個人網路銀行業務風險責任之探討

謝博武

前言

隨著資訊科技的進步使全球各地的電腦都能連成一線，人們透過網路的互動越來越普遍及頻繁，銀行經營透過網際網路之資訊即時性、資源共享性的特性，來提供金融服務並提高附加價值。由於網路銀行無時間地點限制，帶給個人與企業更即時化、多樣化、國際化、個人化的服務。新新一代年輕族群熟悉透過網路來進行各種交易，我們可以預見『網路銀行』發展將更為普及和接受。

一、網路銀行之形成與發展

九〇年代，網際網路發展日趨成熟創新，各銀行開始著手設立專屬網頁，而隨著銀行利用網　提供服務與資訊之情形日趨多元及完整，於一九九五年十月十八日，由美國幾家金融機構合資四千萬美元，成立之第一家完全虛擬之網路銀行「安全第一網路銀行」（Security First Net Bank）誕生，純粹透過網際網路之方式，對客戶提供各項服務，包括帳號餘額查詢、轉帳、票據止付、信用卡帳單查詢與繳納、申購基金、申請貸款、申請支票或公用事業帳單繳納等金融服務，客戶只要以個人電腦或數據機連上網際網路，利用瀏覽器便可進入該銀行之網站，搭配相關之交易安全方案，即時在網路銀行進行所需要之交易或服務。

在亞洲，以日本為例，在二〇〇〇年九月通過由櫻花銀行、富士通銀行及三井物產等企業聯合設立之日本網路銀行（Japan Net Bank）為日本第一家網路專業銀行。至於我國財政部於二〇〇〇年二月十五日核准財金資訊公司建置金融機構網際網路共用系統，提供銀行可經由網際網路提供非約定帳戶轉帳之電子銀行業務，民國二〇〇〇年三月二十八日公布國內首家通過審核，得透過開放性網際網路提供包括轉帳等服務之銀行，至二〇〇〇年九月

後，陸續又有多家銀通過審核，獲准開辦網路銀行。此階段網路銀行所提供之金融服務有：餘額查詢、約定帳戶之轉帳交易、繳稅交易、繳費交易、憑證申請交易、憑證更新交易、其他如基金、外匯之買賣、贖回及試算之功能及非約定帳戶之網路轉帳業務。

二、網路銀行之經營風險

但隨著網路蓬勃發展，也面臨越來越多駭客入侵(植入木馬程式)轉帳盜領或經詐騙網頁被偷竊有價資訊。詐騙網頁又稱網路釣魚（因為Phishing 與「fishing」（釣魚）發音相同，實際意義也相似）是一種網路詐騙手段，詐欺犯利用這種手段誘使您洩露個人資料。詐欺犯使用各種不同的誘騙手法，包括利用電子郵件或網站偽裝成信譽卓著的知名品牌。最常見的網路釣魚手法就是偽裝成知名公司或網站（例如銀行、信用卡公司、慈善團體或電子商務線上購物網站）傳送假造的郵件。這些郵件的目的就是要誘騙您提供個人識別資訊（PII）(個人識別資訊（PII）：透露個人詳細資料的任何資訊，包括姓名、國家、地址、電子郵件地址、信用卡號碼、健保卡號碼、身份證號碼及ㄇ位址等。)，例如：姓名，使用者名稱，密碼或ㄗㄔ。常見釣魚方式包括通知消費者帳號沒有修改或太久沒有登入，或通知需下載新的升級程式，或下載MP3、免費遊戲、身分證產生器等，而被植入木馬程式資料遭受盜取。網路犯罪投訴中心(Internet Crime Complaint Center)在2008年發佈的報告指出，該中心接獲的詐騙案件數在一年間上揚3百分之三十三，達到創記錄的二十七萬五千件。另一家機構美國聯邦貿易委員會(The Federal Trade Commission)則指出，二〇〇八年各個執法單位總共接獲一二〇萬件投訴案，比二〇〇〇年的二十三萬件增加甚多。

三、國內外新聞相關案例

國外：Nordea銀行為北歐最大的銀行，服務範圍涵蓋瑞典、芬蘭、丹麥及挪威四國，總計約有二二〇萬個客戶。根據歐洲各大媒體報導(二〇〇七年一月)，瑞典Nordea銀行發生有史以來損失金額最大的網路詐騙事件。過去三個月以來，駭客鎖定Nordea銀行客戶寄發電子郵件，要求下載謊稱為反間諜軟體的木馬程式，藉此盜取使用者的個人資料，並登入Nordea網路銀行轉走約八百萬瑞典克朗，折合超過一百萬美元。駭客以Nordea

名義寄發詐騙電子郵件給銀行客戶，要求下載宣稱為反間諜軟體的檔案，安裝在個人電腦上以確保交易安全，其實已遭名為Taxdoor.ts的木馬程式所感染。此木馬程式平時潛伏在個人電腦中，當使用者上網連結至Nordea網路銀行時才開始啟動，一一記錄使用者每一個敲擊的按鍵，藉以獲取使用者登入網路銀行所需的兩組密碼。事實上，使用者所連結的網址並非真正的Nordea網路銀行網址，使用者輸入資料後，便會出現錯誤訊息，表示銀行網路系統暫時無法運作，但此時個人資料已遭竊取。瑞典警方相信，這宗史上最大的網路詐騙是由位在俄羅斯的駭客所為，因為遭竊取的資料最先被傳送至位於美國的伺服器，最後再轉送至俄羅斯。目前瑞典警方已鎖定一二一個嫌疑份子。此次共有二五〇個客戶遭網路駭客詐騙成功，Nordea銀行表示這些客戶的個人電腦大多沒有安裝任何的防毒軟體。

國內：刑事警察局於民國96年4月間接獲中華郵政公司報案，指稱公司網路郵局遭駭客入侵，並將數十名客戶內之存款盜轉出後購買臺灣索尼網路購物商城之遊戲點卡等物品，再利用遊戲點卡交易洗錢，訴請偵辦。本案經深入追查發現該駭客集團除入侵中華郵政網路銀行將客戶存款盜轉走數百萬元外並且入侵健保局、教育部及多家電信公司資料庫竊取個資建立全台超過五千萬筆民眾個資資料庫，資料庫內含政府官員、民意代表、企業界人士及一般百姓等等幾乎無一倖免，案經專案小組彙整蒐集相關不法駭客入侵資料，追查網路連線紀錄及不法駭客入侵之路由等事證，發現駭客上網可屬主機代管服務；進一步追查發現該主機係由大陸人士所承租，更發現所有入侵主機的可來源遍及大陸地區且利用國內北中部地區大學當跳板，係兩岸集團性作案，並追查得知在臺之犯罪集團涉有嫌疑，警方更發現該駭客集團除了入侵中華郵政網路銀行將客戶存款盜轉走數百萬元外並且入侵健保局、教育部及多家電信公司資料庫竊取個資及東森購物台刷卡人資料整合建立全台近五千萬筆個資資料庫網站，該集團並以查詢每筆資料約三〇〇元代價販賣給不法集團。

四 我國網路銀行業務相關責任之規定

針對網路銀行業務並無特別公布專門法令，而係以「金融機構辦理電子銀行業務安全控管作業基準」及「個人網路銀行業務服務定型化契約範本」，作為網路銀行業

務之監管基準及網路銀行與消費者間權利義務規範之基礎架構。 修正前之「個人電腦銀行業務及網路銀行業務服務契約範本」內容為界定釐清網路銀行與消費者之間權利義務關係、風險分配及責任歸屬，財政部委請銀行公會擬定相關定型化契約約款，於民國一九九九年五月二十六日以八八台財融字第八八七二五二 三發布「個人電腦銀行業務及網路銀行業務服務契約範本」，擬定關於消費者使用網路銀行之一般性共同約定，提供予各網路銀行參考，作為各銀行與消費者間簽定網路銀行契約之約款內容。

經網路銀行之定型化契約於發布數年之後，行政院金融監督管理委員會採納行政院消費者保護委員會、學者專家及業者代表等之意見予以修正，名稱亦修正為「個人網路銀行業務服務定型化契約範本」。 該範本原有二十四條，本次計增訂三條，修正二十三條，修正後增為二十七條，其修正重點如下：一、為了防堵詐騙集團偽造網路銀行網頁，詐取客戶帳號及密碼，本次範本第三條增訂「客戶使用網路銀行前，請先確認網路銀行正確之網址，才使用網路銀行服務。銀行應盡善良管理人之義務，隨時注意有無偽造之網頁。」二、有關第三人盜用帳號所生之損害，過去網路銀行的使用者必須證明銀行故意或因重大過失不知第三人盜用帳號的事實，才能向銀行請求損害賠償。本次範本將第十三條規定修正為「除非銀行能證明客戶有故意或過失者外，銀行仍負責任」，將舉證責任轉由銀行負擔，使網路銀行的使用者更有保障。三、有關駭客入侵網路系統所發生之損害，本次範本第十四條規定修正為「駭客入侵銀行之電腦或相關設備者所發生之損害，由銀行負擔」，使銀行負起確保電腦及網路之安全義務。四、為了加強個人資料之保密義務，本次範本第十五條增訂經他方同意將其資料告知第三人時，第三人應負保密義務。若該第三人不遵守保密義務，視為本人義務之違反。五、為釐清損害賠償責任，本次範本第十六條規定修正為「當事人僅就他方所生之損害及其利息負賠償責任。但銀行或其履行輔助人有故意或重大過失時，仍應就客戶所失利益負賠償責任」，以加強銀行故意或重大過失時之責任。六、鑑於網路銀行使用之安全性須由銀行與使用者共同維護，增列「客戶使用網路銀行注意事項」，俾網路銀行的使用者注意遵行，以加強網路銀行使用安全。

五 國內責任保險之開發及內容

經銀行公會及保險局邀請研究相關責任保險，產險公會即成立專案小組，收集國外相關網路銀行業務責任保險與國內銀行溝通及收集損失經驗並依保險公司過去開發新保單的經驗綜合各方面需求，於二〇〇九年六月二十二日由產險公會備查（公會版）的個人網路銀行業務責任保險。

其承保範圍為被保險人於追溯日起至保險期間屆滿日前，針對其所提供之個人網路銀行業務，因過失、錯誤或疏漏行為，違反其業務上應盡之義務，致第三人受有損失，依個人網路銀行業務服務定型化契約應由被保險人負賠償責任，而在保險期間內或保險契約所約定之發現期間內初次受第三人賠償請求時，保險公司依保險契約之約定，對被保險人負賠償之責。其理賠項目及範圍為被保險人於保險契約所載之承保範圍內遭受賠償請求時，保險公司就被保險人依個人網路銀行業務定型化契約應負之損害賠償責任及所發生之抗辯費用，負賠償之責：一、依個人網路銀行業務定型化契約應負之損害賠償責任：係指被保險人依法院判決、仲裁判斷書，以及經保險公司參與並同意之和解書所載應負擔之賠償金額。二、抗辯費用：係指被保險人因其所提供之個人網路銀行業務而受賠償請求時，於中華民國臺灣地區所發生之律師費用、訴訟費用、鑑定費用及其他規費，事前經保險公司書面同意者，由保險公司負賠償之責。

結論

新資訊科技不斷引進讓網路銀行更為普級方便但也帶來更多威脅，風險評估充滿許多不確定性。網路銀行與一般電子商務所面臨問題，像管轄權、電子證據、爭端解決機制，都值得進一步研究探討。韓國為了加強網路銀行業務的交易安全依Financial Supervisory Service (The Financial Supervisory Service (FSS) is South Korea's integrated financial regulator that examines and supervises financial institutions）有特別控管及查核的規定並將投保責任保險為強制性以保障消費者的權利。我國目前尚未有強制性投保網路銀行業務責任保險的規定。但國內銀行業者可以藉着購買責任保險，來分散風險並增加網路銀行使用者的信心。

（作者：聯邦產險公司協理）