參、 網路 ATM 安控機制調查項目（無本項業務者免填）

一、 設備實體安全方面：

伺服器是否存放於具備門禁管理之機房？

是 □， 否 □。

二、 網路 ATM 相關設備方面：

（一）Server 廠牌及型號：

（二）Server 作業系統：

（三）網頁設計合作廠商（非委外免填）：

（四）提供最新網路 ATM Server 之安全評估報告或佐證資料（本項資料閱後即歸還）。

三、 交易安控機制方面：

（一）客戶端與伺服器間之交易是否加密？

是 □（所使用之加密機制請說明）：

否 □。

（二）代理行於交易過程中是否加入操作者回應事項（Challenge & Response）？

是 □（所運用之操作者回應方式請提供相關文件說明）

否 □。

（三）晶片金融卡交易不論是透過實體通路或網路通路，是否確實將通路資訊（即端末設備型態，例如 6011 為 CD/ATM、6514 為具硬體亂碼化安全等級之 PC/SC 讀卡機、6524 為具軟體亂碼化安全等級之 PC/SC 讀卡機、6534 為一般的 PC/SC 讀卡機）送至發卡行以核備？

是 □， 否 □。

(四)載具密碼是否未於網際網路上傳送？

是 □（請說明或提佐證資料）：_____

_____

_____

否 □。

(五)系統是否能辨識外部網站及其所傳送交易資料之訊息來源及交易資料正確性？

是 □（請說明或提佐證資料）：_____

_____

_____

否 □。

(六)系統是否能辨識客戶輸入與系統接收之非約轉交易指示一致性？

是 □（請說明或提佐證資料）：_____

_____

_____

否 □。

(七)針對常見網頁程式安全漏洞(如：Injection, Cross-Site Scripting) 是否採取因應措施？

是 □（請說明或提佐證資料）：_____

_____

_____

否 □。

(八)系統是否能偵測網頁與程式異動，並進行記錄與通知？

是 □（請說明或提佐證資料）：_____

_____

_____

否 □。

(九)元件是否能驗證網站正確性？

是 □（請說明或提佐證資料）：_____

_____

_____

否 □。

(十)「晶片金融卡客戶端 ActiveX 處理元件」之保護方式：

□ 元件經合法之 CA 簽章保護，以利瀏覽器辨識元件之合法性。

□ 元件提供交易傳輸資料之隱密性保護，採用加密演算法，如 Triple-DES(112 bit)、AES(128 bit)或 RSA(2048 bit)，支援更換基碼的功能

□ 元件提供交易不可否認性功能，以利伺服器主機端確認元件的合法性

□ 其他（請說明）：_____

_____

□無

(十一) 代理行之交易紀錄保留期限多久？（請說明）

_____

四、 伺服器使用管理方面：

(一) 網頁設計所使用之開發工具。

請填寫：_____

(二) 網頁設計是否委由廠商開發。

是 □， 否 □。

(三) 是否架設防火牆保護該伺服器。

是 □， 否 □。

(四) 是否架設入侵偵測系統（IDS）保護該伺服器。

是 □， 否 □。

（五）伺服器是否安裝防毒軟體，並隨時更新病毒碼。

是 □， 否 □（請說明）：_____

（六）伺服器作業系統是否適時更新修正程式。

是 □， 否 □。

（七）伺服器作業系統最高權限（Administrator）管理方式：

□密碼分持（非1人持有） □停用 □更名

□其他（請說明）：_____

（八）是否定期檢視與掃描伺服器弱點，並適時改善。

是 □， 否 □。

（九）伺服器作業系統是否啟動事件檢視器之安全紀錄功能。

是 □， 否 □。

（十）是否針對模擬 貴行之釣魚網頁定期搜尋。

是 □， 否 □。

五、 其他：

對客戶建議、銷售或贈與使用之晶片金融卡網際網路讀卡機，是否符合下列標準或規範？

□ 通過UL19500，CNS13438，FCC，CE.等至少二種以上安規。

□ 符合ISO 7816標準。

□ 符合PC/SC規範。

□ 通過EMV Level 1認證，能讀取FISC II規格之晶片金融卡。

□ 經銀行公會測試驗證通過，並提供經濟部標準檢驗局所核發「商品型式認可證明書」，商品型式認可證明書須載明型號（USB及RS-232介面）。

□ 具有顯示幕及確認鍵，由讀卡機端發動交易確認之功能。