No.:1-17001-11
出版日期: 2017/01/20 v.1

中信銀—eTrust 網路銀行個資事件[1]

游士瑩　蘇雅惠　林裕得　連文雄[2]

事情是從 ptt 開始的……

2013 年 5 月 13 日晚上九點左右，一位 ptt 鄉民貼文爆卦 (詳見圖 1-1)[3] 指出，因接到不認識的房仲業者打到他家的室內電話詢問，讓他驚覺自己的個資可以透過 Google 被查詢到。ptt 鄉民們紛紛於此貼文下方留言熱議到凌晨左右，時值 5 月 10~16 日「鍵盤開戰行動[4]」事件，台灣與菲律賓兩國駭客陸續攻擊或癱瘓對方重要官方網站 (但不包含交通、金融、醫療資源等民生必需相關網站[4])，因此有兩位鄉民嘲諷「其實是菲律賓駭客搞的[3]」「菜鳥工程師快推給菲律賓就可以無事了[3]」

次日新聞指出：用戶在中信銀 eTrust 網路銀行 (下文簡稱 eTrust) 繳費中心網頁下拉常用繳費項目時，顯現數量眾多的個人資料[5]。「……此事件於 ptt 上爆料之後，隨即於網路間傳開，有科技部落客連上 eTrust，發現洩漏的個資包含姓名、電話號碼、手機號碼、身份證號碼、信用卡卡號、人壽保險號碼、交通違規罰款編號、車主身分證字號、出生年月日……等，估計約有五萬七千多筆，並且不需要登入網站即可看見。」[5]

中國信託商業銀行 (下文簡稱中信銀) 於 5 月 14 日發布新聞稿表示「接獲客戶通知後，在 5 月 13 日晚上 10 點就已經緊急關閉該繳費中心網頁，並聯繫 Google 刪除暫存的網頁」[6]，新聞

---

[1] 本個案摘錄自《中山管理評論》(2016.12) 管理個案專刊，p. 663~703，原題目為「eTrust 網路銀行個資事件」，著作財產權屬於財團法人光華管理策進基金會所有。

[2] 作者游士瑩為上海交通大學凱原法學院經濟法研究所博士候選人；蘇雅惠為國立中央大學資訊管理學系助理教授；林裕得為旭得數位有限公司創辦人兼執行長；連文雄為國立中央大學資訊管理學系助理教授。

[3] http://disp.cc/b/337-5GSB (access date: 2016/4/12)

[4] 此為 2013 年 5 月 9 日上午廣大興事件－台灣的民間漁船廣大興號遭菲律賓海巡署的公務船以機槍射擊造成船長中彈身亡事件－所引發的台菲兩國網路駭客於 5/10 開始之網路戰爭行為後續事件。https://zh.wikipedia.org/wiki/鍵盤開戰行動 (access date: 2016/4/12)

[5] https://tw.news.yahoo.com/中國信託網路銀行疑個資外洩-五萬多筆資料看光光-025435160.html (access date: 2016/4/12)

[6] http://www.ithome.com.tw/node/80425 (access date: 2016/4/12)

稿中證實繳費網頁出錯，但否認有網銀交易資訊外洩[6]。

eTrust 此個資外洩事件，是新版《個人資料保護法》(下文簡稱個資法) 自 2012 年 10 月 1 日正式實施後發生的第一起銀行個資外洩事件[6]。狀況顯示個資已經被 Google 收錄，因此引發銀行用戶對個資安全的疑慮。

Disp BBS guest 註冊 登入(i) 線上人數: 3100	回
列表	
(←) 分享	
※ 本文轉寄自 ptt.cc 更新時間: 2013-05-14 06:15:09	
作者 iam186 (iam186)	看板
標題 Gossiping	
時間 [爆卦] 某銀行疑似洩漏個資	
Mon May 13 21:04:25 2013	
因今天某房仲打到我家室內電話來問是否持有某新竹的房產. 但就很好奇他是怎麼取得我家的電話的. [C 他說他是 google 來的,還說我可以自己 google 看看. 結果 google 下去不得了了~~ 大家快來看看自己繳費時有沒有留下電話歐! http://ppt.cc/KirT 應該是不知哪個死菜兵第一天寫程式 撈錯 table,開心的跑完 for 迴圈也不上線首驗 就這樣把大家的資料公諸於世 大家進去檢查一下吧,option 裡面大約有四千多筆資料	

圖 1 一位 ptt 鄉民貼文「 [爆卦] 某銀行疑似洩漏個資」之本文[3]

資料來源：註腳3 http://disp.cc/b/337-5GSB

We Are Family

中國信託金融控股(股)公司(下文簡稱中信金) 成立於 2002 年 5 月 17 日，最初由中信銀以股份轉換方式成立，企業總部設於臺灣臺北市，全球員工人數超過 15,000 人。中信銀是中信金全資擁有的子公司，前身為由辜振甫先生發起成立於 1966 年的「中華證券投資公司」，2014 年 7 月為止，為臺灣第一大信用卡發卡銀行。1999 年 12 月，中信銀開辦網路銀行服務。[7, 8, 9]

中信銀官網公佈自 2005 年伊始連年得獎記錄，2012 年官網條列國內共 29 與國外共 34 單位頒給的獎項。例如：中信銀於 2012 年元月榮獲歐洲貨幣雜誌 (Euromoney, January 2012) 評選為「臺灣最佳本國財富管理銀行 (Best Local Private Bank)」、「最佳客戶資料保密與安全機制服務 (Best for Privacy and Security)」、以及「最佳高資產客戶銀行服務 (Net Worth Specific Services—super affluent US$500,000 to 1 million)」。[10]

[7] http://www.ctbcholding.com/abo_intro.html (access date: 2016/4/12)
[8] https://zh.wikipedia.org/wiki/中國信託金融控股 (access date: 2016/4/12)
[9] https://zh.wikipedia.org/wiki/中國信託商業銀行 (access date: 2016/4/12)
[10] http://www.ctbcholding.com/honor12.html (access date: 2016/4/12)

展望未來，中信銀將秉持著「We are family」的品牌精神，「守護與創造」的企業使命以及「關心、專業、信賴」的品牌特質，為客戶提供更方便的服務管道和更多元的金融服務，打造臺灣第一、亞洲領先的領導品牌，成為客戶心目中最值得信賴的金融服務機構。[7]

中信銀之 e 化及資訊安全管理

1997 年至 2001 年間，中信銀導入 Financial Network Service (FNS) 系統。1999 年 12 月，中信銀開辦網路銀行服務。2002 年中信銀重金投資、拍攝的「感謝廣告」影片，主要是向推動 e 化的員工表示謝意。這一項投資 10 億元、歷時 3 年 (從 1997 年開始、2001 年 1 月上線 FNS) 的企業 e 化改造工程，讓中信銀從此脫胎換骨，不僅加速了新服務上市和業務流程，也奠定了未來邁向國際的基礎。1994 年中信銀剛改制，一切都還在摸索階段，當時金融界的 IT 應用仍傾向保守，而最賺錢銀行的幕後 IT 推手則是張汝恬，她於 1996 年借調到中信銀，因表現良好，於是被董事長辜濂松直接延攬到企業內部。從中信銀的公司年報顯示，張汝恬於 2010/4/12~2012/6/29 擔任資訊長 (CIO)，而中信銀 2013 年報內的組織圖已經沒有資訊長一職了。[11、12]

2008 年左右，中信銀資訊管理部協理張碩暉表示：「中信銀的 IT 部門，成立之初就被要求要支援業務，4、5 年前更被要求要實現業務的發展，在這樣的情況下，IT 人員當然會瞭解業務的需求。2 年前，中信銀的 IT 組織再造，將原來集中式的資訊管理，改為視需要來和業務串連，至今變成只要和業務有關的應用，IT 的老闆就是各事業單位的主管，IT 思維當然會符合業務的需求。中信銀每年會選一個年度的重要創新業務，在這項業務上，不僅要衝第一家、也要衝最快，對 IT 來說，就是資訊系統要能跟得上，像在 1974 年推出國內第一張信用卡、1990 年是第一家獲准到國外設立據點的民營金融機構等。而 1994 年成立台灣第一家無人銀行，也讓網路和通路開始展開密不可分的關係。一開始是因為要推自動化設備才建置無人銀行，所以中信銀的網路銀行甚至還提供客戶撥接網路的服務，到了 2000 年，政府核准網路銀行，才在網路上提供服務。」[13]

2009 年左右，中信銀拉高了資安委員會 (Security Review Board) 的層級，成為更符合現況的資安政策，該組織是直接報告到作業風險層級，任何資安政策在各部門要如何落實、執行都會透過這個委員會形式的主管機構來形成一個機制，其中包含了資訊、人事、稽核、法務、事業單位、風控代表等，原來是只有在中信銀體系裡建立，如今已經拉到金控的階層，並且會與金控的其他子公司進行意見交換、彼此分享。[14]

---

11 http://www.ithome.com.tw/node/28216 (access date: 2016/4/12)
12 http://www.ctbcholding.com/ir_index.html (access date: 2016/4/12)
13 http://www.cio.com.tw/article_in.aspx?aid=398 (access date: 2016/4/12)
14 http://www.informationsecurity.com.tw/article/article_detail.aspx?aid=5462#ixzz45aaZKo8r (access date: 2016/4/12)

而與資訊安全管理制度相關的銀行必定遵守的「金融機構辦理電子銀行業務安全控管作業基準 (下文簡稱安控法)」以及「中信銀內控內稽制度」，則分別摘錄於附錄 A5 及附錄 A6。

中信銀 eTrust 網路銀行客戶個人資料外洩事件

2013 年 5 月 13 日晚上九點左右，一位 ptt 鄉民發文指出自己的個資可以在 Google 上輕易地被搜尋到，因而被鄉民們接力揭露此次 eTrust 客戶個人資料外洩事件。鄉民們發現在 eTrust 網站的繳費中心可隨意檢視大筆其他用戶的資料，而看過這些資料的部落客重灌狂人表示，繳費資料紀錄包含姓名、家中電話、手機、信用卡號等等總共有 5 萬 7000 多筆[15]。此部落客在自己的部落格發文說明此個資外洩事宜，並於文章一開始先表示「5/13 晚上 10:30 PM 更新：在文章發出去後沒多久，中信銀就把洩漏個資的網頁整個撤掉了，後來去查 Google，似乎還有少部分資訊還搜尋得到！但是在今天之前，有多少人看過、蒐集了這些已經暴露不知道多久的資料…沒人知道。」[16] 此部落客在其文章中，附上 eTrust 網站資料外洩的相關畫面截圖 (如圖 2～圖 7 所示)[16]。

圖 2 部落客之部分截圖與說明一 [16]

資料來源：註腳16 https://briian.com/10793/chinatrust-credit-card.html

[15] http://www.ithome.com.tw/node/80303 (access date: 2016/4/12)
[16] https://briian.com/10793/chinatrust-credit-card.html (access date: 2016/4/12)

圖 1-3 部落客之部分截圖與說明二[16]

資料來源：註腳16 https://briian.com/10793/chinatrust-credit-card.html

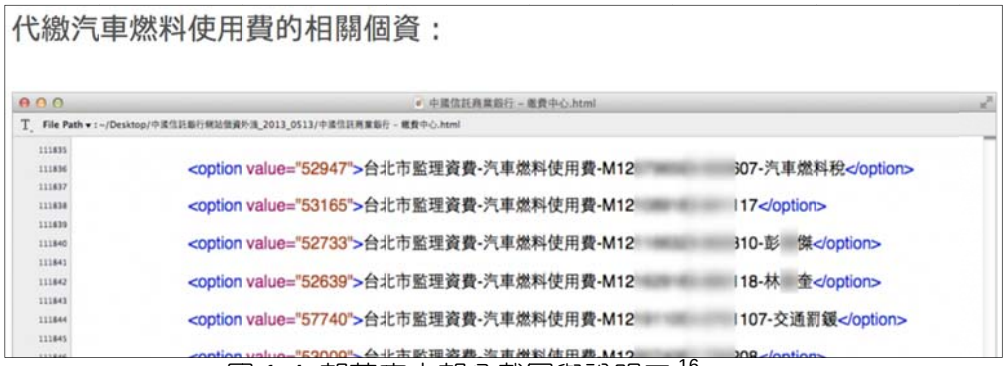

圖 1-4 部落客之部分截圖與說明三[16]

資料來源：註腳16 https://briian.com/10793/chinatrust-credit-card.html

圖 1-5 部落客之部分截圖與說明四[16]

資料來源：註腳16 https://briian.com/10793/chinatrust-credit-card.html

圖 1-6 部落客之部分截圖與說明五 [16]

資料來源：註腳16 https://briian.com/10793/chinatrust-credit-card.html

圖 1-7 部落客之部分截圖與說明六 [16]

資料來源：註腳16 https://briian.com/10793/chinatrust-credit-card.html

5 月 14 日一平面媒體報導：「中信銀公關系統今凌晨回應指出，經內部查證，網銀繳費中心交易系統確實有異常，已先將該系統關閉，但外洩資料均為客戶自行設定的繳費項目 (如電費、水費) 及代號，並無任何客戶姓名與帳號資料外洩。」[17] 該媒體並報導：「5 月 13 日中信銀網銀約在十時於首頁公告：『由於目前交易量大，交易回應速度稍慢，若有無法登入網路銀行的情況，請您稍後再試，造成不便，敬請見諒。』」[17]。

該報導繼續指出：「針對 ptt 相關內容，中信銀公關系統回應，昨晚確有接獲客戶電話，反映網銀交易系統個資外洩，經調查，發現繳費中心交易系統確有異常，但尚無法確知是內部還是外部問題，因此先關閉繳費系統，但其他如網路轉帳等功能均正常運作。中信銀表示，已盡力向客戶說明及溝通，並維護客戶權益，惟針對網友爆料有客戶電話及姓名資料等外洩，中信銀強調，均為客戶自行設定透過網銀繳交費用項目及代號，客戶姓名、帳號等資料並未外洩。」[17]

5 月 17 日另一電子媒體指出，針對此個資外洩事件，金管會限一周完成災情調查。該媒體

[17] http://www.appledaily.com.tw/appledaily/article/headline/20130514/35016413 /中信銀網銀傳外洩四千筆個資 (access date: 2016/4/12)

報導：「5 月 14 日中信銀書面表示，發生異常的是網路銀行『繳費中心』的常用帳號設定功能，這是專供客戶自行設定繳費項目及代號資料，和其他網路銀行的功能無關，也沒有承認有個資外洩，僅表示將主動通知受駭用戶，並委由鑑識團隊調查。不過，金管會銀行局副局長邱淑貞表示，中信銀通報金管會時有說明，外洩個資都是使用者自行註記在備註欄中的資料，沒有信用卡卡號。」[6]「從網路釋出的網站出錯畫面中，可以看到中信銀網路銀行繳費中心網頁外洩的個資包括姓名、室內電話、手機、身份證字號及信用卡號資料等。這些資料都被 Google 搜尋引擎擷取到暫存網頁和索引中。」[6] 媒體報導表示：「經兆法律事務所律師黃意森表示，由於這起事件情節明顯，除非中信銀可以證明已經善盡保管義務，不然受害者可以向中信銀要求法定金額範圍內的賠償。預估受害者一旦提出訴訟求償，3.3 萬名受害者，中信銀可能將面對 1,650 萬元到最高 2 億元的賠償金額。」[6]「儘管中信內部仍在調查中，但若是內部疏失，聖藍科技研發技術長王建興認為，事件可能導因於資料庫程式設計的問題，導致查詢資料條件過於寬鬆，使用者能查詢到的資料遠多於其權限所賦予的。此外，他也認為系統上線前的測試環節不夠嚴謹，案例不夠完備，導致連最容易發生的狀況都沒有檢查到。王表示，雖然漏洞是因程式設計人員設計差錯，但是系統開發流程應要確保所有差錯在上線前，都已被偵測及修正，何況這是個相當明顯的失誤，只要妥善制定好開發流程，應該不難發現這個問題。」[15]

事件發生約一個多月後，6 月 20 日，台北金融系統論壇社發文報導中信銀商業銀行 IT 組織異動 (詳見附錄 A1)。而此事件後續在網路上的討論熱度則如附錄 A2 所示。金管會並於 2013 年 8 月 22 日公佈裁罰中信銀 400 萬元，裁罰全文詳見附錄 A3。金管會網站公佈自 2012 年 1 月以來的所有裁罰案件，關於銀行局 2012/1/1~2013/9/1 的裁罰統計數字則請參考附錄 A4。而此事件發生後，除了金管會裁罰中信銀 400 萬元以外，後續並沒有關於任何客戶告中信銀民事或刑事的相關新聞報導，也沒有中信銀挽回或補償客戶行動的相關新聞報導。附錄 A5 則補充後續相關事件或改變的相關資料。

中信銀在其 2013 年 7 月出版的「2012 年企業社會責任報告」[18] 第 26 頁則以「提高網路安全機制，保護客戶資料免於外洩」為標題，簡要說明此事件及公司針對此事件後的改善措施：

一、2013 年 5 月間發生部分客戶資料疑似洩漏事件，可能洩漏之資料為客戶於網路「繳費中心」自行設定代扣繳之電話號碼、電號、監理資費等常用繳費資料，並未包含帳務交易資料，可能受影響的客戶約 1 萬名。

二、本公司為保障客戶權益，於 2013 年 5 月 14 日向警方報案，警察機關已著手進行調查。為確保不再發生此類事件，進行下列改善措施：

(一)專人電話聯繫或書面專函方式主動通知此一事件受影響之客戶，並妥適溝通客戶權益補償方案，於 2013 年 5 月 24 日完成。

[18] http://www.chinatrustgroup.com.tw/2012CSR.pdf (access date: 2016/4/12)

(二)因應此一事件，針對類似網址內容設定之流程和權限控管，納入複核範圍。每季定期委由外部資安專家執行資安審核及滲透測試。

(三)針對常用繳費功能的「繳費資訊」欄位，部分資料採隱碼顯示，並提醒客戶避免於自行設定之「暱稱」欄位輸入個人資訊。

(四)於本公司網路銀行首頁放置相關聲明警示文句，提醒外界人士勿以非法或未獲授權方式擅自重製、摘錄、擷取、轉載、散佈或改作網站之全部或部份內容。

問題與討論

一、 試分析中信銀在此次事件中，犯了哪些錯誤？你覺得個資外洩的問題，誰該負責？

二、 如果你是中信銀資訊部門最高主管，對於個資保護的資訊安全做到的程度，在成本、安全控制、及使用者便利性三者中，你會如何權衡取捨呢？

三、 你若是中信銀資訊部門最高主管，針對此次個資外洩事件，你覺得公司內部資訊安全管理制度如何能夠改善呢？是否需增加人手進行分工呢？

四、 發生個資外洩事件這類事件，「成本」與「商譽」何者較為重要？

五、 根據本個案提供的資料，你認為中信銀高層對於資訊管理部門的定位是什麼呢？如果你是中信銀資訊部門最高主管，你會如何因應呢？

附錄 A

附錄 A1：台北金融系統論壇社發文報導中信銀商業銀行 IT 組織異動[19]

圖 A-1 2013 年 6 月中信銀商業銀行 IT 組織異動 [19]

資料來源：註腳19 http://www.tbics.com/node/1716

附錄 A2：Google 趨勢之主題討論熱度

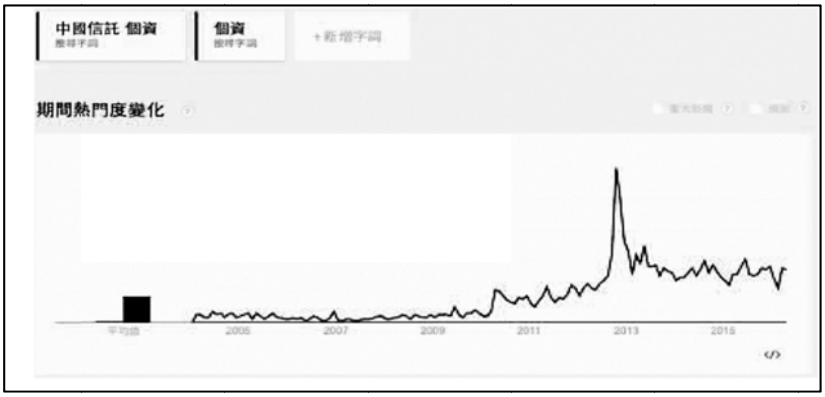

圖 A-2 中信銀個資與洩漏個資之討論熱度[20]

資料來源：註腳20 https://www.google.com.tw/trends/

[19] http://www.tbics.com/node/1716 (access date: 2016/4/12)
[20] https://www.google.com.tw/trends/ (access date: 2016/4/23)

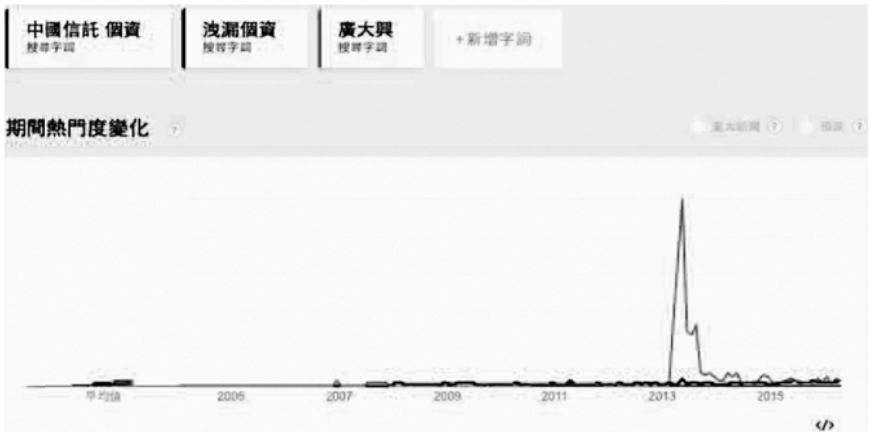

圖 A-3 中信銀個資與洩漏個資討論熱度 vs.廣大興事件討論熱度 [20]

資料來源：註腳20 https://www.google.com.tw/trends/

附錄 A3：金管會銀行局裁罰中信銀個資外洩案全文[21]

目前瀏覽位置：首頁 > 公告資訊 > 裁罰案件

裁罰案件

中國信託商業銀行辦理網路銀行業務發生疏失，導致客戶個人資料外洩，核有未落實執行內部控制制度之缺失，違反銀行法第45條之1第1項規定，依同法第129條第7款規定，核處新臺幣400萬元罰鍰。

受文者： 如正、副本

發文日期：中華民國102年8月22日

發文字號：金管銀控字第10200181601號

受處分人姓名或名稱：中國信託商業銀行股份有限公司

統一編號：03077208

地址：臺北市信義區松壽路3號

代表人或管理人姓名：童兆勤

身分證統一號碼：略

地址：同上

主旨：中國信託商業銀行辦理網路銀行業務發生疏失，導致客戶個人資料外洩，核有未落實執行內部控制制度之缺失，違反銀行法第45條之1第1項規定，依同法第129條第7款規定，核處新臺幣400萬元罰鍰。

事實及理由：貴行於本(102)年4月13日將貴行之網站索引檔案上傳予網路搜尋引擎業者，惟貴行對網站索引檔案產出程式之設計未臻嚴謹，對相關檔案驗證方法及程序亦有欠周延，且未對貴行內部目錄網頁之讀取權限作嚴謹控管，導致一般網路使用者得進入瀏覽並取得貴行內部目錄網頁所留存之客戶資料，受影響之客戶數達33,320戶，資料筆數計57,297筆。貴行亦未能有效發現外部人士瀏覽貴行內部目錄網頁，核有未落實執行內部控制制度之缺失，違反銀行法第45條之1第1項規定。

法令依據：銀行法第129條第7款規定。

繳款方式：

一、繳款期限：自本處分送達之次日起10日內繳納。

二、請依本會銀行局檢附之繳款單注意事項辦理繳納。

三、本案聯絡人：蔡少懷，聯絡電話：（02）8968-9828，傳真電話：（02）8969-1359。

注意事項：

一、受處分人如不服本處分，應於本處分送達之次日起30日內，依訴願法第58條第1項規定，繕具訴願書經由本會（新北市板橋區縣民大道2段7號18樓）向行政院提起訴願。惟依訴願法第93條第1項規定，除法律另有規定外，訴願之提起並不停止本處分之執行，受處分人仍應繳納罰鍰。

二、受處分人如逾本處分所定繳款期限不繳納罰鍰者，即依行政執行法第4條第1項但書規定，移送法務部行政執行署所屬行政執行處辦理行政執行。

正本：中國信託商業銀行股份有限公司（代表人童兆勤）

副本：金融監督管理委員會檢查局、本會銀行局(金融控股公司組、會計室、秘書室)

[21] http://www.fsc.gov.tw/ch/home.jsp?id=131&parentpath=0,2&mcustomize=multimessages_view.jsp&dataserno=201308220001&aplistdn=ou=data,ou=penalty,ou=multisite,ou=chinese,ou=ap_root,o=fsc,c=tw&toolsflag=Y&dtable=Penalty (access date: 2016/4/12)

附錄 A4：金管會銀行局 2012/1/1~2013/9/1 之裁罰統計數字[22]

金管會網站公佈自 2012 年 1 月以來的所有裁罰案件，銀行局於 2012/1/1~2013/9/1 總共裁罰 31 案件，其中有 5 個裁罰案是針對個人罰款 10 萬 (四件) 及 45 萬 (一件)，其他 26 件則針對銀行裁罰，相關統計數字詳見表 A-1。

表 A-1 金管會銀行局 2012/1/1~2013/9/1 針對銀行之裁罰統計表

處罰對象	處罰方式									
銀行	糾正	100萬	200萬	300萬	400萬	500萬	600萬	停止業務	停職	合計
	0	3	12	2	3	2	3	1	0	26
連帶解除銀行職員職務	0	0	7	2	1	2	0	0	0	12
連帶限制措施	0	0	0	0	0	0	1	0	0	1

資料來源：本研究整理

附錄 A5：金融機構辦理電子銀行業務安全控管作業基準[23, 24]

安控法乃銀行公會聯合各銀行討論出的自律規範，並送交銀行之主管機關－金管會銀行局核備，每家銀行一定會遵循並執行，因為金融檢查也會依據安控法來檢查。安控法的自 99 年 7 月開始陸續制定、核備、與修改，最新修訂版於 2016 年 4 月 1 日。本附錄摘錄銀行公會 102 年 3 月 28 日討論通過的安控法中，與本個案相關的部分條文如 2、網際網路應用系統之安全設計：

金融機構提供網際網路應用系統，應遵循下列必要措施：

(1) 載具密碼不應於網際路上傳送。

(2) 系統應設計連線 (Session) 控制及網頁逾時 (TimeOut) 中斷機制。

(3) 系統應辨識外部網站及其所傳送交易資料之訊息來源交易資料正確性。

(4) 系統應辨識客戶輸入與接收之非約轉交易指示一致性 。

(5) 系統應避免存在網頁程式安全漏洞(如 Injection、Cross-Site Scripting 等)

(6) 系統應偵測網頁與程式異動時， 進行紀錄與通知措施。

(7) 元件應驗證網站正確性。

下略

[22] http://www.fsc.gov.tw/ch/home.jsp?id=131&parentpath=0,2 (access date: 2016/4/12)
[23] http://db.lawbank.com.tw/FLAW/FLAWDAT08.aspx?lsid=FL007892&ldate=20130614 (access date: 2016/6/6)
[24] ba.org.tw/word/安控基準修正總說明_20130603.doc (access date: 2016/6/6)

附錄 A6：中信銀官方網站之「內控內稽制度」[25]

- 「內規盤查」清點作業：啟動本公司內規清冊之盤點作業，要求各內規管理單位檢視內部或外部法規是否有不一致情形，以避免作業風險或違法缺失。

- 落實「內部控制」制度：為確實管理內控程序，中信銀亦要求各單位配合進行自我查核，針對管理階層監督與控制文化、風險辨識、控制活動與職務分工、資訊與溝通、監督活動與導正措施等項目進行評估，包括是否訂定適當之內部控制政策及監督其有效性及適切性、是否有效辨識可能產生之重大風險、是否設立完善之控制架構及訂定各層級內控程序、是否有適當職務分工、建立有效溝通管道等。

- 建立「內部稽核」制度：為協助董事會及管理階層查核及評估內部控制制度運作有效性，遵循「金融控股公司及銀行業內部控制及稽核制度實施辦法」建立總稽核制度，並設置隸屬董事會內部稽核單位，秉持獨立客觀的立場執行稽核業務，適時提供改進建議，以合理確保內部控制制度，包含公司內企業社會責任實務守則建立、推動等，得以持續有效實施，進而促進公司永續經營。內部稽核單位對本公司每年至少辦理一次一般業務查核，每半年至少對本公司、子公司的財務、風險管理及法令遵循辦理一次專案業務查核，主要工作項目如下：

  (1) 建立風險導向稽核，依據金控及各子公司的風險訂定稽核計劃並辦理查核

  (2) 督導各單位落實自行查核制度執行。

  (3) 持續追蹤覆查內、外部檢查意見及缺失改善情形。

  (4) 定期向董事會及審計委員會報告稽核業務執行情形及座談。

  (5) 建立內部稽核、法令遵循與風險管理雙向溝通機制，就相關法遵與風管弱點進行討論。

中信銀持續推動內部控制制度三道防線文化，由第一道防線 (自行查核)、第二道防線 (法令遵循與風險管理) 與第三道防線 (內部稽核單位)，共同確保內部控制制度之設計及運作有效執行，強化對風險管理、法令遵循、內部控制文化之意識與遵循，俾確保客戶權益，減少對企業商譽之負面影響。

[25] http://www.ctbcholding.com/care_05_6.html (access date: 2016/6/6)

附錄 A7：補充資料－後續相關事件或改變

本附錄補充與本個案可能相關之後續發生的事件或改變，提供給學員參考：

1. 中信銀於 2014 正式設置企業資訊安全委員會與監控中心[26]：中信銀於 2014 年正式成立企業資訊安全委員會，由總經理及各事業處執行長等高階主管擔任委員，負責企業資安議題審議、重要決策裁示、資安預算的審查等。由上而下的執行方式有利於資安政策與事務的推動。公司並辦理個資保護及資安保護教育訓練以及建立資安事件監控與應變中心 SOC (Security Of Center)。在資安控管認證及改善機制方面，則設立品質監控改善機制、致力中信銀通過 BS 10012 PIMS (Personal Information Management System) 個人資訊管理認證、以及強化資料外洩防治網。

2. 中信銀前資訊長張汝恬轉戰數位電子銀行－王道銀行[27]：2015 年，台灣工銀董事長請來有台灣「信用卡教父」之稱的羅聯福，規畫王道商銀藍圖。他當年一手打造出中信銀的信用卡龍頭市場地位，當年跟隨他的子弟兵，包括張儉生、張汝恬及張智銓等，此次都隨他轉戰「王道銀行」。台灣工銀最高顧問羅聯福說，王道銀行將以數位電子銀行業務為主，別的銀行為轉型 Bank3.0「因為包袱多」，就像打「七傷拳」一樣，每每出拳、都會內傷，但王道銀行沒有包袱，每揮一拳，拳拳都到肉。

[26] http://www.chinatrustgroup.com.tw/2014CSR.pdf (access date: 2016/4/12)
[27] http://udn.com/news/story/7239/1225428-駱錦明拚工銀轉型-不打七傷拳 (access date: 2016/4/23)