專營電子支付機構檢查手冊(異動版)

一、業務管理之查核（共 1 項）

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.1.5	(5)於身分確認程序核驗存款帳戶及信用卡時，是否核驗個人使用者留存於開戶金融機構或信用卡發卡機構之行動電話號碼？如有異常之情事，是否採用符合標準之安全設計加強確認。		電子支付機構資訊系統標準及安全控管作業基準第 7 條	配合本會 112.3.20 金管銀票字第 1120133069 號函同意備查銀行公會所訂「電子支付機構資訊系統標準及安全控管作業基準」，增訂核驗個人使用者留存於開戶金融機構或信用卡發卡機構行動電話號碼之查核項目。

二、資訊作業之查核（共 2 項）

項目編號	查核事項		法令規章	說明
	修正後	修正前		
1.5	5.是否於每年四月底前由會計師檢視提出資訊系統及安全控管作業評估報告？	5.是否定期由會計師檢視提出資訊系統及安全控管作業評估報告？	電子支付機構資訊系統標準及安全控管作業基準第 26 條	配合本會 112.3.20 金管銀票字第 1120133069 號函同意備查銀行公會所訂「電子支付機構資訊

項目編號	查核事項		法令規章	說明
	修正後	修正前		
				系統標準及安全控管作業基準」，增訂資訊系統及安全控管作業評估報告應於每年四月底前辦理之文字。
3.1.4 3.1.4.2 3.1.4.7 3.1.4.8	(4)使用者及特約機構端行動裝置應用程式： ②應於發布前檢視應用程式所需權限應與提供服務相當，首次發布或權限變動應經資安、法遵及風控等主管同意，以利綜合評估是否符合「個人資料保護法」之告知義務。 ⑦應每年由合格實驗室辦理並通過檢測，且由資安專責主管確認完成改善。 ⑧應用程式及其應用伺服器於每年、新功能首次上限、系統架構異動或既有功能異動時，應針對新增或異動之程式辦理程式碼掃碼或黑箱測試，並修正中/高風險漏洞；辦理國內外小額匯兌者，應依據 OWASP 公布之	(4)使用者及特約機構端行動裝置應用程式： ②應於發布前檢視應用程式所需權限應與提供服務相當，首次發布或權限變動應經資安、法遵及風控等單位同意，以利綜合評估是否符合「個人資料保護法」之告知義務。 ⑦應每年由合格實驗室辦理並通過檢測，且由資安專責單位確認完成改善。 ⑧應用程式及其應用伺服器於每年、新功能首次上限、系統架構異動或既有功能異動時，應辦理程式碼掃碼或黑箱測試，並修正中/高風險漏洞；辦理國內外小額匯兌者，應依據 OWASP 公布之 MobileAPPSecurityChecklistL	電子支付機構資訊系統標準及安全控管作業基準第 11 條	配合本會 112.3.20 金管銀票字第 1120133069 號函同意備查銀行公會所訂「電子支付機構資訊系統標準及安全控管作業基準」，修訂查核事項，將「單位」二字修訂為「主管」及增加「針對新增或異動之程式」之文字。

項目編號	查核事項		法令規章	說明
	修正後	修正前		
	MobileAPPSecurityChecklistL2 或 MobileTop10 項目辦理並通過檢測，且由資安專責主管確認完成改善。	2 或 MobileTop10 項目辦理並通過檢測，且由資安專責單位確認完成改善。		