以經濟上相對優勢，訂定不合理契約條款，並依賴詳盡揭露義務與有限責任來保障消費者。

電子資金移轉法第 1693F 條規定錯誤的處理方式(Error Resolution)，根據該條規定所稱錯誤(error)[102]，基本上係指若有不正確之電子資金自消費者帳戶轉入或轉出、或未經授權的電子資金移轉或金融機構有計算上錯誤情事時，得依該規定處理。消費者發現錯誤時，應於收受相關文件(Documentation)六十日內以口頭或書面通知金融機構進行調查；金融機構應於受通知之十個營業日(ten business day)內完成調查並通知消費者有關決定，或暫時性的入帳，並於四十五天內完成調查；若錯誤確實發生，應立即或至遲於決定後一個營業日內更正錯誤；若調查後發現並無錯誤，應於三個營業日內將調查結果遞交或郵寄(deliver or mail)客戶，並應依消費者要求提供可證其決定的文件證明。另外，若金融機構事後被法院發現其未遵守上開十個營業

成支付系統上的影響 *See* Ronald J. Mann, "Regulating Internet Payment Intermediaries", Texas Law Review, at 695 (February, 2004).

[101] EFTA, 15 U.S.C.§ 1693A (6).

[102] EFTA, 15 U.S.C.§ 1693F (F).

日期間的規定，或於調查時未具善意(good faith)，或未附理由否認錯誤，消費者即可於接續的民事訴訟中主張相當於損害三倍(treble)數額的賠償。

除上之外，15 U.S.C.§ 1666 亦設有針對帳單錯誤所為之規定，§ 1666(b)並規定帳單錯誤定義，§ 1666(c)則為貸方收集有關爭議數額的規定，亦值處理時一併注意。

上開規定明顯可以看出對金融機構賦予錯誤調查的「舉證」責任，相對我國信用卡定型化契約範本第十三條要求消費者提供相關證明文件之規範，EFTA 對消費者保護之程度，明顯較我國法制完整。金融機構不但須遵守調查期間的規定要求，事後並可能因未盡義務調查而需負擔損害賠償責任，此種在相對弱勢消費者的保護上給予金融機構較多義務之立法技術，亦值我國參考。

另值一提者，迨為有關§1693H (Liability of financial institutions)(a)項中所揭規定，其中所稱除非金融機構能證明其所導致的未依約定遵照消費者指示完成交易、因金融機構未依約定將足夠資金存入消費者帳戶，致消費者帳戶餘額不足未能完成交易、金融機構未能履行消費者對預先授權的移轉止付指示情形，係因不可抗力、且其已盡合理注意以避免的偶發情形，或係機械故障所致，而消費者於進行交易時已知悉情況，則金融機構應就直接導致(proximately caused)損失對消費者負責。衡諸現況，此規定或可考量引進我國的可行性，作為金融機構發生系統當機時損失處理的規範。

B. 誠實信貸法 Regulation Z-Truth in Lending Act (TILA, TILA/Z)

我國文獻上或有譯為「誠實信貸法」者，其立法目的在於訂定一套合理計算電腦處理借貸之交易費用、有關信用借貸條款之揭露以及

處理借貸帳目錯誤的統一規範。基本上，適用於一般性(regularly)的消費者信用貸款(consumer credit)，亦即舉凡一年使用消費者信用貸款超過 25 次，或其使用之消費者信用貸款一年中超過五次，並有不動產擔保者而言。所稱消費者信用貸款主要針對個人(personal)、家族(family)、家用(household)貸款，並超過四期分次付款(four installments)清償者而言。

該法於 12 C.F.R. §226.13 下規定帳單發生錯誤時之處理機制(billing error resolution)，一開始即對帳單錯誤下定義[103]，並較前揭 EFTA 規定為廣，其中包括有因債權人(creditor)計算或類似會計疏失所造成的錯誤(a computational or similar error of an accounting nature that is made by the creditor.)、帳單中出現消費者未接受或消費者已同意但未傳遞之財產或貸款的錯誤，以及請款日前至少二十日內(at least 20 days before the end of the billing cycle)未對債權人所知悉的消費者最後住址為帳單之寄送等情形。§226.13(b)要求消費者在收受錯誤的帳單後六十天內，對債權人受領帳單錯誤通知的住址(Address for notice of billing errors)發出請款金額錯誤之通知(Billing error notice)；通知中必須表明消費者姓名、消費金額、帳單錯誤認定理由、消費日期以及錯誤金額。債權人必須在三十天之內提出確認，除非債權人恪遵§226.13(e)、(f)之程序，在兩次付款到期日間(within 2 complete billing cycles)至多不超過 90 天內為確認。值此期間，消費者有權請求暫停支付系爭金額與不被催收(Consumer's right to withhold disputed amount; collection action prohibited)尚且有豁免於不良信用記錄

[103] 參見 TILA12 C.F.R. § 226.13(A)以下七款規定。

(Adverse credit reports prohibited)的保障[104]。若債權人在調查過程中確實發現或根本未發現錯誤，皆設有一定法律處理程序[105]。

上開 EFTA 和 TILA 法規中針對錯帳的相關規定，相較於我國的處理流程，更顯精細縝密。錯帳事故的處理影響消費者對於電子金融支付機制的信任與處理成本，若損失的風險越高，作業成本相對提高，勢將嚴重影響支付工具的流通。

二、詐欺

1、我國法制現況

金融安定涉及金流交易機制之健全與否，基此，如何建構有關詐欺的防範機制當然更顯重要。金融的交易安全維護成功與否牽涉到金融安全網濫用(safety net abuse)[106]。盜刷事件，依我國刑法相關規定似得以偽造變造支付工具罪(刑法第 201-1 條第一項)或行使偽造變造支付工具罪(同條第二項)論處。實務上認為行使偽造有價證券以使人交付財物，如果所交付者即係該證券本身價值，則其詐欺取財仍屬行使偽券的行為，不另成立詐欺罪名[107]，而行使偽造變造支付工具罪與詐欺罪可以同一法理處理。

新興電子錢包支付機制與信用卡皆強調「支付」功能，惟電子錢包目前僅針對小額支付開放，仍須先以實體貨幣交換與其支付實體貨幣等值的虛擬貨幣，以作為日後小額消費的支付工具。電子錢包的交易流程設計其實和現金儲值卡較為類似，都是經由「預付」一定金錢換取等值的虛擬貨幣，準此，電子現金的盜用應依刑法第 339-3 條以下規定論處。另外值得一提者，迨為金融控股公司法第 57-1 條所設

104 TILA12 C.F.R. § 226.13(D).
105 請參照 TILA12 C.F.R. § 226.13(E),(F).
106 *See* Charles W. Calomiris & Joseph R. Mason, "Credit Card Securitization and Regulatory arbitrage", Working Papers 03-7, Federal Reserve Bank of Philadelphia, (April 2003).
107 22 上 1814，62 年刑事庭會議第一次決議。

有關利用金融控股公司詐欺取財或得利的刑罰規定，交互參照同法第57-4規定，亦有洗錢防制法之適用；此外，銀行法第一百二十五條之三則為向銀行為詐欺行為時所設之特別規定。至於信用卡遭偽造、盜刷情形，在民事上則多以消費者保護法觀點審視消費者與發卡銀行間定型化契約以定其責任[108]，個案中亦見探討特約商家是否盡到 居發卡銀行履行輔助人地位所應負之善良管理人注意義務[109]。基此，信用卡定型化契約範本第17條亦設有約定的歸責依據。

綜前所述，現行法制上對於金融消費者在電子支付系統詐欺問題上，並未設有得以主張之法源，僅以定型化契約範本作為規範，位階嫌低，保障亦嫌失衡。值此消費者享受金融服務日趨便利之際，卻不見法制上相對的保障，似亦有商榷之餘地。

2． 美國立法例

A. 電子資金移轉法 Electronic Fund Transfer Act (EFTA, EFTA/E)

詐欺的犯罪手法在電子資金移轉法，涵攝在資金移轉非經授權(unauthorized electronic fund transfer)的規定，美國法 15 U.S.C. § 1693G (Consumer liability)設有提供消費者一定程度的保障。

未經授權的資金移轉(unauthorized electronic fund transfer)定義為「未經消費者實際授權，而自消費者帳戶所進行之電子資金移轉，且消費者並未因此獲得任何利益[110]」，例外排除消費者外之人經消費者

---

[108] 92 簡上 575 決、90 小上 56 決。

[109] 依據所謂「最適風險承擔者」之理論言，於信用交易各方之關係中，應將風險分配於支付最少成本即可防止風險發生之人，始能達成契約最高經濟效率之目的。基此，實務上多認應課予特約商店於刷卡後交貨時，重新辨識卡片真偽之義務於作業成本上較爲經濟。

[110] 15 U.S.C. § 1693a(11)：the term “unauthorized electronic fund transfer” means an electronic fund transfer from a consumer’s account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit, but the term does not include any electronic fund transfer
(A) initiated by a person other than the consumer who was furnished with the card, code, or

授權使用卡片、密碼或其他方式進入消費者帳戶、消費者故意詐欺或第三人與消費者共謀詐欺與金融機構因錯誤造成的資金移轉等情形。電子資金移轉法不僅保障透過電腦終端機的交易，還包括在 ATM 交易與零售交易時使用簽帳卡(debit card)自存款帳戶領取現金行為[111]。

若消費者遺失卡片，銀行有義務回復被竊賊以失卡所為的資金移轉[112]，除非存在重要例外：若消費者發現該筆未經授權交易後二個營業日內通知銀行，消費者至多負擔 50 元美金的損失，若消費者於 2~60 個營業日內通知，消費者責任最高限額將提高至 500 美元，若消費者在 60 天內怠於通知金融機構，則消費者可能必須負擔該未經授權之資金移轉的所有損失[113]。將消費者的責任按照通知銀行時程而限制在一定成數下，不僅保護消費者，更能發揮被詐欺後將損失減到最低的功能。

關於非經授權之資金移轉舉證責任的規定，任何涉及未經授權的電子資金移轉之消費者責任訴訟，應由金融機構負舉證責任，證明該筆移轉已獲授權，同時若係未經授權移轉之交易，金融機構亦需舉證本法所規定消費者責任要件已符合[114]。立法技術上旨於促使消費者善

---

other means of access to such consumer's account by such consumer, unless the consumer has notified the financial institution involved that transfers by such other person are no longer authorized,
(B) initiated with fraudulent intent by the consumer or any person acting in concert with the consumer, or
(C) which constitutes an error committed by a financial institution.

111 *See* Ronald J. Mann, *Regulating Internet Payment Intermediaries*, Texas Law Review, February, (2004).

112 *ID.*

113 15 U.S.C. § 1693G(A).

114 15 U.S.C. § 1693g(b)Burden of proof: "In any action which involves a consumer's liability for an unauthorized electronic fund transfer, the burden of proof is upon the financial institution to show that the electronic fund transfer was authorized or, if the electronic fund transfer was unauthorized, then the burden of proof is upon the financial institution to establish that the conditions of liability set forth in subsection (a) of this section have been met, and, if the transfer was initiated after the effective date of section 1693c of this title, that the disclosures required to be made to the consumer under section 1693c (a)(1) and (2) of this

盡卡片、密碼或其他存取設備的保管義務，同時責成金融機構負擔舉證責任，保障了相對弱勢的終端消費者。最令人激賞的，除了本條所賦予的責任外，消費者對於未經授權的資金移轉沒有其他責任[115]，將消費者保護發揮到淋漓盡致。

詐欺案件中，有關消費者保護更顯其重要。美國在未經授權的資金移轉案件中，係將消費者保護的部分責任移轉到金融機構方，使金融機構在事前有加以預防的誘因，事後亦有減少損失的利基，凡此種種的金融立法技術，皆頗有值得我國參考之處。

B. 誠實信貸法 Regulation Z-Truth in Lending Act(TILA)

相較於前揭 EFTA 法規中對未經授權資金移轉的諸多規定，TILA 12 C.F.R.§226.12(b) (Liability of cardholder for unauthorized use)所設未經授權使用的保護規範，與 EFTA 略有不同，惟大致意旨近似。該條款[116]與 EFTA 相關規定中不同者計有：

(一) TILA 針對未經授權使用所設規定提供了更見周全的保護，如消費者若沒有通知銀行其所持卡片遭竊，消費者的責任上限仍然為美金 50 元[117]。

(二) 如特約商店未依約定，即使是有授權的資金移轉，消費者仍然可以停止支付[118]。此外，該條款在 12 C.F.R. 226.12(b)(4)亦設有明文，若州法規定或雙方約定在持卡人與發卡人之間約定較低度的責任，則應依所約定較低度責任資以處理未經授權之使用。

---

title were in fact made in accordance with such section."

[115] 15 U.S.C. § 1693G(E).

[116] 該條款針對未經授權使用定義原文：UNAUTHORIZED USE MEANS THE USE OF A CREDIT CARD BY A PERSON, OTHER THAN THE CARDHOLDER, WHO DOES NOT HAVE ACTUAL, IMPLIED, OR APPARENT AUTHORITY FOR SUCH USE, AND FROM WHICH THE CARDHOLDER RECEIVES NO BENEFIT.

[117] 12 C.F.R. 226.12(B)(1).

[118] 12 C.F.R. 226.12(C).

C. 授信規範 15 U.S.C. § 1643 a

揆諸該條款規定意旨，主要係針對「授信」業務(credit)所涉之明文規範，並規定信用卡持卡人之責任(Liability of holder of credit card)。簡言之，持卡人須符合下述條件下才應歸責：例如該卡片係一有效卡(the card is an accepted credit card)、責任上限為 50 美金(the liability is not in excess of $50)、發卡人已提供持卡所需負責的相關資訊予持卡人(the card issuer gives adequate notice to the cardholder of the potential liability)、發卡人已提供卡片遭竊或遺失後對未授權使用的處理方式、未授權使用發生在持卡人通知發卡人卡片遭竊或遺失前(the unauthorized use occurs before the card issuer has been notified that an unauthorized use of the credit card has occurred or may occur as the result of loss, theft, or otherwise)以及發卡人已知會持卡人在一定情況下的卡片使用會被當成已經授權使用(the card issuer has provided a method whereby the user of such card can be identified as the person authorized to use it)。

本條亦規定了包括發行信用卡在內之授信行為中當事人間的舉證責任分配(burden of proof)，任何爭議凡涉及未授權使用卡片，應由發卡人負擔證明使用其已獲授權之舉證責任，若係未經授權之交易，發卡人亦需舉證持卡人已符合需負責的法律要件。準此，持卡人基於該條規定所應負的責任外，對未經授權之使用則一概不需負責[119]。

三、洗錢

1、我國法制現況

[119] 15 U.S.C. § 1643(D).

我國洗錢防制法在最近一次修法後，係以「洗錢防制法第七條授權事項[120]」、「洗錢防制法第八條授權事項[121]」設為主要建構[122]。在金融資訊庫建置上，我國僅設置有「金融帳戶開戶查詢系統」，是否應仿照美國成立金融資訊庫，值得深思。金融控股公司法第五十七條之一連結同條之四的規定，使以不正方法將虛偽資料或不正指令輸入金融控股公司電腦或相關設備、造成財產權變更或取得財產行為亦有洗錢防制法之適用。惟徵諸現行洗錢防制的實務規範機制中，尚無專門針對電子金融交易設有防制的相關規定，似亦有進一步檢討如何補強的必要。

2、美國立法例

A. 銀行秘密法 The Bank Secrecy Act(BSA)，31 U.S.C. § 5311~30、12 U.S.C. § 1818 (s)、1829(b)、1951~59

洗錢防制和銀行顧客的隱私權間，一直存在著拉鋸戰，孰重孰輕左右法規機制的架構。美國銀行秘密法要求金融機構必須配合政府保存金融紀錄及申報可疑交易資料，而非規定銀行如何保密。BSA 中金融機構定義非常廣泛，而金融機構的存在往往構成洗錢防制中交易和顧客紀錄同一性確認的障礙，金融機構提供交易與客戶資料對偵察犯罪很有幫助。BSA 要求金融機構針對個人單筆金額達 10,000 美金之交易以上製作交易紀錄(Currency Transaction Reports (CTRs))，且在 BSA 授權下，美國財政部長(the Secretary of the Treasury)可以對不遵守規定的機構處以聯邦處罰。結果是不遵守規定的機構在申請營業許

[120] 財政部 92 年 11 月 18 日台財融(一)字第 0928011641 號令。
[121] 財政部 92 年 8 月 4 日台財融(一)字第 0920035253 號令。
[122] 參照 蔣淑芬，洗錢防制法之交易申報制度，月旦法學，第 119 期，2005 年 4 月。

可或存款保險上可能會被拒絕。惟目前 BSA 在非物理交易的電子交易紀錄上也有漏洞[123]。

另值注意，美國 1990 年財政部長在 BSA 下設立了金融犯罪稽查局(Financial Crime Enforcement Network, FinCEN)，設立目的在提供聯邦及地方執法機關有關洗錢之情報及分析資料，並推動國際合作。該單位在自己建立或透過協定得以使用各種不同資料庫，如：商業資料庫、金融資料庫等。FinCEN 在 2002 年推動 PATRIOT Act Communication System(PACS)，為一更安全、便利的金融機構網路申報系統，PACS 可望達成資料歸檔更快速與更省錢的目標。2003 到 2005 年，FinCEN 強調透過入門系統(Gateway system)可使資料收集、保存與回復更現代化，減少金融機構與執法人員間資訊流通的成本，對追查不法與洗錢行為將更有利。但是新的系統也有其問題，財政部長審查每年資訊申報傳輸的結果，報告顯示若一年收到超過一千二百萬筆資料，有超過三成的資料是重複傳輸而不必要的[124]。2004 年 4 月，美國財政部與國稅局共同推出一個新措施，使非銀行的金融機構與非金融的交易或企業遵守 BSA 下登記、申報與資料保存的要求。

B. 洗錢防制法 Money Laundering Control Act of 1986 (MLCA),18 U.S.C. §1956~57

該法規範意旨乃用於補強前揭 BSA 的規範缺漏，MLCA 在違反前揭交易申報 CTR 義務之處罰外，並對於洗錢行為設有單獨處罰之規定，禁止資金來源緣因特定非法行為之國內、國外超過美金 10,000 元的交易或移轉資金以及財產買賣，當該筆資金來源為特定非法行

[123] *SEE* CHRISTINA JACKSON, "COMBATING THE NEW GENERATION OF MONEY LAUNDERING: REGULATIONS AND AGENCIES IN THE BATTLE OF COMPLIANCE, AVOIDANCE, AND PROSECUTION IN A POST-SEPTEMBER 11 WORLD," JOURNAL OF HIGH TECHNOLOGY LAW, 2004.
[124] *ID.*

為。不論是意圖促使上開行為成功的人，或是隱瞞、掩飾上開不法行為者，還是逃避將此交易報經紀錄的人，都是該法所要處罰的行為態樣。併值一提者，MLCA 同時包含民事與刑事的處罰規定。

C. 愛國者法案 USA PATRIOT, Act of 2001，31 U.S.C. 5311＆the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 , 3 U.S.C. § 302(a)(2)[125]

九一一事件後，為抑止恐怖組織洗錢，第 107 屆的美國國會通過了上開規定，立法目的在於賦予美國政府更多對抗國際性洗錢與恐怖行動。美國財政部長在該法授權下可以要求美國境內金融機構追查洗錢行為，還可以與他國協商共同防制洗錢。該法下美國國內金融機構必須有留存交易紀錄並認識其客戶(know your customer)，以便擁有足夠的資料以及與其他金融機構、主管機關與執法者交換資訊。金融機構被要求建立內控機制，設置法令遵循主管(designate compliance officers)，訓練員工以及獨立的審計來抑制和打擊洗錢。藉由金融機構與執法單位間更頻繁的資訊溝通機制，該法建立了一套促進跨國交易安全的記錄機制，更希望因此將該法打擊洗錢的目標擴展到全世界。該法給予財政部長得享抵制不合作的金融機構與對抗司法單位不配合的壓力，更賦予其禁止不提供資料的國外銀行與美國銀行從事交易之裁量權。為防範帳面上懷疑為在境外進行的洗錢行為，該法允許對外國銀行在美國本土的財產扣押，而毋須探究是否與犯罪所得或被調查的個人具有直接關聯性。此外，該法更禁止美國金融機構擁有專

[125] *ID.* 另值附帶一提者迨爲有關該法四年落日條款（SEC. 303.－ 4-YEAR CONGRESSIONAL REVIEW; EXPEDITED CONSIDERATION.）之規定，揆諸該規定尚僅適用於對抗資助恐怖份子之法案部份，併此說明。

供接收外國空殼銀行[126](foreign shell banks)存款，以代替外國金融機構處理支付和金融交易的帳戶[127](correspondent accounts)。

目前實務上交易人間亦設有許多新興方式規避追查，如透過網路交易和電子現金，國際間打擊洗錢不遺餘力的「金融犯罪與洗錢防制組織」- Financial Action Task Force(FATF)[128]提出警告金融機構在使用高科技便利的同時，也提醒金融界要更小心檢視高科技亦可能幫助洗錢行為的後果。洗錢也有可能藉由慈善事業(charities)或非營利機構進行，FATF 強調該類機構所為的籌款行為，可能是全球性洗錢防制的弱點[129]。

四、金融資訊隱私權(兼論消費者保護)

1、我國法制現況

我國有關該部分的法制建構，除於消費者保護法第§4、11~17、22-1 等條文中針對企業提供服務的消費者保護原則、定型化契約訂定與解釋原則與廣告揭露規定外；「個人電腦銀行業務及網路銀行業務服務契約範本」更建主管機關為電子金融的網路服務所為的低度規範[130]；電腦處理個人資料保護法[131]§6、23④牽涉非金融機關對個人資料的利用；金融控股公司法§42、43、48、60[132]與銀行法§28IV、48II 成

[126] 31 U.S.C. §5318(J)(1-4): SHELL BANKS ARE DEFINED AS A FOREIGN BANK WITHOUT A "PHYSICAL PRESENCE" IN ANY COUNTRY.

[127] 31 U.S.C. § 5318A(F)(1)(B): CORRESPONDENT ACCOUNTS ARE DEFINED AS ACCOUNTS :"ESTABLISHED TO RECEIVE DEPOSITS FROM, MAKE PAYMENTS ON BEHALF OF A FOREIGN FINANCIAL INSTITUTION, OR HANDLE OTHER FINANCIAL TRANSACTIONS RELATED TO SUCH INSTITUTION."

[128] FATF 對洗錢防制的 40+9 點建議(40+9 RECOMMENDATIONS)，請參閱網址：HTTP://WWW.FATF-GAFI.ORG/DOCUMENT/28/0,2340,EN_32250379_32236930_33658140_1_1_1_1,00.HTML，最後瀏覽日：2005/12/29。

[129] 參見前註 122。

[130] 有關該範本與消保法間之詳細探討，請見下述五、3.。

[131] 法務部已於九十年研擬修正草案，擬擴大規範範圍並更名爲「個人資料保護法」，並引進團體訴訟制度。

[132] 金控法隱私權規範的介紹與遺漏，請參照施峰達，「我國『金融檢查』與『財務隱私

為不同金融主體關於客戶金融資料保密與使用的準則[133]。電子簽章法於 2001 年 11 月 14 日公布，2002 年 4 月 1 日施行，其中鑑於憑證機構將大量蒐集、處理個人資料，亦在第十一條第二項將「保護當事人個人資料之方法與程序」明定為憑證實務作業基準應載明事項之一。電子簽章法制訂有助於電子世界的法律化，但在技術上不斷革新的今天，法律無法時時更新，僅能藉助主管機關經濟部中資訊專業人才處處監督。

上開規定或契約範本看似多元，其實彼此之間的相互勾稽就會造成資訊隱私權防護的漏洞。且保密義務規定不夠詳細，僅作原則性保密規範，似乎無法完全保障消費者資訊隱私權[134]。

2、美國立法例

A. 金融服務業現代化法案 Financial Services Modernization Act of 1999

美國金融服務現代化法案，15 U.S.C. § 6801~6809 為金融資訊與消費者保護重心，限制金融機構揭露客戶非公開的資訊(discourse on nonpublic personal information)予非分支機構之第三人(nonaffiliated third parties)，且要求金融機構對其所有客戶揭露該機構與分支機構與非分支機構之第三人資訊分享的隱私權政策與方法[135]。

權』法制關連性之探討-以銀行業之監理爲中心」，中原大學財經法律學系碩士論文，91 年 1 月，頁 81~84。

[133] 不同金融機構主體違反保密義務的處罰應歸統一，金融機構對於顧客造成較大損害僅可做爲顧客求償的依據，而非差別處斷的依據。見前註 29 文章，頁 83。

[134] 例如，個資法第 23 條但書第四款規定下，金融機構多半在定型化契約中即取得客戶同意，得以將客戶資料爲銀行業務外的使用。其他介紹，請參見 羅培方，「試析銷售點轉帳業務(POS)及可能產生的法律問題」，我國電子支付暨信用工具法制導論，2003 年 5 月，頁 1338-139。

[135] 有關 GLBA 的詳細介紹，同前註 29，頁 68~77。

B. 金融消費者資訊隱私權法 Regulation P- Privacy of consumer financial information, 12 C.F.R. 216

消費者金融資訊隱私權法[136]，在 GLBA 授權下由美國之金融機構監理部會組成聯合工作小組制訂，將 GLBA 之規範落實為具體措施。立法目的乃要求金融機構提供消費者有關隱私權政策與執行資訊，描述金融機構在什麼情況下可以揭露客戶非公開的個人資料給非分支機構的第三人，以及提供消費者避免金融機構揭露其相關資訊的選擇權(opting out)措施。

金融機構[137]必須提供清楚、明確反應其隱私權政策與執行的初次告知給將成為金融機構顧客的個人以及消費者，金融機構原則上告知其顧客的時點不能晚於建立顧客關係時[138]，對消費者則必須在揭露任何消費者個人非公開資訊予非分支機構的第三人前告知之。但若金融機構沒有揭露任何消費者非公開的個人資訊或未與消費者建立顧客關係，就沒有告知的義務[139]。金融機構亦必須在與其顧客持續的關係中，每年向顧客提供清楚、明確反應其隱私權政策與執行的告知。若金融機構與顧客結束關係後，即毋須向其提供年度告知[140]。

本規則下，金融機構必須提供清楚且足夠的事先通知且能夠完全反映其隱私權政策與執行給消費者(consumer)與顧客(customer)。金融

---

136 REGULATION P 將 GLBA 落實爲下述具體措施：一、金融機構需以明確、清楚且顯著的方式告知消費者關於金融機構在何種情況下，將會對分支機構或非分支機構之第三人揭露消費者非公開之個人資訊；二、金融機構需定期以明確、清楚且顯著的方式告知客戶金融機構的隱私權政策；三、金融機構需提供消費者得選擇個人資訊不被揭露的機制。轉引自林育廷，「淺談我國網路金融法治相關問題之研究」，科技法律透析，2001年 2 月，頁 56。

137 必須遵守本規則的金融機構爲州體系成員的銀行、銀行控股公司、爲前二者之子公司或關係密切者(不包括非聯邦儲備體系者、由證交法管理的證券商、由投資公司法管理的投資公司等等)、外國銀行的州際代辦處與分社(其存款非由聯邦存款保險公司承保)和由外國銀行控制或持有的商務借貸公司等。

138 適時告知的例外規定 C.F.R.(§216.4(E))，如建立顧客關係非來自顧客的選擇，或適時提供告知會造成顧客交易的實質遲延且顧客同意事後再取得告知。

139 12 C.F.R.§216.4(A).(B).

140 12 C.F.R. § 216.5.

機構對原來的客戶(existing customer)提供新的金融商品或服務時，也必須滿足事先足夠通知的要求。但若建立顧客關係非消費者自己的選擇，或者顧客同意延後獲通知，則可以延後通知。必須包含在隱私權通知裡的訊息有：1. 金融機構可能收集到有關個人的非公開資訊種類(The categories of nonpublic personal information that you collect)；2. 金融機構會揭露的個人非公開資訊(The categories of nonpublic personal information that you disclose)；3. 將對之揭露資訊之分支機構或非分支機構之第三人(The categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information)；4. 有關從前顧客非公開的個人資料被揭露的種類以及對之揭露的分支機構或非分支機構之第三人(The categories of nonpublic personal information about your former customers that you disclose and the categories of affiliates and nonaffiliated third parties to whom you disclose nonpublic personal information about your former customers)；5. 若對非分支機構之第三人揭露個人非公開的資料需有一獨立通知(a separate statement)；6. 向消費者解釋在本法規定下得選擇終止金融機構向非分支機構之第三人揭露關於其非公開之個人資料的權利(An explanation of the consumer's right under §216.10(a) to opt out of the disclosure of nonpublic personal information to nonaffiliated third parties, including the method(s) by which the consumer may exercise that right at that time)；7. 任何在公平信用評等法(the Fair Credit Reporting Act,15 U.S.C. 1681a(d)(2)(A)(iii))規定下的洩露、8. 機構本身關於保護個人非公開資料機密及安全的政策與實踐(Your policies and practices with respect to protecting the confidentiality and security of nonpublic

personal information)；9. 任何在§216.6 第二項中所必須揭露的事項[141]。

金融機構針對非顧客的消費者所給予簡短的選擇權初始告知必須清楚(clear)、明確(conspicuous)地陳述其隱私權注意事項如何遵循法令，說明消費者如何透過合理方法行使上開選擇權利[142]。此所稱「合理方法」例如：提供消費者免付費電話或是在金融機構辦公室取得告知書的影印本。而在給予消費者的選擇權告知中，必須表明：1. 金融機構揭露或保留將消費者非公開之個人資訊揭露予非分支機構的第三人之權利；2. 消費者擁有終止揭露的選擇權，以及 3. 消費者合理行使上述選擇權的方法[143]。合理行使選擇權的方法例如：在有關選擇權告知書中明顯標示出選擇權選項、在選擇權告知書裡附上回覆表格(a reply form)、提供行使選擇權的電子方式(例如寄發電子郵件或透過金融機構網站)、提供免付費電話供消費者做選擇[144]。消費者可以在任何時候行使選擇權[145]，而金融機構必須在接到消費者選擇權決定後在合理可執行的時間內立即遵守[146]。消費者所做的選擇決定，其效力將持續到消費者自行另以書面撤回為止，而與同一人重新建立的顧客關係，將不適用於先前顧客關係中所為的選擇[147]。金融機構不可直接或透過任何分支機構提供予消費者初次的隱私權告知內容外，揭露

[141] 12 C.F.R.§216.6(B)原文：**DESCRIPTION OF NONAFFILIATED THIRD PARTIES SUBJECT TO EXCEPTIONS**. IF YOU DISCLOSE NONPUBLIC PERSONAL INFORMATION TO THIRD PARTIES AS AUTHORIZED UNDER §§216.14 AND 216.15, YOU ARE NOT REQUIRED TO LIST THOSE EXCEPTIONS IN THE INITIAL OR ANNUAL PRIVACY NOTICES REQUIRED BY §§216.4 AND 216.5. WHEN DESCRIBING THE CATEGORIES WITH RESPECT TO THOSE PARTIES, YOU ARE REQUIRED TO STATE ONLY THAT YOU MAKE DISCLOSURES TO OTHER NONAFFILIATED THIRD PARTIES AS PERMITTED BY LAW.

[142] 12 C.F.R.§216.6(D)(2).

[143] 12 C.F.R.§216.7(A)(1).

[144] 12 C.F.R.§216.7(A)(2)(II).

[145] 12 C.F.R.§216.7(F).

[146] 12 C.F.R.§216.7(E).

[147] 12 C.F.R.§216.7(G).

其他非公開個人資訊，除非：1. 金融機構已經對消費者提供清楚、明確描述修正的隱私權政策與執行的告知；2. 金融機構提供消費者再一次選擇機會；3. 在揭露消費者資料給非分支機構的第三人之前，曾經提給予消費者合理的機會(a reasonable opportunity)以行使選擇終止的權利，以及 4. 若消費者沒有選擇終止揭露[148]的情形。

金融機構必須滿足§216.4 與§216.7 的「告知」要件，並且在將個人非公開的資訊揭露予非分支機構的第三人之前，提供消費者選擇終止的機會；但消費者沒有選擇終止時，金融機構才可以例外地直接或透過分支機構揭露資訊。金融機構可以提供消費者個人非公開資訊揭露的部分終止權(partial opt out)[149]。針對資訊的再度揭露或重複使用限制，若金融機構因§216.14 或§216.15 例外規定而自其他非分支機構的金融機構取得個人非公開的資訊，則允許將此資訊揭露予資訊來源金融機構的分支機構、本身的分支機構或為一定目的而使用。

若金融機構非因前揭 §216.14 或 §216.15 規定而取得資訊，金融機構得將該資訊揭露予資訊來源金融之分支機構、本身的分支機構或合法透露給任何與此資訊來源機構相關的任何個人。而在 §216.14 或 §216.15 例外規定下取得資訊之非分支機構的第三人，該第三人可將此資訊揭露予其分支機構或為一定目的而揭露使用。非因 §216.14 或 §216.15 例外規定取得資訊之第三人，則得將資訊揭露予其分支機構與合法情況下可對之揭露的其他個人[150]。原則上，金融機構不得直接或透過分支機構，對非分支機構的第三人以電話銷售(telemarketing)、郵件銷售或其他電子郵件銷售目的，為消費者帳戶金額、帳戶密碼、存款數額、信用卡密碼或交易數額的揭露。例外的情形，則是在金融

[148] 12 C.F.R.§216.8(A).
[149] 12 C.F.R.§216.10.
[150] 12 C.F.R.§216.11.

機構將帳戶數額或密碼單獨揭露予其代理人或服務提供時，以便為金融機構產品及服務的實現，或為私人的信用卡計畫而揭露予顧客知悉的相關參與者，則允許揭露之[151]。

上開 §216.7 與 §216.10 的選擇權相關要求，在金融機構提供個人非公開的資訊予非分支機構的第三人，旨於使第三人對之提供服務(perform services)或以金融機構名義(functions on your behalf)時，則不適用。但此時金融機構必須滿足 §216.4 所指初次告知的要求，以及與第三人簽訂契約協議，禁止第三人在上述目的外揭露或使用金融機構所揭露之資訊，包括在 §216.14 或 §216.15 例外規定下以日常營業過程實踐這些目的。

簡言之，若依本條規定經由共同行銷方式揭露非公開性之個人資訊予金融機構，且與該金融機構間之約定符合依本條中第(a)(1)(ii)款所規定，除因實施共同行銷或第 216.14 或第 216.15 條中所載之一般正常業務範圍內之共同行銷之例外情形，金融機構不得揭露或使用該非公開性的個人資訊[152]。至於 §216.4(a)(2)對消費者初次告知的規定，§216.7 與 §216.10 所稱選擇權規定，以及 §216.13 所指對服務提供者與共同行銷的要求，若金融機構揭露非公開的個人資訊乃與下列行為有關，則例外不適用－為達成、實現或執行來自消費者的要求或授權之必須(necessary to effect, administer, or enforce a transaction)、服務處理消費者要求及授權、處理消費者帳戶及私人信用卡問題、研議中或已進行的證券化(proposed or actual securitization)及次級市場買賣(secondary market sale)與關係到消費者交易的類似交易等[153]。另

---

[151] 12 C.F.R.§216.12.

[152] 12 C.F.R.§216.13(A).同條(B)段規定服務(SERVICE)目的可以包括共同行銷(JOINT MARKETING)。

[153] 12 C.F.R.§216.14(A).此段中有關“NECESSARY TO EFFECT, ADMINISTER, OR ENFORCE A TRANSACTION”的解釋請參見(B)段。

外，若取得消費者未撤回(revoked)之同意(consent)或指示[154]，或為對抗實質及潛在的詐欺、非授權交易，或提供資訊予保險費率諮詢機構(insurance rate advisory organizations)、保證基金或金融機構之律師、會計師、審計人員，或為了買賣、併購、交易或轉讓全部或部分營業，或遵守聯邦、洲、當地法令及其他應適用的規定之目的，或為了民刑事的調查(investigation)、傳喚(subpoena)、約談(summons)等，金融機構毋須適用 §216.4(a)(2)初次告知要求、§§216.7 與 216.10 選擇權要求，以及 §216.13 對服務提供者和共同行銷之規定[155]。

綜前所述，進一步介紹過 Regulation P 的相關內容後，足知該規則中金融機構必須在詳盡的程序規定下方可揭露消費者個人非公開的資訊，相較我國目前僅在「金融控股公司及其子公司自律規範」中得以窺見有關消費者資訊揭露的規定，顯然我國對於隱私權與消費者的保護尚嫌薄弱。主管機關或可參考 Regulation P 的相關規定，將金融消費者資訊隱私的保護規範更予細緻化，且提高規範的法律位階，促使金融機構依法執行更為健全的財務隱私權保護措施。

C. 財務隱私權法 Right to Financial Privacy Act, 12 U.S.C. chapter 35

財務隱私權之相關規範，原肇始於銀行秘密法的制訂造成金融機構很大負擔，且無法滿足顧客對金融機構資訊保密的要求，故催生出財務隱私權法，以期在政府犯罪調查與財務隱私保障下取得平衡點。本法建立了將消費者金融紀錄對政府機關揭露的程序規定與例外，提供消費者在聯邦政府對金融機構監督下可以享有合理隱私權對待權利。

[154] 12 C.F.R.§216.15(B)(2)：消費者可以撤回對揭露資訊的同意。
[155] 12 C.F.R.§216.15.

政府若欲取得顧客的財務資料，必須符合五種方式規定：經由顧客授權(customer has authorized such disclosure)、取得行政傳票或傳喚(an administrative subpena or summons)、取得搜索票(search warrant)、取得司法傳票(judicial subpena)、經由正式的書面請求(formal written request)[156]。惟金融機構或其主管、雇員、代理人通知政府當局，其持有可能有關違反法律或規則的資訊時，例外地排除上開方式規定的適用，上開揭露者毋須負任何法律責任。此外，金融機構為附隨於完整擔保利益，證明破產請求權，債務催收或處理關於政府貸款、貸款保證等之申請而提供紀錄[157]亦不在禁止之列，併此說明。

D. 公平信用評等法案 Fair Credit Reporting Act(FCRA), 15 U.S.C. § 1681 et seq

公平信用評等法，係由美國聯邦貿易委員會(the Federal Trade Commission)專責執行，立法目的在要求消費者信用報告代理機構採用合理的程序，以符合消費者信用、個人與保險或其他金融資訊的機密性、正確性、中肯與適當使用，並確保公平、公正且尊重消費者隱私權。本法並建立修正消費者信用報告錯誤的程序，確保只在合法的商業目的下提供有關消費者報告。信用報告必須為判決、留置權、訴訟等保留七年，但為了破產事件應保留十年。本法並修正了 TILA 誠實信貸法的規定，要求針對所有有關信用卡、賒帳卡的申請或要約，必須有新的揭露，包括每年利率(annual percentage rates)、定期會員費用(periodic membership fees)、最低限度的金融規費(minimum finance

[156] 12 U.S.C.§3402.

[157] 12 U.S.C.§3403(C)(D).

charges)以及餘額結算方法(the type of balance calculation method)。應予特別說明者，此法優先於州法適用[158]。

目前公平信用評等法的最新動態，係依據 2003 年「公平正確信用交易法」the Fair and Accurate Credit Transactions Act of 2003 (FACTA) (PL 108-159, 12/04/03)所為之部份修正，FACTA 要求聯邦貿易委員會和相關機構在 2004 年以 FCRA 授權所制訂的規定來執行 FCRA 中的修正條款[159]。

除了上開法案提供消費者保護外，本文前已述及的電子資金移轉法(EFTA)與誠實信貸法(TILA)都有消費者保護的相關部份規定。如 EFTA 中§1693c 中規定對於消費者對於非經授權交易責任的事先揭露、§1693g(b)所設有關舉證責任分配規定中要求金融機構應負擔「主要的」舉證責任等，將消費者保護理念深入實踐於每一個金融交易。另外，誠實信貸法(TILA)認金融機構有提供資訊的義務，也是消費者保護的表現，值得參考。

貳、其他

一、網路銀行業務規範

目前我國銀行享有金流處理機制中的特許地位，[160]，且同條二項針對經營銀行間資金移轉帳務清算之「金融資訊服務事業」[161]亦需經主管機關許可，顯見金融業仍屬高度管制產業。實務上迭生疑義者迨

---

[158] *SEE* JONATHAN R. MACEY, GEOFEREY P. MILLER& RICHARD SCOTT CARNELL, BANKING LAW AND REGULATION, 3D, AT 172~173 (2001).

[159] 有關 FCRA 的全文與簡介，請參見聯邦貿易委員會(FTC)網站，網址：HTTP://WWW.FTC.GOV/PRIVACY/PRIVACYINITIATIVES/CREDIT.HTML，最後瀏覽日：2005/11/20。

[160]觀之銀行法第二十九條即規定非銀行不得經營收受存款、受託經理信託資金、公眾財產或辦理國內外匯兌業務。倘違反非銀行收受存款的限制，依同法第一百二十五條規定對其違反專業經營行為處以刑罰併科罰金。足以得窺所謂高度管制之立論。

[161] 請參照財政部 90/09/28 台財融(二)字第 0090719310 號令訂定之「銀行間資金移轉帳務清算之金融資訊服務事業許可及管理辦法」。

為，網路銀行究竟要不要劃歸為受高度管制的獨佔事業而受管制？從我國網路銀行的發展觀之，各家金融機構架設網路銀行的目的不外乎在微利時代如何加強競爭、提高利潤等考量，皆以原有實體銀行組織架構之思考擴展經營、服務業務通路，與國外單純以完全虛擬、無實體型態出現的網路銀行基本考量多所差異，故我國網路銀行業務的開展似可視為乃以傳統銀行經營業務的另一型態，似應納入原先實體金融業高度管制的規範體系。

惟如何在高度管制和不阻礙電子金融活力發展間衡平？向為電子金融監理上的難題。首應克服者，當係如何界定經由網路銀行通路所呈現金融業務的法律定位，主管機關政策上一方面鼓勵金融 E 化，對金融業者進行網路銀行一律採取由業者向主管機關提出有關網路金融業務的申請，主管機關再按照「金融機構辦理電子銀行業務安全控管作業基準[162]」與「個人電腦銀行業務及網路銀行業務服務契約範本[163]」作形式上核備，準此，論者多認為雖有事前核准之外觀，執行上卻流於僅具申請的形式。

進一步細究我國有關網路金融相關規範，亦即目前的監理審查依據欠缺法律授權的基礎。易言之，現行有關銀行辦理網路金融的監理規範，未見金融業者在銀行法或相關法規的法位階有一可資遵循的適用法源。倘交互參照銀行法第一百三十二條所揭有關違反本法或本法授權所定強制或禁止規定之行政罰鍰規定，亦明顯得窺上述二監理標準非基於「本法或本法授權所定」之窘境[164]。若謂將銀行法第三條第二十二款「經中央主管機關核准辦理之其他有關業務」之概括條款解釋為金融業者經營網路銀行的依據，似乎又有違銀行業務應列舉規

[162] 1998.5.5 制訂(台財融字第 87721016 號函)，2005.2.22 修訂公布(行政院金融監督管理委員會金管銀(二)第 0948010020 號函備查)。
[163] 請參閱 2004.11.30 最新修正版本。
[164] 請參閱謝易宏，「網路銀行法律問題之研究」，月旦法學雜誌第 71 期，頁 128。

定、事先核准的性質，恐導致概括條款的運用無限擴大，影響金融管制的基石。

承上所述，上位階規範金融業者經營網路銀行業務的依據似應先予確立，建議在制度面上納進銀行法實體規範，下位階授權之法規命令，如：審查安全控管基準，才得以在穩固的實體法授權下逐步開展。惟違反的法律效果攸關人民的權利義務，依中央法規標準法的規定應在法律中設有規定[165]。

二、銀行轉投資之限制

在金融業務全面邁入數位化經營環境，原有實體銀行的規範體制顯有調整之急迫，商業銀行轉投資限制在銀行法第三條與第二十二條等規定所建構的監理，與原財政部金融局台財融字第八五五〇五〇四二號函(轉投資目的性之例外核准)下，現已經銀行法第七十四條規定對商業銀行轉投資限制大幅度放寬，並將上開函令內容納入實體法規範[166]，「商業銀行轉投資應具備條件及檢附文件之規定」[167]則具體呈現商業銀行轉投資金融相關事業或非金融相關事業之應備條件與自我評估表。

另外，跟隨銀行業進行電子化的腳步，限制銀行業轉投資非金融相關事業中有關 E 化的「資訊服務業」投資，似乎不符實際發展需要，故主管機關在 2000 年 9 月 18 日發佈「銀行申請轉投資資訊服務業屬金融相關事業之認定標準」，其中第一項：「銀行申請轉投資之資訊服務業，其主要業務為從事與金融機構資訊處理作業密切相關之電子資料處理、涉及銀行帳務之電子商務交易資訊之處理，或研發設計支

[165] 同上註。
[166] 請參見現行銀行法第 74 條第二、三項規定。
[167] 2001 年 5 月 8 號發佈之台財融(一)字第 90738588 號函

援銀行業務發展之金融資訊系統者，視為本部 85 年 3 月 22 日台財融字第 85505042 號函規定所稱之金融相關事業。」將銀行如申請轉投資資訊服務業，若主要業務為從事與金融機構資訊處理作業密切相關的電子資料處理、涉及銀行帳務電子商務交易資訊處理及研發設計支援銀行業務發展之金融資訊系統者，可視為金融相關事業投資之。此一函令雖因民國 85 年 3 月 22 日台財融字第 85505042 號函已停止適用而可能造成無所附麗的結果[168]，但在轉投資限制逐步開放上仍具有一定的意義。

綜上所述，目前銀行的轉投資已較原有規範大幅開放，金融電子化的潮流可謂居功不小，政策決定方向亦值肯定。

三、消費者保護議題[169]－以「個人電腦銀行業務及網路銀行業務服務契約範本」為主

舉凡產品或服務提供，皆難免涉及消費者保護議題。金融產業健全與否悠關金流業務之活絡，其中所涉有關消費者保護是否妥當更顯重要。從上述「個人電腦銀行業務及網路銀行業務服務契約範本」與主管機關公佈的「信用卡定型化契約範本」觀之，似仍有以下問題有待進一步斟酌。

1. 消費者保護法之相關規定

金融業為一高度管制產業，業務概多設有定型化契約範本(以下簡稱「範本」)以資憑藉，並作為紛爭解決時之參考遵循依據。關於網路銀行服務與信用卡申請所可能涉及的消費者保護規定，首推消費

[168] 主管機關評估銀行轉投資金融或非金融相關事業重心似乎隨著 2001 年 5 月 8 號發佈之台財融(一)字第 90738588 號函「商業銀行轉投資應具備條件及檢附文件之規定」之發佈而轉移注意力，在投資相關金融事業著重資本適足性、風險控管與內控機制，投資非相關事業則另看重配合政府發展國內經濟發展計畫目的。

[169] 以下有關消費者保護議題乃參照許秀雯，「電子銀行之法政策及相關法律問題研析」，台灣金融財務季刊，第三輯第二期，91 年 6 月，頁 166－167。

者保護法第四條「企業經營者對於其提供之商品或服務，應重視消費者之健康與安全，並向消費者說明商品或服務之使用方法，維護交易之公平，提供消費者充分與正確之資訊，及實施其他必要之消費者保護措施。」，同法第十一條至第十七條規定之定型化契約解釋原則，以及甫於 2005 年 2 月 5 日增訂的第二十二條之一「企業經營者對消費者從事與信用有關之交易時，應於廣告上明示應付所有總費用之年百分率。前項所稱總費用之範圍及年百分率計算方式，由各目的事業主管機關定之」等規定。惟以渠等定型化契約作為紛爭解決之依據，恐怕約定條款是否足夠周全反應監理法規的規範精神，甚或還原雙方當事人交易時之本意，將之置於尚未形成統一見解的司法處理機制之前，或仍有進一步商榷的餘地。

2. 「個人電腦銀行業務及網路銀行業務服務契約範本」分析

前揭定型化契約範本中涉及風險與責任分配條款的公平性問題[170]，直接關係歸責事由的舉證分配。一般來說，以侵權行為作為請求權基礎時，故意或過失的歸責要件或經由舉證責任之分配歸於相對弱勢之被害人方負擔；若以契約為據提出請求賠償請求，責任歸責要件(債務不履行、不完全履行等)的舉證責任卻有由債務人方負擔。徵諸前揭舉證責任分配，於電子金融的實務中，倘相關定型化契約條款之解釋發生疑義，原應為利於消費者之解釋原則，是否逕自得解為銀行應負擔該條款之舉證責任；又或以定性電子訊息錯誤更正行為來決定舉證責任分配，顯然影響後續因錯誤所引發的損害賠償責任。另外，雖然契約範本僅為基準規範，金融業者可以自行增減內容，但目前尚

[170] 服務契約範本第十條：「客戶利用本契約之服務，如其電子訊息因不可歸責於銀行之事由而發生錯誤時，銀行不負更正責任，惟銀行同意提供必要之協助。但因可歸責於銀行之事由而發生錯誤時，銀行應負責更正。」

嫌簡略的範本內容條款之間的橫向配合似仍有疑問，是否可以加以增訂補充，又將見管制和促進開放、發展的目標間的衡平折衝。

此外，範本中對於冒用或盜用之損害僅課予「故意或重大過失責任」[171]，非屬一般有償契約的抽象輕過失責任，且在舉證責任分配上因消費者無法證明銀行有故意或重大過失，可能因而無法請求銀行負擔賠償責任。如此適用消費者保護法之規定，則該條款違反定型化契約條款平等互惠原則，當應推定為無效，而由銀行業者負擔提出反證推翻的舉證之責，較符衡平之旨。

至於範本中對於「駭客行為」的定義[172]過於狹隘，駭客有時根本不必採取上述破解授權使用者代號或密碼而入侵網路系統之行為即可進入系統造成消費者損害，此時其行為又回到本範本第十一條「其他任何未經合法授權之情形」規範，形成對消費者不利情形。

除應用上述消費者保護規定外，契約範本或應參照刑法第 339 條之三與第 360 條對於電腦犯罪的規定，對駭客行為做更廣泛定義，或於民事上修正駭客行為的舉證責任分配問題，使消費者僅需負主張責任，而由銀行負擔證明損害非由駭客行為造成之責。

相較於民事基本法－民法，前揭範本所涉賠償責任範圍似僅限於「所受損害」[173]，或許係考量到金融機構對風險控制與利潤合理需求

---

[171] 請參閱前揭「服務契約範本」第十一條：「雙方同意確保所傳送至對方之電子訊息均經合法授權。雙方同意於發現有第三人冒用或盜用授權使用者代號、密碼或憑證申請識別碼、私密金鑰，或其他任何未經合法授權之情形，應立即以電話或書面通知他方停止使用該服務並採取防範之措施。銀行接受通知前，對第三人使用該服務已發生之效力，除非銀行故意或重大過失而不知係未經合法授權之電子訊息，銀行不負責任。」

[172]有關駭客侵入的問題，涉及「服務契約範本」第十二條：「雙方應確保電子訊息安全，防止非法進入系統、竊取、竄改或毀損業務記錄及資料。因第三人破解授權使用者代號或密碼而入侵網路系統(駭客行爲)所發生之損害，由銀行負擔其危險。」的基本規定。

[173]請參閱「服務契約範本」第十四條：「雙方同意依本契約傳送或接收電子訊息，因可歸責於當事人一方之事由，致有遲延、遺漏或錯誤之情事，而致他方當事人受有損害時，該當事人僅就他方之積極損害(不包含所失利益)及其利息負賠償責任。」

所致，但對於處於資訊不對稱、資力不對等的消費者與金融業者間，似乎仍值進一步斟酌調整。

參、小結

面臨產業政策大力推展金融電子化的世代，強調便利的電子金融產品或支付機制已是不可避免，如何在促進發展與穩健監理間尋求調和，並由此出發建構兼顧公平的法制環境，實已刻不容緩。

圖表 7：

	我國法制現況	美國相關規定	我國與美國法制之比較
錯帳	信用卡定型化契約範本第十三條	1. Regulation Z－Truth in Lending Act(TILA) 12 C.F.R. § 226.13 2. Electronic Fund Transfer Act(EFTA) 15 U.S.C. § 1693 f、1693 h、1693 f (e)	1. 僅使用主管行政機關委由公會制訂、再經其同意的契約範本，似乎在法源位階上有所失衡。 2. 且定型化契約中之簡略規定使個案爭議全委由司法裁決，不確定性高。
詐欺	1. 信用卡盜刷-偽造變造支付工具罪(刑法§201-1 I)或行使偽造變造支付工具罪(§201-1 II)。 實務上認為行使偽造有價證券以使人交付財物，如果所交付者即係該證券本身價值，則其詐欺取材仍屬行使偽券的	1. Electronic Fund Transfer Act(EFTA) 15 U.S.C. § 1693 g 2. 15 U.S.C. § 1643 a (1) 3. Regulation Z－Truth in Lending Act(TILA) 12 C.F.R.	1. 法源位階低，規範保護不足。 2. 電子金融支付未見特別國外立法例。 3. 定型化契約中之簡略規定使個案爭議全委由司法裁決，不確定性高。

	行為，不另成立詐欺罪名[174]，而行使偽造變造支付工具罪與詐欺罪可以同一法理處理。 2. 電子現金-刑法§358 以下 3. 民法-侵權行為 4. 信用卡定型化契約範本第十七條		
洗錢	洗錢防制法(92.2.6 修正公布)及相關特別法，如金控法§§57-1、57-4	1. The Bank Secrecy Act(BSA) 31 U.S.C. § 5311~30、12 U.S.C. § 1818 (s)、1829(b)、1951~59 2. Money Laundering Control Act of 1986 (MLCA)18 U.S.C. § 1956~57, 31 U.S.C. § 5324~26 3. USA PATRIOT, Act of 2001 31 U.S.C. 5311 , the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 , 3 U.S.C. § 302(a)(2)	1. 金融資料庫 v.s.金融帳戶開戶查詢系統-隱私權保護疑慮 2. 無電子金融交易防制規範
財務隱私權&消費者保護	1.消保法§4、11~17、22-1 2.「個人電腦銀行業務及網路銀行業務服務契約範	1. Financial Services Modernization Act of 1999, 15 U.S.C. § 6801~09 2. Regulation P-PRIVACY OF	服務契約範本法源位階較低 2. 服務契約範本中消費者權益保護未周(ex：§10、11、12、14) 3. 個資法「事前同意」授

[174] 22 上 1814，62 年刑事庭會議第一次決議。

	本」 3.個資法§6、23④ 4.金控法§42、43、48、60 5.銀行法§28IV、48II	CONSUMER FINANCIAL INFORMATION 3. Right to Financial Privacy Act, 12 U.S.C. chapter 35 4. Fair Credit Reporting Act 15 U.S.C. § 1681 et seq	權尚具疑慮 4. 銀行法與金控法保密義務規定仍乏周延

第六章　結論與建議

隨著網際網路發展之日新月益，國際通行的支付工具及支付手段已由傳統之現金、支票、信用卡，演進為電子信用卡、電子支票、電子現金、及網路銀行等。而隨著網際網路公司經營型態的改變，帶動了消費者付費的觀念與習慣的改變，強調便捷與低成本的小額付費機制，包括：數位儲值卡、智慧卡與行動付款等，亦於各國蓬勃發展。從整體市場趨勢觀之，電子金融與電子付款機制乃為未來支付工具之新主流。基於前述研究及專家訪談之結果，本計畫就電子金融與電子付款機制可能面臨之問題，作出如下建議：

一、電子金融與新興付款電子機制涉及之法律問題

(一) 錯帳

我國金融法規中針對發生錯帳情形僅有在「信用卡定型化契約範本」第十一條及第十三條規定中，針對暫停支付機制與帳單疑義設有爭議處理規範，且規定內容對金融服務終端消費者過於嚴苛，無法涵蓋其他電子資金移轉錯帳之權益保護。由於錯帳事故的處理將影響消費者對於電子金融支付機制的信任與處理成本，若損失的風險越高，作業成本相對提高，勢將嚴重影響支付工具的流通。

就金融機關之責任，1. 建議仿照美國電子資金移轉法(EFTA)及美國誠實信貸法(TILA)之規定，首先定義錯誤。其次規定錯誤的處理方式：

a. 消費者發現錯誤時，應於收受相關文件一定期間內通知金融機構進行調查；

b. 金融機構應於受通知之一定期間內完成調查並通知消費者有關決定，或暫時性的入帳，並於一定期間內完成調查；

c. 若錯誤確實發生，應立即或至遲於決定後一個營業日內更正錯誤；

d. 若調查後發現並無錯誤，應於三個營業日內將調查結果遞交或郵寄客戶，並應依消費者要求提供可證其決定的文件證明；

e. 若金融機構未遵守上開期間規定，或未以善意進行調查時，或未附理由否認錯誤，消費者即可提起民事訴訟，主張相當於相當於若干倍錯賬金額之賠償。

2. 另建議依美國 15 U.S.C. §1693H 之規定，金融機關僅得於特別情事限制其賠償責任。

(二) 洗錢

就金融服務之洗錢防制，我國係以 1. 洗錢防制法第七條授權事項、第八條授權事項為主要建構；2. 在金融資訊庫建置上，我國僅設置有「金融帳戶開戶查詢系統」；3. 金融控股公司法第五十七條之一連結同條之四的規定，使以不正方法將虛偽資料或不正指令輸入金融控股公司電腦或相關設備、造成財產權變更或取得財產行為亦有洗錢防制法之適用。惟目前尚無專門針對電子金融交易設有防制的相關規定。

建議：

1. 仿照美國立法例銀行秘密法(BSA)，

a. 擴張金融機構之定義；

b. 要求金融機構必須配合政府就個人單筆金額超過特定數額之交易製作並保存交易紀錄及申報可疑交易資料；

c. 建立國內商業資料庫及金融資料庫，並透過推動國際合作以便使用國際資料庫。

2. 仿照洗錢控制法(MLCA)，

a. 對洗錢行為單獨處罰；

b. 禁止國內、國外超過特定數額之交易或移轉資金以及財產買賣，當該筆資金來源為特定非法行為；

c. 對意圖促使前述行為成功之人，或隱瞞、掩飾前述不法行為者，或漏未將此交易報經紀錄者，科刑處罰。

3. 並仿照美國愛國法(USA Patriot Act)，

a. 要求金融機構建立內控機制，設置專責主管，訓練員工及獨立審計以抑制和打擊洗錢；

b. 藉由金融機構與執法單位間更頻繁的資訊溝通，建立一套安全記錄機制；

c. 禁止金融機構擁有專供接收外國空殼銀行，以代替外國金融機構處理支付和金融交易的帳戶 (correspondent accounts)。

其他可行方法包括：保留查帳存底(audit trail)、確定客戶身份、發卡僅限於信用機構之帳戶持有人等。

(三) 詐欺

網路與行動付款之安全議題均涉及避免濫用及防止未經授權使用者之詐欺。

1、第三人未經授權使用之詐欺

盜刷事件，依我國刑法相關規定似得以偽造變造支付工具罪(刑法第 201-1 條第一項)或行使偽造變造支付工具罪(同條第二項)論處。在民事上則多以消費者保護法觀點審視消費者與發卡銀行間定型化契約以定其責任，個案中亦見探討特約商家是否盡到居發卡銀行履行

輔助人地位所應負之善良管理人注意義務。此外，信用卡定型化契約範本第 17 條亦設有約定的歸責依據。

實務上認為行使偽造有價證券以使人交付財物，如果所交付者即係該證券本身價值，則其詐欺取財仍屬行使偽券的行為，不另成立詐欺罪名，而行使偽造變造支付工具罪與詐欺罪可以同一法理處理。準此，新興電子錢包、儲值卡與智慧卡的盜用應依刑法第 358 條以下規定論處。另外，銀行法第 125-3 條則為銀行的詐欺特別規定。

至於信用卡遭偽造、盜刷情形，消費者在電子支付系統詐欺問題上，並未設有主張之法源，僅以定型化契約範本作為規範，位階嫌低，保障亦嫌失衡。值此消費者享受金融服務日趨便利之際，卻不見法制上相對的保障，似亦有商榷之餘地。建議仿照美國資金移轉法(EFTA)及誠實信貸法(TILA)，

a. 首先定義資金移轉；

b. 明定金融機構負有提供消費者關於遺失支付工具處理資訊之義務；

c. 明定消費者遺失支付工具時，除有例外情形(如消費者未於發現未經授權交易後一定期間內通知金融機構)，由金融機構回復被竊賊以遺失之支付工具所為的資金移轉，以及消費者應自行承擔損失之最高額；

d. 將未經授權的電子資金移轉之消費者訴訟，由金融機構負舉證責任，證明該筆移轉已獲授權，或證明符合消費者應自負責任之例外情形；

e. 並將重要資訊例如重要契約條款、利息計算方式、可能之風險等，以公告方式，公佈於網站明顯處，使消費者易於瀏覽，以決定是否與該金融機構進行交易。

在技術上，可建議消費者將帳戶金額分成兩部分管理。僅提撥少量數額至電子金融卡，如此一來，在操作之介面上不會看到消費者全部存款金額，即使帳號被盜，亦不會損失帳戶中之全數金額。另參酌美國財政部貨幣金融局(OCC) 建議各銀行的作法，建立雙重身份確任機制。並要求金融機構善盡宣導義務。

2、網址偽裝與網釣

常見之網路詐欺除第三人未經授權使用之詐欺外，還有網址偽裝與網釣，將消費者導引至詐欺網站，並被誘使消費者提供資訊，例如網路銀行之使用者名稱與帳號、信用卡資料、或其得使用客戶帳號以進行詐欺或竊取客戶身份之資訊。

此類盜用消費者資料之行為，在我國並無明確之刑法規定，雖然我國採用晶片金融卡的身份辨識後，可對於該等盜用行為有所防堵，但仍建議未來採用雙重身份確認機制，並採納美國財政部貨幣金融局(OCC) 2004 年第 24 號公告，

a. 明定金融機構應採行之偵測與收集偽裝網址資訊程序；

b. 指定並訓練特定員工負責針對此類事件作出必要且有效之回應，以降低網址偽裝帶來之衝擊；

c. 金融機構協助執法單位調查之義務；以及

d. 要求金融機構擬定具體應變措施。以保障金融交易之安全、消費者之權益以及金融機構之信譽。

(四) 隱私權

1、個人資料

我國有關個人資料之保護，散見於各個不同之法律：消費者保護法、電腦處理個人資料保護法、金融控股公司法、電子簽章法以及個人電腦銀行業務及網路銀行業務服務契約範本。上開規定或契約範本

看似多元，其實彼此之間的相互勾稽就會造成資訊隱私權防護的漏洞。且保密義務規定不夠詳細，僅作原則性保密規範，似乎無法完全保障消費者資訊隱私權。

A. 就金融機構之義務與責任，建議仿照美國金融服務現代化法案(FSMA)及消費者金融資訊隱私權法(Regulation P)，採行下列規定，將金融消費者資訊隱私的保護規範更予細緻化，且提高規範的法律位階，促使金融機構依法執行更為健全的財務隱私權保護措施：

a. 限制金融機構揭露客戶非公開的資訊予非分支機構之第三人；

b. 明定金融機構於何種情況下始得揭露客戶非公開的個人資料給非分支機構的第三人；

c. 要求金融機構必須提供清楚、明確反應其隱私權政策與執行的初次告知給將成為金融機構顧客的個人以及消費者，對消費者則必須在揭露任何消費者個人非公開資訊予非分支機構的第三人前告知之；

d. 明定隱私權告知應包含之事項；

e. 向消費者解釋其有避免金融機構揭露相關資訊的選擇權(opting out)，以其行使前述選擇權之合理方法；

e. 金融機構必須在接到消費者選擇權決定後在合理可執行的時間內立即遵守；

f. 消費者所做的選擇決定，其效力將持續到消費者自行另以書面撤回為止，而與同一人重新建立的顧客關係，將不適用於先前顧客關係中所為之選擇；

g. 晶片金融卡與之發卡銀行與其他事業合併或結盟時，消費者就儲存於晶片內之消費與信用資料所為之選擇，應不繼續適用，

h. 除有法定事由外，金融機構不得直接或透過分支機構，對非分支機構的第三人以電話銷售、郵件銷售或其他電子郵件銷售目的，提

供消費者帳戶金額、帳戶密碼、存款數額、信用卡密碼或交易數額之資訊。

並參酌美國美國財政部貨幣金融局(OCC) 2005 年第 13 號公告，就第三人非法取得金融機構客戶敏感資料之情形，為如下之規定：

a.定義客戶敏感資料；

b.明定金融機構知悉有未經授權取得客戶敏感資料之情事時，負有立即進行合理調查之義務，以決定該資料是有可能已被使用，或即將被使用；

c. 若該機構認為不當使用客戶資料之情事已發生或可能發生，明定該機構負有立即通知可能受影響之客戶之義務。然若執法機構認為通知客可能妨礙對犯罪活動之調查，且以書面請求金融機夠暫緩通知客戶時，金融機構得延緩通知受影響之客戶；

d. 要求提供服務之金融機構就未經授權取得該機構客戶資料之情事，擬定應變計畫等；

f. 要求金融機構建立內部控制機制，保留接觸客戶敏感資料之員工使用紀錄，並進行不定期查核。

且針對使用無線網路之金融機構，參酌美國財政部貨幣金融局 2003 年第 10 號 行政函令中，要求金融機構採行下列關鍵措施：

a. 於使用無線網路前，應先具備安全風險評估、合適的政策及充分的內部控制；

b. 安全措施應保護銀行之網路及無線設備免於未經授權之進入、截取傳輸資料、揭露機密客戶資訊及其他漏洞威脅；

c. 針對無線網路之安全測試計畫；

d. 應針對服務水準協議之表現水準進行監督，以確保無線解決方案之有效性；

e. 於決定計畫是否成功時，執行及維護網路之擁有權總成本或投資報酬率目標，包括增加之安全成本(例如身份驗證、監控、更新、測試)，亦應一併考量。

此外，在技術上可採行電子金融交易詳細資料分離保管制度，並依金融機構人員之職務需要，設定不同之讀取權限。

B. 就政府取得金融機構顧客財務資料之方式，建議仿照美國財務隱私權(Regulation F)之相關規範，限於以下列方式為之：經由顧客授權、取得行政傳票或傳喚、取得搜索票、取得司法傳票以及經由正式的書面請求。惟金融機構或其主管、雇員、代理人通知政府當局，其持有可能有關違反法律或規則的資訊時，例外地排除上開方式規定的適用，上開揭露者毋須負任何法律責任。此外，金融機構為附隨於完整擔保利益，證明破產請求權，債務催收或處理關於政府貸款、貸款保證等之申請而提供紀錄亦不在禁止之列。

C. 就消費者信用報告代理機關之義務，建議仿照美國公平信用評等法(FCRA)：

a. 要求此等機構採用合理的程序，以符合消費者信用、個人與保險或其他金融資訊的機密性、正確性、中肯與適當使用，並確保公平、公正且尊重消費者隱私權；

b. 建立修正消費者信用報告錯誤的程序；

c. 確保只在合法的商業目的下提供有關消費者報告；以及保留信用報告之義務。

2、位置隱私

目前我國對於行動支付之消費者隱私保障與安全，幾無任何監管法規與機制，建議政府單位針對行動電話製造業者與電信業者，仿照

日本「行動通訊個人資料保護辦法」、「個人資料保護法」、美國「位置隱私保護法」及歐盟「關於個人資料處理以及此類資料自由流動的個人保護指令」、「電子通訊隱私指令」：

a. 定義位置資訊；

b. 要求提供無線位置服務的公司於收集位置資訊時，須取得用戶同意，且客戶須能隨時撤回該同意；

c. 禁止未經用戶許可而逕行收集、銷售資訊或將資訊揭露予任何第三人。

四、未來政府政策之方向與相配套之措施

1、建立安全之交易環境

A) 最低法定要求與業者自律

因為交易安全性悠關電子金融之推行成敗，因此交易安全不宜完全放任業者自律，政府機關宜在技術上訂定最低法定標準，例如：各金融機構採用之系統廠商應符合之最低安全標準、安全讀取之限制、多功能用途智慧卡遭申報遺失後，透過第一次交易(如提款機、線上交易等)，產生追蹤功能，並就金融機構與參與小額付款系統之業者採行之身份確認與認証之標準與程序，作對低限度之要求。

B) 業者損害賠償責任與消費者權益之平衡

關於電子金融與電子支付機制中，特別是小額付費機制中，涉及之錯誤與詐欺，因最有風險承擔能力者，為金融機構，且金融機構得透過保險機制分散風險。故金融機構應對消費者明確揭示相關之可能風險，且於發生糾紛時，若消費者已善盡其誠實且立即告知之義務，由金融機構承擔風險。

2、智慧卡與行動付款之多重/整合運用

針對消費者小額消費之普遍與使用塑膠貨幣之消費習慣，現今台灣之企業，確有發行跨業現金儲值卡之需求，且隨著科技與網際網路為代表的新經濟發展，行動付款與遠端支付是電子錢包未來的一個重要發展方向。

惟目前礙於銀行法及金管會「銀行發行現金儲值卡許可及管理辦法」之規定，非銀行業之其他企業，縱算其企業達於一定規模或甚至比銀行之規模更大，仍礙於法令限制，不得發行跨業現金儲值卡。

借鏡香港八達通卡之經驗，為促進小額支付系統，政府宜推動電子錢包之統一的標準，並修改法令規定，使得不同產業之商家得聯合發行跨業之現金儲值卡，以加快電子支付系統發展之腳步。

3、其他

由於目前所行之 Micro-payment 機制大多欠缺政府機構或國際金融機構所提出，其間並缺乏清算體系，多種交易機制的提供並未對消費者產生實質的效益，反而造成無所適從的選擇成本問題及交易成本問題。因此，一個實質有效的 Micro-payment 機制，必須且必要建立起一套交易基準與清算體系，以降低交易成本。建議如下：

a. 市場中為達交易效率，本研究建議必須建立 Micro-payment 標準交易機制，並建立中介機構(其功能如同期貨市場之清算機構，以公正的第三者立場提供清算服務，不僅降低交易雙方之資訊不對稱問題，降低部份之資訊安全問題，且可提供基於同一電子金融支付工具應用於多種行業之間，或是在同業之競爭環境中，提供公正之中介清算服務)，透過這些機制的建立方能有效降低交易成本及效率損失。

b. 對於價值移轉的功能，在視同電子貨幣的情況之下將 Micro-payment 的內部貨幣外部化，建立交易基準之後方能達到規模

經濟，擴及其他之市場交易，方能擴大市場之接受度與相容度。另外，有關換匯機制的建立，亦可能是進行跨國網路交易時必須注意的。

c. 對於 peer to peer 的價值移轉，由於台灣地區現行的法令限制個人之間有關儲值卡的價值，對於支付層面而言，無疑多所限制，在價值移轉額度已經限制的情況之下，可以有限度地開放 peer to peer 的價值移轉，以利個體交易機制的進行。

4. 由於 Micro-payment 機制所建立的支付工具，因有邊際效用遞減的特色，有別於信用卡的發行市場，在整體發行計畫上必須提供整合之財務資訊服務給持卡者，方有效提升持卡者的持卡誘因，擴大發卡利基；但於財務資訊分享時，則宜考量資訊分類及防火牆。

5. 台灣由於地狹人稠，就小額儲值的支付工具發行雖有其潛力；但發卡市場由於屬於淺碟型經濟環境、亦有其有先天的環境上限制。是故，在小額消費的支付工具建立清算體系，將使其原有之替代性更加強化，而對於長期無法達成規模經濟和範疇經濟的發行計畫，發行業者必須謹慎評估其獲利基礎是否具有長期競爭力，在利基基礎不大的情況之下，發行計畫的風險將會危及獲利能力，此亦為業者自律範圍的考量因素。