## 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		1. 人 旧 立	חח געב
	修正後	修正前	法令規章	說明
1.1.5	(5)於身分確認程序核驗存款帳戶及		電子支付機構資訊系統標準	配合本會 112.3.20 金管
	信用卡時,是否核驗個人使用者留		及安全控管作業基準第7條	銀票字第 1120133069 號
	存於開戶金融機構或信用卡發卡			函同意備查銀行公會所
	機構之行動電話號碼?如有異常			訂「電子支付機構資訊
	之情事,是否採用符合標準之安全			系統標準及安全控管作
	設計加強確認。			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		11 人 旧 立	AV nu
	修正後	修正前	法令規章	說明
1.5	5. 是否於每年四月底前由會計師檢視	5. 是否定期由會計師檢視提出資訊系	電子支付機構資訊系統標準	配合本會 112.3.20 金管
	提出資訊系統及安全控管作業評	統及安全控管作業評估報告?	及安全控管作業基準第 26	銀票字第 1120133069 號
	估報告?		條	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		14 人 14 立	TV utt
	修正後	修正前	法令規章	說明
				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辨
				理之文字。
3. 1. 4	(4)使用者及特約機構端行動裝置應	(4)使用者及特約機構端行動裝置應	電子支付機構資訊系統標準	配合本會 112.3.20 金管
	用程式:	用程式:	及安全控管作業基準第 11	銀票字第 1120133069 號
3. 1. 4. 2	②應於發布前檢視應用程式所需	②應於發布前檢視應用程式所需	條	函同意備查銀行公會所
	權限應與提供服務相當,首次發	權限應與提供服務相當,首次發		訂「電子支付機構資訊
	布或權限變動應經資安、法遵及	布或權限變動應經資安、法遵及		系統標準及安全控管作
	風控等 <u>主管</u> 同意,以利綜合評估	<b>風控等單位同意,以利綜合評估</b>		業基準」,修訂查核事
	是否符合「個人資料保護法」之	是否符合「個人資料保護法」之		項,將「單位」二字修
	告知義務。	告知義務。		訂為「主管」及增加「針
3. 1. 4. 7	⑦應每年由合格實驗室辦理並通	⑦應每年由合格實驗室辦理並通		對新增或異動之程式」
	過檢測,且由資安專責主管確認	過檢測,且由資安專責單位確認		之文字。
	完成改善。	完成改善。		
3. 1. 4. 8	⑧應用程式及其應用伺服器於每	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	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	異動或既有功能異動時,應辦理		
	新增或異動之程式辦理程式碼	程式碼掃碼或黑箱測試,並修正		
	掃碼或黑箱測試,並修正中/高	中/高風險漏洞;辦理國內外小		
	風險漏洞;辦理國內外小額匯兌	額匯兌者,應依據 OWASP 公布之		
	者,應依據 OWASP 公布之	MobileAPPSecurityChecklistL		

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