行政院及所屬各機關出國報告

（出國類別：研究）

信用卡防偽機制之研究

服務機關：臺灣土地銀行資訊室
出國人 職　　稱：副科長
姓　　名：蔡秋惠

出國地區：新加坡、香港

出國期間：91年12月11日至91年12月24日

報告日期：92年3月23日

系統識別號:C09105892

公 務 出 國 報 告 提 要

頁數: 35　含附件: 否

報告名稱:

信用卡防偽機制之研究

主辦機關:

臺灣土地銀行

聯絡人／電話:

陳元雙／02-23483170

出國人員:

蔡秋惠　臺灣土地銀行　資訊室　副科長

出國類別: 研究

出國地區: 香港　新加坡

出國期間: 民國 91 年 12 月 11 日 -民國 91 年 12 月 24 日

報告日期: 民國 92 年 03 月 23 日

分類號/目: D3／銀行　D3／銀行

關鍵詞:　信用卡防偽機制之研究

內容摘要: 本次奉派赴新加坡、香港研習「信用卡防偽機制之研究」，主要目的在瞭解國外信用卡風險管理及防偽機制之建置技術、實際應用方向，以及瞭解晶片信用卡發展趨勢及相關技術，蒐集相關資料，以作爲本行強化信用卡防偽機制之應用，提昇本行信用卡服務品質，並期能俾利本行信用卡晶片化轉置作業之參酌。

本文電子檔已上傳至出國報告資訊網

摘　　要

目　　的：赴新加坡、香港研習「信用卡防偽機制之研究」

內容重點：本次奉派赴新加坡、香港研習「信用卡防偽機制之研究」，主要目的在瞭解國外信用卡風險管理及防偽機制之建置技術、實際應用方向，以及瞭解晶片信用卡發展趨勢及相關技術，蒐集相關資料，以作為本行強化信用卡防偽機制之應用，提昇本行信用卡服務品質，並期能俾利本行信用卡晶片化轉置作業之參酌。

目　　錄

壹、研究目的 …… 1

貳、考察內容 …… 2

叁、研習心得 …… 9

一、信用卡不法使用型態 …… 9

二、信用卡防偽機制 …… 13

三、晶片信用卡作業 …… 24

肆、建議事項 …… 29

一、信用卡防偽機制建議 …… 29

二、晶片信用卡建置作業機制建議 …… 31

參考文獻 …… 35

壹、研究目的

依據行政院主計處九十一年十一月十二日發表的國情統計通報，九十一年八月底信用卡發卡數5,117萬張，較九十年同月底增32.8%，流通卡數2,877萬張，年增率34.6%。一至八月信用卡簽帳金額5,739億元，較九十年同期增11.0%；信用卡預借現金金額785億元，年增率18.5%。信用卡使用在台灣社會中已經越來越普遍。

然而，另一方面，根據聯合信用卡中心、財金公司與外商銀行等國內三個主要的信用卡會員中心統計國內信用卡詐欺損失金額，八十六年各發卡銀行的損失總金額僅有新台幣二億二千多萬元，八十七年達到三億七千多萬元，八十八年倍數成長到六億九千多萬元，八十九年信用卡犯罪盜刷金額竟一舉突破新台幣二十億元，九十年更創歷史新高，直逼30億元大關。此數據顯示，信用卡的盜刷偽冒情形越來越嚴重，消費者享受信用卡消費便利的同時，亦面臨有被盜錄或盜刷的風險，而對銀行業者來說詐欺盜刷金額逐漸增高，亦造成銀行呆帳的負擔。

如今電子商務的活動漸趨頻繁，越來越多的交易行為透過信用卡來進行。為提供持卡人更安全的信用卡支付工具及支付環境，並減少詐欺偽卡損失，信用卡業者無不積極著手於詐欺防偽功能之提昇。本次奉派至新加坡及香港研習信用卡防偽機制，主要目的在瞭解國外信用卡風險管理及防偽機制之建置技術、實際應用方向，以及瞭解晶片信用卡發展趨勢及相關技術，蒐集相關資料，以作為本行強化信用卡防偽機制之應用，提昇本行信用卡服務品質，並期能俾利本行信用卡晶片化轉置作業之參酌。

貳、考察內容

為瞭解信用卡防偽機制及晶片卡之應用現況，經呈核准，奉派赴新加坡及香港研習。

一、至斯倫貝謝神碼（SchlumbergerSema）公司研習

斯倫貝謝有限公司是一家全球性的資訊技術服務公司，該公司業務項目爲電信、能源和公用事業、金融機構、交通、以及公共領域市場提供諮詢、系統集成、管理服務和產品，該公司在65個國家有3萬多名員工，總部設於紐約。該公司在金融方面的服務包括：智慧卡系統（包括支付卡和電子商務解決方案）、客戶交互工具（包括POS終端，以及客戶關係管理和資料庫系統）、用於網路管理和財務應用的交易系統、付款後臺辦公系統、交易和核心系統。此次參訪研習其SemaCard系統之詐欺偵測模組。

SemaCard系統因日益增加的詐欺偽卡交易發生，發卡行因此遭受之損失日益提升，以及詐欺偽卡交易行為之千變萬化，為減少銀行損失因應開發信用卡詐欺偵測模組。

■信用卡詐欺風險因素

－高風險國家：如泰國

－高風險業別：如 Mail/Telephone order、E-commerce

－交易金額：如 Higher amount; more risk

－不正常交易金額：如 Exceed average spending amount

－重複交易：詐欺商店、Hack issuer system in a very short period

－國外交易：偽卡在國外刷卡交易

■**信用卡詐欺偵測模組提供**

－參數設定方式（Parameter driven）

－依風險因素訂定風險指數高低（Define scoring points by risk factor）

－依需要訂定風險指數公式（Define scoring formula）

－依每日累計風險限額作即時檢核（Velocity check on accumulated daily risk limit）

－風險指數參數調整（Scoring parameter tuning）

－多元化之風險指數模組（multiple scoring model profiles）

■**交易風險指數設定**

－國家別（Country）：可依不國家群組設定風險指數

--低風險指數國家群組：如歐洲

--中風險指數國家群組：如香港

--高風險指數國家群組：如泰國

－特店行業別（Merchant industry）：可訂定高風險特店行業群組給予高風險指數

--低風險特店行業群組：如飯店、餐廳、便利零售店

--高風險特店行業群組：如郵購、e-commerce

－交易金額（Transaction amount）：可依交易金額層級訂定風險指數

--低風險交易金額層級：如 0～5,000

--中風險交易金額層級：如 5,000 以上～20,000

--高風險交易金額層級：如 20,000 以上

－交易金額差異數（Transaction amount variance）：可依高風險指數訂定較高差異數層級，差異數可依據最後幾次交易金額的平均數而訂

--低風險差異數層級：如 100%～300%

--中風險差異數層級：如 300%以上～600%

--高風險差異數層級：如 600%以上

－交易時間差異（Transaction time difference）：最後兩筆連續交易的時間差

--低風險時間差：如＞60 分鐘

--中風險時間差：如＞30 分鐘＆＜＝60 分鐘

--高風險時間差：如＜30 分鐘

－國外交易（Foreign transaction）：訂定兩地旅遊時間差，根據經緯度算出兩地距離及時間，研判交易合理性

--低風險交易時間差：如到達後＞2 小時

--高風險交易時間差：如到達前 1 小時

二、至斯倫貝謝神碼（SchlumbergerSema）公司晶片卡製卡廠研習

斯倫貝謝神碼在晶片卡行業已有20多年，至今該公司已銷售晶片卡20多億張，由於晶片卡已被視為信用卡防偽機制之最佳利器，因此行程中參訪該公司在香港的亞洲晶片卡製卡廠，瞭解晶

片卡應用範圍、晶片卡產製流程、晶片類別、安全品管等相關資訊。

■晶片卡應用範圍

晶片卡發展至今，已具有憑證、運算、記憶、安控、處理、決策等諸項基本能力，是故其可延伸的範圍至為廣泛，而且晶片卡應用範圍仍在不斷的延伸成長中，善用的持卡人亦與日俱增。目前晶片卡應用範圍如下：

－信用卡及轉帳卡：用於訂位、消費。

－儲值卡或電子錢包：用於停車、公車、捷運、電影票、電話、報紙。

－個人身分識別：用於身分證、福利證、駕照。

－個人資料檔案：用於病歷、戶政。

－電子 Key：用於個人用電腦、Set-Top-Box、家庭銀行。

－網際商務：用於行銷，Content。

－數位憑證（電子簽章）：金融，身分認證。

－忠誠度計劃（Loyalty Program）。

－其他，如汽車、政府、軍事等。

■晶片卡產製流程

晶片卡是由矽晶片與塑膠卡片所組成，當矽晶圓產製後，經過切割後成為矽晶片，加入晶片專屬的 OS 作業系統，賦予其基本的邏輯運算與記憶等功能。在加入作業系統後，矽晶片還須經微模組（Micro Module）的製程，才能與塑膠卡片結合，通

常這個過程稱為晶片著床（Embedding），之後會交由晶片卡的製卡廠商（Card Fabricator），進行訂貨機構指定的相關作業程式（Application）處理，才能交由發卡機構進行個人化（Personalization），一張晶片卡才算大功告成。晶片卡的產製作業：

－晶圓廠生產出晶圓，切割成矽晶片

－晶片加入專屬作業系統（OS）

－矽晶片須經微模組處理（Micro Module）

－晶片與塑膠卡片結合，稱為植晶（Embedding）

－進行指定的相關作業程式（Application）處理

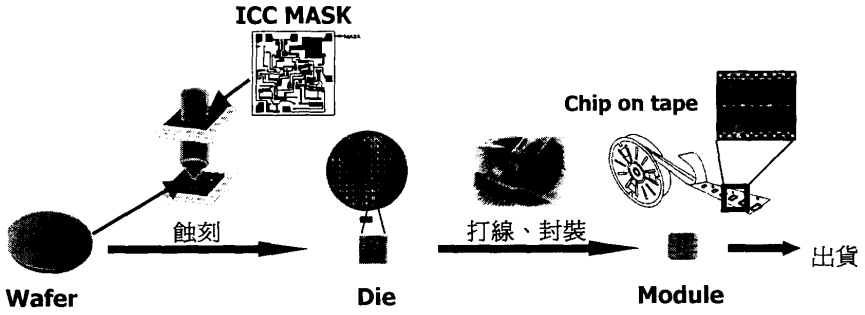
－交由發卡機構進行個人化（Personalization）

－完成之晶片卡交給持卡者使用

產製流程詳如下圖：

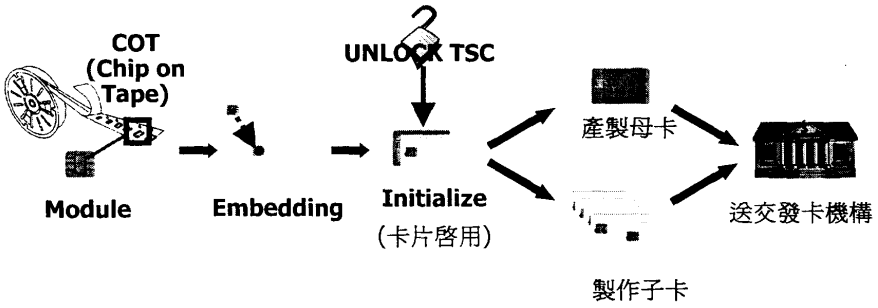
❖ 晶圓（晶片）製造商

- 接受Card OS公司委託生產晶片
- 出售晶片予授權之卡片廠商



❖ 卡片廠商

- 取得Card OS公司授權
- 向晶圓廠購買晶片（Module）並植入塑膠卡片
- 對卡片進行初始化
- 製作子卡及母卡送交發卡機構



■**晶片卡類別**

晶片卡可分為記憶卡（Memory Card）與智慧卡（CPU Card），記憶卡只能儲存資料，CPU 卡則有邏輯演算等處理能力。此外，晶片卡可依進出卡片之資料或指令流通的管道分為：「接觸式晶片卡」（Contact Card）及「非接觸式晶片卡」（Contactless Card）。接觸式晶片卡是以接觸到晶片表面的金屬面（或稱晶片腳位）作為下達指令及傳送資料的方式進行，非接觸式晶片卡是以非接觸式的金屬線圈感應的方式進行指令下達及資料傳送的動作。最新晶片卡設計已將兩種作業方式組合在一起，使一個晶片可以同時使用「接觸式」及「非接觸式」的方式指令下達及資料傳送的動作，此種晶片卡稱為「Combi Card」（為 Combination Card 之簡寫）。Combi Card 之應用將可符合各式各樣的業界需求，如捷運票證及金融支付的整合應用，而成為最重要的晶片卡之一。此外晶片卡之共容性（ISO7816、VOP、MULTOS、JAVA、FISCPlus）、記憶體大小（ROM & EEPROM Size（16K、32K、64K））及應用程式開發彈性（C、JAVA、VB）等均與晶片卡功能息息相關。

叁、研習心得

一、信用卡不法使用型態

國內信用卡犯罪於八十七年開始走向集團性犯罪，由原先和不肖商家勾結，以假消費方式使用偽卡刷卡，八十八年間開始發展出在刷卡終端機旁裝設一台側錄機，勾結店員側錄客人信用卡，然後交由偽卡集團製卡；甚至有偽卡集團吸收信用卡相關作業人員盜賣客戶信用卡資料，或整批轉到國外製作偽卡。在科技日新月異下，如今側錄的技術，更是由過去如香煙盒一樣大小、容易被察覺的「側錄機」，發展到目前的側錄晶片。側錄晶片直接裝在刷卡終端機裏，刷卡終端機外觀並無異樣，只要有刷卡的動作就會"全都錄"，持卡人就算刷卡不離開視線，也無法防範信用卡不被側錄，偽卡風險亦隨之提高。

據統計在亞太地區，台灣為信用卡詐欺犯罪率最高國家之一，在聯合信用卡中心會員銀行九十年之詐欺損失型態分析中，偽卡占80.71%、遺失卡占7.21%、被竊卡占5.46%、申請但未收到卡占1.62%，冒用申請卡則占1.01%。而從信用卡國際組織之統計數字亦顯示，在全球信用卡各種盜用損失比率中，亦以盜用及冒用之情形最為嚴重，約占所有信用卡詐欺損失額百分之五十以上。茲將信用卡不法使用型態概略敘述如下：

(一)盜用信用卡

偷竊他人信用卡或因持卡人遺失卡片遭他人拾獲並持之消費刷卡冒用。

(二)盜用信用卡卡號

不肖業者刷卡時記取他人信用卡卡號、撿拾持卡人刷卡消費後隨意丟棄之各種印有持卡人簽名及卡號之簽帳單等，由於郵購、電購、網路購物這三種交易並不需持卡人持用卡片刷卡，只要報卡號及有效日期即可取得授權碼完成交易，故較容易遭冒用。部分發卡單位已陸續發現，國外犯罪集團有盜用國內信用卡卡號，並於國外刷卡冒用之情事。

(三)冒用信用卡

在發卡單位郵寄信用卡的過程，可能發生在遞送途中遺失、被竊，或代收信件等方式取得他人信用卡，抑或是在掌握持卡人的姓名、出生年月日、卡號以及帳單地址等資料後，向發卡行辦理「掛失手續」重新發卡等，進而簽名開卡冒用。由於上列遺失、被竊等信用卡上之簽名已為非法冒用者之簽名，故冒用者在刷卡交易過程中，並不易為商店所發覺。

(四)偽造信用卡

所謂偽造信用卡乃指以不當途徑取得信用卡持卡人資料，利用電腦、錄碼機、打凸字機、燙印機等加工所製作出之卡片（偽造信用卡外觀上具有一般信用卡的美麗外表），再持偽造卡至正常商店詐購商品，或與商店勾結共謀詐財。

其不當途徑，例如由製造偽卡者與不肖業者勾結，以側錄器或非法安裝於刷卡終端機上之側錄晶片，盜錄取得持卡

人信用卡之磁條內碼資料、向發卡行或信用卡資料處理公司之不肖職員購買持卡人資料、抑或透過電腦網路入侵發卡行之電腦系統擷取信用卡資料紀錄等相關之資料檔案，將取得的內碼交給偽卡犯罪集團，或者偽卡集團從境外帶回偽卡成品或半成品偽造信用卡盜刷使用。最近警方調查發現有不法者專門在各醫院、商場附近擺設攤位，自稱為銀行的信用卡部門專員，以「舊卡換新卡可兌換高級紀念品」進行詐騙。以騙發新卡盜錄資料，因此有部分持卡者上當，將信用卡交予辦理換發新卡手續，集團成員趁機利用機器取得舊的信用卡磁條內碼，再將內碼轉製成偽卡。此類犯罪特性常有集團性犯罪組織成員參與其中，所造成的經濟損失也最為嚴重。

據相關單位表示，國內偽卡集團已經轉型成跨國性犯罪，目前最熱門的是將國內盜錄的信用卡資料帶出國，利用國際連線查核的時間差，在國外製作偽卡後盜刷，再變賣貨品轉成現款，外國發行的信用卡被盜錄偽造後，也由偽卡集團帶到國內刷卡。帶著偽卡周遊列國盜刷，成為新興犯罪手法。

(五)變造卡

將不當方法取得之信用卡（如偷竊或收購掛失、停用卡）上真卡號局部或全部壓平後，重新打上或貼上有效卡號、期限之偽卡後（即凸字偽造），持該變造卡至特約商店詐購商品。

(六)白卡

係指不法犯罪集團以勾結特約商店或特約商店店員，利用信用卡消費刷卡時直接以側錄機盜刷取得信用卡持卡人之資料，再憑該資料大量製作白卡（偽冒信用卡磁條內容，外觀上並無一般信用卡所具有的美麗外表），並與上述特約商店共謀大量刷製簽帳單，以便向銀行報帳取得刷卡金額；或者配合具有計劃性、組織性之偽卡製造集團成員直接以白卡盜刷。

(七)人頭戶信用卡

詐欺集團常利用人頭戶資料或偽造薪資證明、在職證明文件用以向多家發卡機構申請信用卡，並於刷卡後拒不付帳，或以按時繳款培養信用之方式，於獲得發卡機構之信任而提高信用額度後，再高額消費刷卡，將呆帳轉嫁於發卡機構。

(八)網路上信用卡詐欺

一般來說，網路上信用卡交易較可能會有的風險包括：一是交易時因為網站的加密不夠，導致傳輸過程中，個人資料被擷取；另一種則是不法集團藉由竊取個人資料，竊取持卡人信件，利用信用卡帳單上所提供的信息，如信用卡卡號、有效期限及身分證字號，就可以以持卡人的名義在線上進行信用卡交易。

隨著國際網絡的發達，電子商務日益普及，網路上信用

卡詐欺所產生的損失也跟著直線上升。透過網路不當蒐集消費者信用卡資料，國際間已有多起透過網路入侵網路商家資料庫，竊取消費者信用卡資料等案例的發生，今年二月美國發生大宗信用卡資料竊取案，有近八百萬張信用卡卡號遭駭客入侵取得，目前也成為國外網路犯罪調查單位偵防的主要目標。

二、信用卡防偽機制

由於不法組織利用信用卡犯罪手法，隨著電子、金融科技的高度發展，詐欺犯罪型態亦不斷翻新，使得各發卡機構信用卡詐欺損失仍逐日攀升，因此無論信用卡國際組織抑或國內各發卡機構均絞盡腦汁建立各項風險管理監控機制系統，以達防堵日益攀升的冒刷損失。而在各相關單位的共同努力之下，相關的防偽機制概分下列項目：

- CRIS-NS（Cardholders Risk Identification Service-National Solution）類神經中樞網路風險辨識服務系統
- PRISM（Proactive Fraud Risk Management）詐欺風險偵測系統
- 網路線上刷卡資料盜取防偽機制－SET、SSL 安全交易機制、VISA 3-D Secure
- 信用卡簡訊服務
- 對社會大眾及持卡人進行信用卡風險認知及個人資料保護之宣導
- 發卡行寄送信用卡相關之簽單、帳單、信函等不可列印完整的信用卡卡號

■指紋刷卡系統

■晶片信用卡

■政府修法透過重罰手段來遏阻信用卡偽卡犯罪

■銀行公會九十年「全國信用卡會議」研討加強信用卡風險管理並建立短、中、長期防制信用卡犯罪機制

茲將上列信用卡防偽機制概述如下：

(一)CRIS-NS（Cardholders Risk Identification Service-National Solution）類神經中樞網路風險辨識服務系統

由於過去風險管理單位，以傳統報表及人工方式逐筆/次查核有疑問的刷卡行為，再採取相關之調查/管制作業，較為耗時、費力，效果不彰顯。由 Visa 國際組織與聯合信用卡中心推出的持卡人風險辨識服務系統，透過 CRIS-NS 的類神經中樞網路系統，以評出盜刷風險指數，並藉由大量數據的歸納、分析與學習判斷出持卡人特定的行為模式與一般行為模式的差異性，即時偵測刷卡交易，一發現異常即能提出警訊、暫停交易、封鎖卡片授權，可有效抑止偽卡盜刷，提供持卡人安全的交易保障。

(二)PRISM（Proactive Fraud Risk Management）詐欺風險偵測系統

財金公司為降低所屬會員銀行之信用卡偽冒損失，特建置 PRISM 詐欺風險偵測系統供會員銀行使用，該系統可結合持卡人資料及授權資料作監控，透過規則化的參數設定，

以因應多樣新興之詐欺行為，即時偵測及防堵偽冒交易，提供詳盡報表，以精密的數字分析，供風險管理人員可隨時分析冒刷趨勢，掌握執行時效，並可透過及時通知的簡訊功能，通知持卡人消費刷卡狀況，達到即時偵測即時通知的功效。

(三)網路線上刷卡資料盜取防偽機制

1.SET、SSL安全交易機制

SET（Secure Electronic Transaction）安全交易機制，是一種網路安全保障方式來保障使用者在網際網路上進行交易時的安全性。具有SET規格的軟體，儲存在持卡人的個人電腦及特約商店的電腦網路中；此外，收單銀行的電腦也能夠解讀金融資訊密碼，以及確認認證單位所發出的電子證書。經由SET的數位簽名認證，商家可以確認消費者身分無誤。對消費者而言，有了SET，商家不會看見他們的卡號，卡號直接傳輸到發卡銀行進行轉帳，因此沒有被商家盜刷的危險。而SSL（Secure Socket Layer）可以在網際網路使用者的瀏覽器程式與購物網站伺服器之間建立起一個安全的溝通管道。台灣有越來越多的電子購物廠商也開始使用SET，並與SSL機制並行。

2.VISA 3-D Secure

為提供網路線上刷卡基本的安全機制及兼顧持卡人的方便度，VISA推出3-D Secure，並已獲JCB採用並即將與

MasterCard達成協議。

在e-commerce支付環境中，若持卡人惡意否認該交易，由於沒有實體簽單可供調單，特店往往得承受損失。3-D Secure即是一種驗證持卡人身份的過程。也就是說在整個網路交易的過程藉由身份的認證使得整個交易具有不可否認性。所謂3-D即3 Domain，包含發卡行Domain（Issuer Domain），Interoperability Domain以及收單行Domain（Acquirer Domain）。持卡人在Issuer Domain註冊，取得密碼及個人訊息之後，往後在任何網路特店消費時必需輸入密碼。收單行將相關訊息送往Interoperability Domain（即VISA），VISA在驗證完BIN之後再送給Issuer Domain確認密碼，確認無誤後即可進行授權交易。整個確認流程約多出6、7秒鐘。在作業效益安全性上消費者不可否認，商家風險降低，且商店無法得知持卡人卡號，確實保護持卡人權益。

(四)信用卡簡訊服務

為保障信用卡持卡人用卡安全，部分發卡機構針對海外刷卡交易、網路刷卡交易、大額刷卡交易、信用額度使用情況等提供信用卡簡訊服務，並配合偵測防偽系統，如經系統偵測為高風險可疑消費，會立即傳送不正常消費情形簡訊通知持卡人，讓持卡人隨時掌握刷卡情況，如有發現信用卡被盜刷，即可迅速與發卡行聯繫，保障刷卡交易的安全性。

(五)對社會大眾及持卡人進行信用卡風險認知及個人資料保護之宣導

除了上述各項信用卡單位建置之防偽機制外，發卡單位亦應加強信用卡功能與正確使用之宣導教育，使社會大眾及持卡人自己多加小心防範，並注意相關權利和緊急補救的方法，以減少損失。

1.申請信用卡不應隨便把資料交給非銀行專員或是民間代書委託代辦，應該直接找銀行信用卡專員辦理，以免資料遭到盜用。

2.申請信用卡時，記得註記採「親自領取」或「掛號郵寄」方式取得信用卡，郵寄收件地址以本人能親自收到者為宜，以防因他人代收盜用。

3.持卡人收到卡片後要立即簽名，並注意簽名字型不宜過於簡單和工整，以免容易遭人仿冒。

4.應仔細核對對帳單消費金額及明細是否有誤，發現不明費用項目應立即向發卡銀行查證。

5.信用卡及預借現金密碼須分開存放，以免卡片遺失而遭盜領現金。並隨身攜帶發卡銀行服務中心電話，以便緊急聯絡。

6.網路購物，針對商店不明或交易方式不安全，未取得「SET電子交易安全規格認證」之網站，不可隨意將信用卡卡號、卡片有效期限或個人資料公布在網路上，以避免

資料被盜用之虞。

7.遺失的身分證、路邊的街頭調查和抽獎活動，也有可能會使基本資料流落在不肖集團手上，針對個人資料保護，社會大眾及持卡人自己應多加小心防範。

(六)發卡行寄送信用卡相關之簽單、帳單、信函等不可列印完整的信用卡卡號

1.為確保持卡人資料安全，杜絕有可能在網路購物或郵購時盜用隱憂，發卡行於寄送相關信用卡帳單及信函時，應將信用卡卡號先行予以適當處理，不宜列印完整的信用卡卡號或持卡人身分證字號於信件上，以免持卡人資料被不法人士擷取而遭冒用。

2.目前信用卡刷卡購物時，國內部分商店發票上印有卡號與到期日。銀行公會已多次討論，未來信用卡簽單上都可望不列印完整的信用卡卡號，以保障客戶資料安全。

(七)指紋刷卡系統

為了打擊日漸嚴重的信用卡詐騙罪行，國外有使用「指紋擦卡系統」，要求以信用卡簽帳的顧客留下指紋。信用卡持卡人須把手指按在一個特製的無油墨指紋版上，然後再在信用卡單據印上指紋。透過指紋系統，警方可以將懷疑盜用信用卡人之指紋與指紋庫配對，找出騙徒身分，用以防堵信用卡犯罪。

(八)晶片信用卡

傳統上，信用卡以磁條作為支付工具，因容量限制且可儲存資料不多，先天上限制了信用卡功能，又隨著犯罪集團在技術與手法的不斷翻新，磁條信用卡的防偽機制已無法抵擋日益嚴重的偽卡盜刷情況，因此，能夠提供更嚴謹防偽機制的晶片信用卡即成為當前的迫切需要。茲將晶片卡功能概述如下：

■安全防偽功能：晶片卡在系統、軟體及硬體設計上，均各有專門的保密安全機制，具有安全防偽功能。

■個人化風險管理功能：晶片卡可以把龐大的個人資料存在晶片當中，因此可以做到個人化的風險管理，包括授權、信用額度與交易管控等，降低銀行的信用風險。

■離線授權功能：信用卡交易在不少國家遭受到的主要問題之一是連線授權的電信通訊成本，晶片卡有多數交易可交由晶片來做風險控管，可以離線方式進行授權交易，降低授權成本。

■業務需求：越來越多的零售通路、聯名團體主動提出發行晶片卡的需求，希望藉由晶片卡的儲存處理能力，進行忠誠顧客回饋、客戶管理等專案，晶片卡可配合不同的顧客忠誠計畫，將持卡者之消費直接計算紅利回饋並累計儲存於晶片中，也可隨時下載或更新所需的應用程式（動態存取），依其容量不同可放置數個所需要之程式，程式與程式間有防火

牆作為間隔，可避免程式間互相干擾造成晶片卡無法使用的狀況。

■**磁條信用卡與晶片信用卡之比較：**

磁條信用卡每次刷卡時，讀卡機就會讀取磁條內的信用卡卡號、卡號檢查碼、持卡人姓名、使用期限等資料，連同交易金額、交易時間與商店名稱等資料連線送至銀行系統取得授權，始完成交易。而在此過程中，犯罪集團即可趁機進行磁條側錄，再將資料轉錄至空白磁條卡，若配合精美印刷和其他信用卡特徵，即為一張以假亂真的信用卡。因此消費者、銀行與商店在不知情的情況下，已遭受信用卡被盜刷的風險及損失。

晶片信用卡，除包含傳統磁條卡的卡號、持卡人姓名、使用期限等資訊，在持卡人的身分辨識方面，晶片可以個人密碼（PIN）進行身分辨識，透過晶片卡進行加解密，可避免現行簽名所帶來偽造的缺點，此外還可提供晶片信用卡專有的離線及網上使用控制、確認有效卡片、離線密碼認證及修改卡片資料等功能。除了提供網上交易、訊息傳遞的安全性保障之外，持卡人也可以隨時透過個人電腦，自發卡銀行的網站上下載最新增加的服務項目，而不用為了新的服務前往發卡銀行申請換發一張新的卡片。晶片信用卡就類似一個小型電腦，如果有外力破壞晶片卡，也無法像盜錄磁條卡一樣，那麼容易取得持卡人所有的資料。

表一、磁條信用卡與晶片信用卡之差異比較

項　　目	晶片信用卡	磁條信用卡
儲存容量	大（3K 以上）	小（不足 1K）
防偽安全性	佳	不佳
行銷資訊存放	可	不可
放置應用程式	可	不可
卡片成本	高	低

晶片卡的轉換有助於銀行快速減少在偽卡方面的損失，更可因運用多功能的晶片卡，在行動商務與電子商務中，為消費者帶來更多的便利性，為銀行製造更多的商機。

根據 VISA 國際組織亞太區委員會會議中決議，在二〇〇八年年底完成亞太區的晶片卡建置工程，並規定：從二〇〇三年一月起，所有收單銀行新購的刷卡終端機需符合 EMV 國際晶片標準規格；並將獎勵亞太區已從事晶片卡交易的發卡及收單銀行。現行採用晶片卡技術的 VISA 信用/轉帳計劃，也須在二〇〇四年一月前與 EMV 規格相容；所有現行 VISA 發卡機構的刷卡終端機均需符合 EMV 國際晶片標準規格。而自二〇〇六年一月起，結合磁條及晶片的晶片卡若在非晶片卡終端機交易，磁條被盜錄而產生偽卡盜刷，將由收單銀行自行負擔損失，以促進收單銀行願儘速將終端機更新為晶片卡規格。目前，財政部、銀行公會正研議相關晶片卡升級計畫，以貫徹杜絕偽卡決心。

(九)政府修法透過重罰手段來遏阻信用卡偽卡犯罪

在信用卡犯罪步步高昇的情形下，有人覺得這與對付偽造信用卡的刑罰過輕有關係，以往偽卡詐騙案只能依刑度較輕的偽造文書罪送辦。因此立法院在九十年六月三讀修法通過，在刑法分則的第十三章偽造有價證券罪章中，增列第二百零一條之一的條文，明定：「意圖供行使之用，而偽造信用卡、金融卡、儲值卡或者其他相類作為簽帳、提款、轉帳或支付工具之電磁紀錄物者，處一年以上七年以下有期徒刑，得併科三萬元以下罰金。行使前項電磁紀錄物者，或意圖供行使之用而收受或交付於人者，處五年以下有期徒刑，得併科三萬元以下罰金。」在政府修法透過重罰手段來遏阻信用卡偽卡犯罪日漸增加的情形後，根據刑事警察局就查獲的信用卡詐騙案件的金額來看，由八十九年最嚴重的新台幣十一億多元，降到九十一年僅二億多元，似乎有降低趨勢。

(十)銀行公會九十年「全國信用卡會議」研討加強信用卡風險管理並建立短、中、長期防制信用卡犯罪機制

1.加強信用卡風險管理

- 銀行公會應訂定發卡及收單機構之內部安檢稽核作業範本供會員機構遵循，以徹底落實相關稽核工作，並避免持卡人個人資料或特約商店之信用卡交易資料外洩。
- 收單機構應訂定對特約商店之徵信及管理作業準則，以落實對特約商店之管理，並應加強對特約商店辨識偽卡

之教育工作。

■對信用卡磁條資料側錄點、疑似地下融資特約商店及不當利用客戶資料之離職員工等應建立完整、即時之同業通報系統，並訂定通報程序，由業者即時通報聯合信用卡處理中心後，再由聯合信用卡處理中心主動即時通報業者及金融聯合徵信中心，並由金融聯合徵信中心建立完整資料檔。

2.建立短、中、長期防制信用卡犯罪機制

■**短期方面：**

--應加強或研發發卡或收單銀行內部偵測信用卡盜刷之防偽系統，如引進先進之類神經人工智慧詐欺偵測系統，另成立詐欺防制中心（可發揮資訊情報蒐集、異常訊息或報表分析等功能），並搭配報案專線之建立以有效防制信用卡犯罪。

--為建立業者與檢警調單位之協調機制，信用卡業者應統合力量成立專責單位，負責與偵查機關之溝通連繫工作，未來可由公會擔任以具代表性。

--業者應儘量提供完整之偽卡案件資料，協助檢警調機關偵辦信用卡犯罪案件。

■**中期方面：**

--應由公會針對已三讀通過之刑法修正案評估其實行成效，以作為未來檢討信用卡犯罪問題之方向。

■**長期方面：**

--應由信用卡國際組織應用先進科技，更新、研發信用卡之防偽技術，如晶片卡之替換或磁紋辨識系統之推行等，以防堵信用卡詐欺犯罪。

三、晶片信用卡作業

為防堵日趨嚴重的信用卡詐欺行為，國際組織因此訂定了信用卡晶片化作業，將信用卡由磁條規格作業轉換成晶片規格作業，除了訂定轉換規格外，為了確保卡片、刷卡終端機以及發卡行、收單行的後台系統均要能接受並處理全球的卡片及刷卡終端機所傳送的信用卡刷卡交易，因此國際組織針對晶片卡、刷卡終端機以及發卡行、收單行的後台系統均訂定了相關的作業規範。

(一)晶片卡作業

1.EMV規格晶片卡

在ISO7816標準中，明確規定晶片卡之硬體架構及電氣訊號，對晶片所在位置、晶片功能等作了定義；由於只對硬體定出規格，隨著不同應用的出現，後來又衍生出在通訊產業（例如SIM卡）與支付機制兩部分的應用。在支付機制金融交易應用方面，Europay、MasterCard、Visa三家國際組織共同制定出EMV規格，以作為晶片信用卡的國際共通標準。在EMV規格中定義了辨認卡片真偽的方式、辨認持卡人真偽的方式、交易的流程、交易時必須檢查的參數與風險管理的方法等，訂定共用的標準即可達到業界

互通、使用者便利等目的，以及確保卡片能在全球互通使用。所以，必須合乎這些標準的晶片信用卡才能稱之為EMV晶片信用卡。

2.EMV晶片卡作業平台

晶片卡內若沒有作業程式，則晶片卡所有的功能都將無法發揮效用，而要在晶片卡上加裝作業程式，就必須先有作業平台(Operation System)，所有的功能程式才能往上添加。

從實體、作業平台與應用程式三個角度來看，就實體面來說，一般是規範晶片的相關硬體標準規格，因此晶片信用卡須符合ISO7816的標準。在作業平台上，兩大國際組織之作業平台為：萬事達卡國際組織制定了「MULTOS作業平台」，從OS到API（Application Interface）都有明確的定義，MULTOS目前支援C、MEL、VB與JAVA等程式開發語言；Visa國際組織依據EMV的基本規格制定以JavaCard為基礎的「VISA開放式平台」（VOP：VISA Open Platform）作為會員銀行發展晶片卡應用程式的作業平台。而針對應用程式的共容性，晶片信用卡與晶片轉帳卡須符合EMV國際標準的規格，萬事達卡國際組織開發的EMV標準PAYMENT的規格稱為M/Chip，意即未來在晶片卡上進行MasterCard/Cirrus/Maestro的交易，都必須符合M/Chip規格。VISA國際組織也協助晶片卡廠商開發完成

VSDC（VISA Smart Debit and Credit）晶片信用卡與晶片轉帳卡的應用程式。並且也將儲值卡（VISACash）功能建置在晶片的唯讀記憶體（ROM：Read-Only-Memory）中，使其成為晶片卡的標準應用程式之一。

晶片卡和電腦一樣，有所謂的ROM記憶體（ROM：存放晶片卡作業系統），而一般所稱16K、32K則指的是EEPROM存放密鑰、口令、計數器（通常是金額的計數）和被保護的安全單元與資料）的容量（EEPROM：Electronically Erasable Programmable Read-Only Memory），容量越大，可以存入的程式越多。

3.由於VISA及MasterCard國際組織均各自訂定EMV應用程式規格，因此製卡廠商開發EMV晶片卡，須分別取得VISA及MasterCard國際組織測試認證的合格證明，以確保此卡能符合在任何已通過EMV level 2合法認證之刷卡終端機刷卡交易，達全球通用之功能。

(二)刷卡終端機作業

1.EMV刷卡終端機規格

- EMV level 1：此乃針對終端機之相關硬體規格如電器（Electrical）、機械（Mechanical）、傳輸定義（Protocol）以及回應重置（Answer to reset）等部分訂定規格標準。
- EMV level 2：此乃為開發EMV信用/轉帳功能及應用程

式之需，針對應用程式之重點核心部分（kernel），如軟體模組（software module）、中心主軸（core）、程式館（library）等訂定規格標準。

2. 為確認刷卡終端機符合國際組織訂定之EMV level 1及level 2標準，終端機廠商開發終端機，須取得國際組織EMVCo測試認證的合格證明，以確保刷卡終端機能接受全球EMV晶片卡的刷卡交易，而達全球通用之功能。

(三)發卡行作業

萬事達卡國際組織為確認發卡行主機系統在處理國際組織傳送之晶片信用卡交易是否符合相關作業程序，因此亦訂定二階段之發卡行認證作業（Issuer Validation）：

- ICC Testing using simulators
- ICC Testing using the MTF

由於本行參加財金公司之信用卡清算系統，並不與國際組織直接連線，因此此項作業不須執行。

(四)收單行作業

萬事達卡國際組織為確認收單行主機系統在處理國際組織傳送之晶片信用卡交易是否符合相關作業程序，並確保此晶片卡及刷卡終端機之全球功能性，因此訂定三階段之收單行認證作業（Acquirer Validation）：

- ICC Network Interface Validation Using Chip Simulator
- Terminal Integration Process（TIP）

- ICC Network Interface Validation Using Member Test Facility（MTF）

由於本行參加財金公司之信用卡清算系統，並不與國際組織直接連線，因此不須執行第一及第三階段作業。而第二階段作業認證仍須執行，其作業目的如下：

- 測試收單行刷卡終端機是否能接受所有 MasterCard 晶片卡。（Perform all tests related to acceptance of MC brands on Chip）
- 加強 EMVCo Level 2 功能測試。（Highlight EMVCo Level 2 Kernel regression tests）
- 測試刷卡終端機與收單行主機系統之交易傳輸作業是否正確執行。（Test the correct implementation of the protocol between the terminal and the acquirer host system）

肆、建議事項

一、信用卡防偽機制建議

為有效監控信用卡異常交易，本行目前已使用VISA國際組織之「VISA CRIS」及聯合信用卡處理中心之「CRIS-NS」等之信用卡偵測系統，前者乃監控經由VISA國際組織授權系統之交易，後者則監控聯合信用卡處理中心所屬特約商店之交易，然此二系統無法監控本行之所有信用卡交易。目前財金公司正建置「PRISM」詐欺風險偵測系統，本行正規劃參與，此系統可監控本行之所有信用卡交易，並結合持卡人資料及授權資料作監控，且可視需要以參數設定方式因應多樣化之詐欺型態，可有效遏止詐欺交易之發生。

本行除使用上述詐欺偵測系統外，在信用卡風險管理政策上可以評估強化下列防制措施：

(一)偽冒申請之防制

近幾年各銀行均極力開發消費金融領域，很多銀行只是一味要求行員發卡業務量之擴展，以致造成申請審核不嚴謹，詐欺集團趁機偽冒申請，詐欺風險因而提高。由於詐欺集團常利用人頭戶資料或偽造薪資證明、在職證明文件請領信用卡，再憑以詐欺刷卡，造成銀行嚴重損失。有鑑於此，本行在推展信用卡發卡業務量之同時，針對偽冒申請之防制應特別注意。本行行員在受理信用卡申請時，針對客戶所提供之資料審核應嚴謹慎重，除應查明確認真偽外，向聯合徵

信中心信用資料庫查詢申請人個人信用紀錄更應落實，以降低偽冒申請之風險。

(二)可以重新檢討信用卡刷卡終端機維護作業，強化維護作業安全機制

在信用卡詐欺偽冒行為中，偽卡集團常利用電子側錄機方式盜錄刷卡資料、複製偽卡，或假冒刷卡終端機廠商藉維修測試刷卡終端機時植入晶片、竊取資料、製造偽卡等方式作業。為防止不肖份子假借本行刷卡終端機維護廠商之名，藉機植入晶片盜取信用卡資料，本行針對信用卡刷卡終端機之維修作業可以重新檢討，強化維護作業安全機制，以降低刷卡終端機被側錄之風險。

(三)提供簡訊通知服務

提供簡訊通知服務，當信用卡刷卡交易發生後，即時傳送簡訊給持卡人。讓持卡人立即核對刷卡交易，一旦有偽卡盜刷，可立即察覺，並可迅速與發卡行聯繫，對持卡人是一種保障，對發卡行而言，藉由持卡人的及早發現，也能減少銀行的損失。目前財金公司建置之 PRISM 詐欺風險偵測系統提供即時通知簡訊服務功能，本行可評估透過該系統將監控交易訊息即時傳送持卡人，讓持卡人隨時掌握刷卡情況，保障刷卡交易的安全性。本行亦可評估是否自行建置簡訊通知服務系統，提供本行客戶更優良之即時服務。

二、晶片信用卡建置作業機制建議

(一)可以配合銀行公會訂定之補貼方案，積極進行晶片信用卡轉置作業，以提昇信用卡業務服務品質

晶片卡已被視為信用卡防偽機制之最佳利器，晶片卡的轉換能快速減少銀行在偽卡方面的損失，銀行公會有鑑於晶片信用卡轉換之必要性及全面性，委請財團法人聯合信用卡處理中心自九十二年一月一日開始調整 IRF 費率，啟動補貼方案如下：

- 於四年內發卡行提供新台幣 13.3 億元，作為磁條信用卡刷卡終端機轉換成晶片信用卡刷卡終端機之補貼。
- 補貼期間為期四年，自九十二年一月一日開始，至九十五年十二月三十一日截止；調降比率為萬分之四．四二，由現行發卡回佣費率（IRF）為百分之一．五五，調降至百分之一．五〇五八。

而國際組織亦訂定轉置作業詐欺債務移轉方案：

- 自二〇〇六年一月起，結合磁條及晶片的信用卡若在非晶片卡刷卡終端機交易，磁條被盜錄而產生偽卡盜刷，將由收單行自行負擔損失，以促進收單行願儘速將刷卡終端機更新為晶片卡規格。

由於本行佈建之刷卡終端機台數已逾兩千五百台，在銀行公會訂定之補貼方案配合下，本行宜把握機會，積極進行晶片信用卡轉置作業，提昇本行信用卡業務服務品質。

(二)培訓相關作業人員晶片信用卡專業知識

晶片信用卡的轉換作業除了晶片卡、刷卡終端機、收單行、發卡行後台系統以及軟硬體製卡設備等的配合外，消費者、商店、收單行及發卡行相關人員對流程熟悉、風險管理等教育訓練的配合也相當重要。本行應積極參與相關單位舉辦的教育訓練，對 EMV 晶片作業知識作深入瞭解，培訓相關作業人員，加強專業知識，瞭解相關的業務特性、作業方式、市場經驗，建立良好的業務觀念，以助於晶片信用卡之轉換作業、業務訂定及推展。

(三)明確訂定本行晶片信用卡業務策略方針及目標，訂定資訊作業配合事項及作業時程

由於晶片卡具有 CPU、儲存容量大及後發卡(post issuance)功能，可加入不同的應用程式，如進行轉帳、會員卡管理、紅利積點及客戶忠誠方案等更多元化的應用，因此晶片信用卡不僅可提升消費者使用信用卡的頻率，銀行與商店也能夠應用並創造多元化行銷及商機。本行宜妥善規劃晶片卡作業之業務策略方針及目標，把握市場商機。對於未來業務推展及規劃之方向，宜針對消費市場應用定位、卡片功能策略、企業合作策略等，進行資訊蒐集及消費行為分析，並針對不同產業特性、企業需求，尋求合作對象、拓展應用通路，訂定有效之行銷策略，以符合業務需求及市場推廣效益。有了完整的業務策略方針及目標，據以擬定資訊作業配

合事項及作業時程，俾便整體業務之推展。

(四)提供本行客戶全方位服務

在各國際組織全面推動晶片信用卡的同時，本行可以評估，如能將晶片金融卡及晶片信用卡結合發行，並集多方位服務應用功能於一卡，將客戶服務從「金融支付功能」延伸到「生活服務功能」，舉凡身分認證、醫療保健、電信、門禁差勤管理、忠誠計畫，乃至於交通票證等生活所需之食衣住行育樂，提供客戶全方位的服務，可強化銀行的市場競爭力。

(五)刷卡終端機新增線上軟體即時派送功能，因應市場多元化之忠誠行銷客戶關係管理服務，提昇本行作業執行效率及節省換版作業成本

晶片卡行銷的重要功能之一是客戶關係管理，利用晶片卡「立即累積、立即回饋」（Instant Accumulation，Instant Redemption）的客戶忠誠回饋方案（Loyalty Program）可以掌握客戶與該產品或服務提供者的往來狀況，進而運用這些動態資料提昇對客戶的服務品質，加強往來關係並刺激往來頻率，晶片卡中並可記錄客戶的個人偏好，以達到更貼心的一對一專業行銷。由於晶片卡的客戶關係管理是未來行銷的重要工具，且企業或商店常須依市場競爭狀況、業務方針等訂定產品行銷策略，機動調整忠誠回饋方案，刷卡終端機須能隨時因應配合此調整方案，讓持卡客戶能享有最新立即之

回饋服務功能，因此刷卡機之換版作業如再以人工作業方式執行，將耗時費力不符時效，評估新增線上軟體即時派送功能，因應市場多元化之忠誠行銷服務，提昇本行作業執行效率及節省換版作業成本。

參考文獻

1.中華民國銀行商業同業公會全國聯合會法規及函文決議 91/11/6 本會全信字第二五九〇號

http://www.ba.org.tw/word/Doc1.doc

2.財金資訊網－金融資訊生活－專題企劃－聰明世代智慧選舉

http://www.fisc.com.tw/information/maz

3.陳景旭，偽造信用卡集團及犯罪行為研究，行政院及所屬機關出國報告，民國九十年五月。

4.財政部金融局全球資訊網

http://www.boma.gov.tw/new/news/news900709.htm

5.行政院主計處國情統計通報

http://www.dgbasey.gov.tw/dgbas03/bs3/report/N911112.htm

6.萬事達卡國際組織新聞網

http://global.mastercard.com/tw/about/pressroom

7.VISA 國際組織新聞網

http://www.visa.com.tw/newsroom/tw_140801.shtml

8.財金資訊網－會員專區

https://www.fisc.com.tw/member/login1.asp

9.財團法人聯合信用卡中心新聞網

http://www.nccc.com.tw/yearbook/fraud2.htm