收文編號：1050006310

立法院議案關係文書

中華民國 105 年 10 月 5 日印發

案由：行政院函送本院委員賴士葆等 18 人於第 9 屆第 1 會期第 19 次會議所提臨時提案之研處情形，請查照案。

行政院函

受文者：立法院

發文日期：中華民國 105 年 9 月 23 日

發文字號：院臺金字第 1050038816 號

速別：速件

密等及解密條件或保密期限：普通

附件：如文

主旨：貴院函送賴委員士葆等 18 人所提之臨時提案，經貴院第 9 屆第 1 會期第 19 次會議討論決議：「函請行政院研處」一案，經交據金融監督管理委員會函報會商相關機關研處情形，復請查照。

說明：

一、復貴院 105 年 7 月 13 日台立院議字第 1050704033 號函。

二、影附金融監督管理委員會 105 年 9 月 21 日金管銀國字第 10500214750 號函及附件各 1 份。

正本：立法院

副本：金融監督管理委員會

金融監督管理委員會函

受文者：行政院

發文日期：中華民國 105 年 9 月 21 日

發文字號：金管銀國字第 10500214750 號

速別：普通件

密等及解密條件或保密期限：

附件：如文

主旨：關於函囑就立法院賴委員士葆等 18 人所提之臨時提案，會商相關機關於 2 個月內研處具復一案，經洽會鈞院資通安全處、國土安全辦公室、法務部、內政部等相關機關意見，擬具說明資料如附件，請鑒核。

說明：依據鈞院秘書長 105 年 7 月 14 日院臺金字第 1050030747 號函辦理。

正本：行政院

副本：本會銀行局

主任委員　丁　克　華

關於立法院賴委員士葆等 18 人就「強化查緝詐騙集團在 ATM 側錄卡片之手法，及提出針對惡意軟體/勒索軟體之金融網絡資安預警執行計畫」所提提案，經洽會行政院資通安全處、行政院國土安全辦公室、法務部及內政部等相關機關意見，說明如下：

一、我國金融卡已全面晶片化（金管會）：

為解決磁條金融卡易遭偽冒、側錄之交易安全問題，金管會已督促金融機構於 100 年 6 月 30 日完成國內金融卡全面晶片化。另若 ATM 遭植入惡意軟體，因無法側錄晶片卡金鑰，且晶片金融卡交易驗證碼僅對當次交易有效，爰藉由側錄晶片金融卡交易無法複製偽卡，或產製有效之偽冒交易。又因晶片金融卡採用之晶片皆經國際安全認證，能防堵市面常見之攻擊，尚無安全之疑慮。

二、全方位落實 ATM 防護（金管會）：

為防範 ATM 淪為詐騙集團之犯罪工具，或遭受惡意軟體/勒索軟體攻擊，已督促金融機構積極落實 ATM 各項防護措施，以確保金融機構資訊安全：

(一)設備面之安全設計：

1. ATM 金庫裝置應符合國際規格或其他相同安全強度之金庫標準。
2. ATM 鍵盤應符合亂碼化鋼製安全鍵盤規格。
3. ATM 讀卡機應符合 ISO 規範。
4. 敏感性資料應透過硬體亂碼化設備加密防護，亂碼化設備應符合國際規格或其他相同安全強度之標準。

(二)應用程式之安全設計：

1. 應設計唯一端末設備代號。
2. 應加強 ATM 網路存取權限管控（如防火牆、存取名單 ACL 等）及可執行程式辨識（如防毒軟體、白名單或限制使用執行權限）。
3. ATM 端可及的伺服器（如軟體派送伺服器、SNA 伺服器）應安裝防毒軟體並及時更新，另對該等伺服器應進行弱點掃瞄及修補。
4. 採用軟體派送機制更新 ATM 程式者，應定期更換密碼；並設計兩人（含）以上管控或採用兩項（含）技術以上管控（如密碼及 IC 卡）等機制。
5. 應檢視 ATM 網段是否達到必要區隔，包含分行人員、可連線之人員與操作設備、環控設備等。

(三)環境面之安全維護：

1. 應裝置於明亮處所，機身及周邊夜間照明狀況良好。
2. 應保持自動化服務區之環境實體完整性，不定時派員檢視是否遭放置非授權設備（如磁條讀卡機、監視器）。
3. 應裝設監視系統及警示通報系統，並於隱密處裝置監視錄影系統，以清晰監控客戶之面貌、動作、機具運作情形及機器維修、鈔匣換裝等人員動態。

(四)資安評估之落實：

1. 每年應針對 ATM、ATM 端可及之伺服器、工作站、網路設備進行資訊安全評估作業，以發現資安威脅與弱點，改善並提升網路與資訊系統安全防護能力。
2. 每年應辦理社交工程演練，加強資安意識訓練。

(五)監控機制之執行：

1. 應建置 ATM 監控系統，ATM 設備與應用程式運作異常時，應即時通報監控中心。
2. 應建立 ATM 提領監控機制，並產生監控報表，由專人每日檢視有無應申報之可疑交易。

(六)委外作業之管理：

1. 與委外廠商簽訂之合約中，應特別要求簽訂未曾植入非法或足以損害正常作業與保密之功能，及未於機器上作任何不正當作業之行為。
2. 應檢視 ATM 安裝、維護作業之人員並造冊列管，如有異動，應即時更新。
3. 委外廠商維修時，應查明身分，並派員在場監督，且留存紀錄。

三、深化關鍵基礎設施之安全防護能量（行政院國土安全辦公室）：

(一)已訂定「國家關鍵基礎設施安全防護指導綱要」，關鍵基礎設施（CI）分類之八大主部門包括銀行與金融。

(二)成立關鍵基礎設施防護推動小組推動相關事宜，要求各相關部會以「全災害」防護概念（含意外事件、恐怖攻擊、網路攻擊等），落實執行各項風險與資產評估、防護計畫與機制訂定、應變能量整合、防災韌性提升等工作，且每年以各項講習訓練/指定演練/訪評檢核其應對之防護能量，並驗證關鍵基礎設施安全防護機制及應變處置程序，提升國家關鍵基礎設施整體防護能量。

四、推動跨部會合作機制（內政部）：

內政部、法務部、通傳會、經濟部、金管會及科技部等相關部會已成立跨部會協商平臺，定期共同研商犯罪偵防相關政策與推動重要業務。

五、積極查緝詐欺集團，以嚇阻詐欺車手犯罪（法務部、內政部）：

(一)以不正方法由收費設備、自動付款設備取得他人之物，或以不正方法將虛偽資料或不正

指令輸入電腦或其他相關設備，製作財產權之得喪、變更紀錄等不法行為，於刑法第 339 條之 1 至第 339 條之 3 均有明文處罰規定。如知有犯罪嫌疑，均積極查辦。

(二)駭客集團多透過網路跳板進行犯罪，針對境外來源入侵事件，積極與大陸、港澳地區及第三地警方擴大合作範圍與深度，穩固辦案聯繫窗口合作機制及擴大警務交流層面，以情資交換與案件協查之方式，期能有效追緝境外集團核心與成員。

六、強化調查人員訓練及金檢重點（法務部、金管會）：

(一)法務部調查局已重新佈署網路犯罪調查人力，並強化各項專業訓練，充實數位鑑識、惡意程式解析技能。

(二)金管會已將金融業發展數位金融之資安措施，列為金融檢查重點。

七、加強宣導資安觀念（行政院資通安全處）：

製作勒索軟體之宣導教材，透過各管道、相關活動或社群網站，加以宣導。

八、未來工作重點：

行政院除督促各相關部會積極落實上揭各項防護措施外，並適時檢討及強化防護措施。