金融機構辦理電子銀行業務安全控管作業基準部分條文修正對照表

附件三

修正條文	現行條文	說明
第二條　本基準用詞定義如下： 二十、結構型商品：係指 (一)「銀行辦理衍生性金融商品業務內部作業制度及程序管理辦法」第二條所稱之結構型商品。 (二)「信託業營運範圍受益權轉讓限制風險揭露及行銷訂約管理辦法」第二十二條之一所稱之境內結構型商品及「境外結構型商品管理規則」第二條所稱之境外結構型商品。 二十四、客戶端電腦應用程式：指金融機構提供並安裝於客戶端電腦(如 Windows, UNIX,MacOS)之應用程式(EXE,OCX,SCR,COM,DLL 等)。 二十五、C3 憑證：指符合我國電子簽章法且經本會認可之憑證，其註冊中心應為金融機構，且身分識別方式有二：採當面辦理者，必須由本人親自辦理或持有授權文件之代理人親自辦理，採非當面辦理者，得以視訊或由往來金融機構確認客戶身分等方式辦理。	第二條　本基準用詞定義如下： 二十、結構型商品：係指「銀行辦理衍生性金融商品業務內部作業制度及程序管理辦法」第二條所稱之結構型商品，不含結構型債券及「境外結構型商品管理規則」所稱之境外結構型商品。 <新增> <新增> <新增>	一、原第二十款第一目涉及信託部分移至同款第二目並刪除「，不含結構型債券」。 二、第二十款第二目係依金管會民國 109 年 10 月 16 日金管銀票字第 1090221817 號函放寬境外結構型商品得以電子設備方式辦理，及依「信託業營運範圍受益權轉讓限制風險揭露及行銷訂約管理辦法」第二十二條之一立法說明，開放境內結構型商品得透過電子設備辦理，修正第二十款。 三、新增第二十四款客戶端電腦應用程式用詞定義，係指安裝

		於個人電腦之可執行應用程式，不包含已另有其他規範之應用程式(如行動裝置應用程式)。 四、新增第二十五款C3憑證用詞定義並明訂註冊中心應為金融機構，包含銀行、證券及保險及身分識別方式。
第四條　電子銀行業務之交易類別及風險 一、電子轉帳及交易指示類 (一)服務項目 2、申請指示，其服務項目舉例如下： (3)授信業務 甲、本行既有個人客戶及新戶得申辦無涉及抵押權或質權設定之個人貸款、限於原抵押權擔保範圍內增貸之房貸及車貸、同意金融機構查詢聯徵中心個人信用資料。 乙、本行既有法人客戶、法人新戶及法人戶之負責人得申辦無涉及抵押權或質權設定之貸款、同意金融機構查詢聯徵中心信用資料。 丙、既有貸款戶得申辦授信條件變更。 丁、保證人得申辦同意金融機構查詢聯徵中心信用資料、成立保證契約。	第四條　電子銀行業務之交易類別及風險 一、電子轉帳及交易指示類 (一)服務項目 2、申請指示，其服務項目舉例如下： (3)授信業務 甲、本行既有客戶及新戶得申辦個人貸款、限於原抵押權擔保範圍內增貸之房貸及車貸、同意金融機構查詢聯徵中心個人信用資料。 <新增> 乙、既有貸款戶得申辦授信條件變更。 丙、保證人得申辦同意金融機構查詢聯徵中心個人信用資料、成立保證契約。	一、授信業務新增法人服務項目，係依據110年6月2日金管銀國字第1100271627號函、110年7月23日金管銀國字第11001381351號函及110年9月29日授信業務委員會召開「銀行辦理線上貸款相關議題」專案小組第7次專案會議紀錄辦理。 二、考量線上辦理質權設定之貸款，如屬銀行自行之定存單，依民法規定，應將實

戊、法人戶依信保基金規定應查詢之關係人(如配偶)得申辦同意金融機構查詢聯徵中心信用資料。	丁、法人戶得申辦同意金融機構查詢聯徵中心信用資料。	體定存單交付質權人，此交付形式目前尚無法以線上取代。如為他行之定存單，尚須要求他行同意拋棄對存款行使抵押權，涉及權利義務者眾多，將增加線上辦理定存單設質之困難。另有關有價證券設質部分，尚涉及發行公司(或股務代理機構)、集保公司等機關，依目前相關業務規範亦無法線上完成設質作業。如為境外之有價證券，可能存在更多技術上之困難，故有價證券線上設質實務上亦屬不可行。據此，爰不開放線上辦理質權設定之貸款業務。 三、依金管會 111 年 5 月 16 日金管銀國字第 1110205052 號函示，法人客戶得線上申請貸款，並同意金

		融機構查詢聯徵中心信用資料，惟如非屬3位以下本國籍自然人股東之法人新戶無法線上申請貸款及同意金融機構查詢聯徵中心信用資料，將不利線上業務發展，爰將第一款第二目第三子目之乙有關法人新戶係指3位以下本國籍自然人股東之公司，不包括有法人股東公司等相關文字刪除。
第四條 電子銀行業務之交易類別及風險 一、電子轉帳及交易指示類 （一)服務項目 2、申請指示，其服務項目舉例如下： （5)財富管理業務：認識客戶作業(KYC)、客戶風險承受度測驗、同意第二條第二十款第一目結構型商品業務之推介或終止推介。 （6)信託業務：已開立存款帳戶者得申辦信託開戶或終止信託契約、認識客戶作業(KYC)、客戶風險承受度測驗、同意信託業務之推介或終止推介、同意成為專業投資人之簽署、專業投資人表	第四條 電子銀行業務之交易類別及風險 一、電子轉帳及交易指示類 （一)服務項目 2、申請指示，其服務項目舉例如下： （5)財富管理業務：已開立存款帳戶者得申辦信託開戶、認識客戶作業(KYC)、客戶風險承受度測驗、同意信託業務之推介或終止推介、同意結構型商品業務之推介或終止推介。 <新增>	一、刪除第一款第一目第二子目之(5)財富管理業務中與信託相關業務，係因已另外新增(6)信託業務，配合將原列於財富管理業務之信託項目移列，以符實際。另為配合修正第二條有關結構型商品定義，明定財富管理業務項下之結構型商品業務係指第二條第二十款第

示已充分審閱而無須適用審閱期之聲明。 (7)共同行銷業務：同意共同行銷。	(6)共同行銷業務：同意共同行銷。	一目。 二、新增(6)信託業務之終止信託契約、同意成為專業投資人之簽署、專業投資人表示已充分審閱而無須適用審閱期之聲明，係依據金管會民國109年10月16日金管銀票字第1090221817號函辦理。
第四條　電子銀行業務之交易類別及風險 一、電子轉帳及交易指示類 （二）交易指示 1、高風險交易：係指該訊息執行結果，對客戶權益有重大影響之各類電子轉帳及交易指示，包含非約定轉帳交易超過最高限額之交易指示。 2、低風險交易：係指…： (4)辦理約定轉入帳戶之設定及轉帳。	第四條　電子銀行業務之交易類別及風險 一、電子轉帳及交易指示類 （二）交易指示 依據其交易指示執行結果對客戶權益影響之不同，可再行區分為高風險性之交易及低風險性之交易。 1、高風險交易：係指該訊息執行結果，對客戶權益有重大影響之各類電子轉帳及交易指示。 2、低風險交易：係指…： (4)辦理約定轉入帳戶之轉帳。 (6)約定轉入帳戶之設定，其交易限額同(10)之乙要求，若配合採用各種嚴密之技術防護措施，提供客戶確認設定內容並能防止或偵測設定內容被竄改，其限額可由個別金融機構 視其風險承擔之能力斟酌予以適當提高。	一、補充說明高風險交易係指低風險交易以外且對客戶權益有重大影響之交易指示。 二、合併低風險交易之(4)及(6)並將(6)內容移至第八條第三款第一目第四子目之三集中說明。 三、低風險交易之(6)及(7)明定可透過透過金融資訊服務事業、票據交換所平台驗證同一統一編號帳戶後於任一金融機構

(６)任一金融機構同一統一編號帳戶間轉帳、定存或投資。 (７)貸款撥款至任一金融機構同一統一編號帳戶或學校之就學貸款指定帳戶。 (８)客戶非直接獲取金融機構之服務且需其人工確認客戶身分與指示內容之申請指示、交易指示及資料預處理。 (９)辦理非約定轉入帳戶之轉帳。 (１０)個人資料異動（如…等）	(７)同一統一編號帳戶間轉帳、定存或投資。 (８)貸款撥款至同一統一編號帳戶或學校之就學貸款指定帳戶。 (９)客戶非直接獲取金融機構之服務且需其人工確認客戶身分與指示內容之申請指示類。 (１０)非約定轉入帳戶 甲、ATM、POS 等之低風險性交易… 乙、網際網路之低風險性交易… 丙、透過網站、行動 APP、電子郵件… 丁、配合採用各種嚴密之技術防護措施… (１１)個人資料異動（如…等）。	辦理轉帳、定存、投資或貸款撥款。 四、低風險交易之(８)新增交易指示(如透過電子郵件之交易指示)及資料預處理(如資料輸入)。 五、低風險交易(１０)之甲、乙、丙、丁移至第八條第二款第五目集中說明。
第七條 交易面之介面安全設計 客戶發送訊息時，其介面及訊息之通訊傳輸應達到之安全防護措施，相關安全設計區分如下，並應符合第九條規定： 一、使用憑證簽章，其安全設計應簽署適當內容並確認該憑證之合法性、正確性、有效性、保證內容及用途限制。 四、使用「兩項以上技術」，其安全設計應具有下列三項之任兩項以上技術： (一)客戶與金融機構所約定之資訊，且無第三人	第七條 交易面之介面安全設計 係指客戶發送訊息時，其介面及訊息之通訊傳輸應達到之安全防護措施之設計方法，亦即金融機構於系統開發設計時，應加以考量或應具備之基本原則及項目。應用於高風險交易之安全設計可應用於低風險交易；應用於低風險交易之安全設計可應用於身分確認(如簽入作業)。 各項介面安全設計，區分如下： 一、使用憑證簽章，其安全設計應簽署適當內容並確認該憑證之合法性、正確性、有效性、保證等級及用途限制。 四、使用「兩項以上技術」，其安全設計應具有下列三項之任兩項以上技術： (一)客戶與金融機構所約定之資訊，且無第三人	一、酌修文字。 二、高低風險交易之應用原則移至第八條第一款及第二款分別說明。 三、第一款依據金管會檢查局 110 年 8 月 18 日檢局(地)字第 1100606104 號函辦理並考量部分憑證機構並未指定其憑證之保證等級，為保護客戶權益金融機構仍應確認其保證內容。

知悉（如密碼、圖形鎖、手勢等）。 (二)客戶所持有之設備，金融機構應確認該設備為客戶與金融機構所約定持有之實體設備(如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具、SIM卡認證等)。 (三)客戶提供給金融機構其所擁有之生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)，金融機構應直接或間接驗證該生物特徵。間接驗證係指由客戶端設備(如行動裝置)驗證或委由第三方驗證，金融機構僅讀取驗證結果，必要時應增加驗證來源辨識。	知悉（如密碼、圖形鎖、手勢等）。 （二）客戶所持有之設備，金融機構應確認該設備為客戶與金融機構所約定持有之實體設備(如密碼產生器、密碼卡、晶片卡、電腦、行動裝置、憑證載具等)。 （三）客戶提供給金融機構其所擁有之生物特徵(如指紋、臉部、虹膜、聲音、掌紋、靜脈、簽名等)，金融機構應直接或間接驗證該生物特徵。間接驗證係指由客戶端設備(如行動裝置)驗證或委由第三方驗證，金融機構僅讀取驗證結果，必要時應增加驗證來源辨識。	四、增加第四款第二目使用案例，該SIM卡認證係指驗證SIM卡為所約定之實體設備，無須查驗門號租用人。
第八條 交易類別之安全設計 一、「非電子轉帳及交易指示類」：辦理帳務類、個人資料類之查詢應採用第七條第一款至第三款之任一款、第七條第四款之任一項技術、或第七條第五款至第七款之任一款安全設計進行身分確認。	第八條 交易類別之安全設計 一、「非電子轉帳及交易指示類」 辦理帳務類、個人資料類之查詢應採用第七條第二項第一款至第三款之任一款、第七條第二項第四款之任一項技術、或第七條第二項第五款至第七款之任一款安全設計進行身分確認。	本條配合第七條項次調整由二項改為一項，刪除所有「第二項」文字。
第八條 交易類別之安全設計 二、「電子轉帳及交易指示類」之交易指示：辦理高風險交易每筆或每批應採用第七條第一款硬體金融FXML憑證簽章安全設計，辦理低風險交易應採用第七條第一款至第七款之任一款安全設計進行身分確認，其中非約定轉帳交易每筆應採用第七條第一款至第四款之任一款安全設計進行身分確認，但辦理下列業務，應遵循下列要求： (一)辦理「限定性繳稅費」應遵循下列要求：	第八條 交易類別之安全設計 二、「電子轉帳及交易指示類」之電子交易、轉帳授權、帳務通知等服務 辦理高風險交易應採用第七條第二項第一款安全設計，辦理低風險交易應採用第七條第二項第一款至第七款之任一款安全設計進行身分確認，但辦理下列業務，應遵循下列要求： （一）辦理「限定性繳稅費」應遵循下列要求：	一、第二款明定辦理高風險交易應每筆或每批進行硬體憑證簽章；低風險非約轉交易應每筆進行身分確認。 二、新增第二款第五目並合併第四條第一款第二目第二子目(10)之甲、乙、丙、

2、進行消費扣款之入帳帳戶，事業單位應指定一用於款項收取作業之活期性存款帳戶，客戶無需輸入該存款帳戶以避免遭竄改，另以行動 APP 進行每筆達等值新臺幣五千元以上之消費扣款時，應以簡訊、APP 推播、電子郵件或其他方式通知，若無法及時通知，應於如對帳單上提示請客戶提供及時聯繫管道，以利後續帳務通知，確保客戶權益，另金融機構得採用第七條第一款、第三款、第四款之任一款安全設計進行客戶身分確認後提供取消通知機制。 3、客戶辦理事業單位或金融機構發動交易指示之扣款約定時，扣款金融機構應採用第七條第一款至第四款之任一款安全設計進行客戶身分確認。 5、客戶向事業單位或金融機構終止扣款約定後，無需承擔遭冒用之損失，金融機構或事業單位應於十四日內返還帳款，客戶應配合協助後續調查作業。 (二) 辦理ＡＴＭ無卡提款業務，於申請時應採用第七條第一款硬體憑證簽章、第二款晶片金融卡、第三款密碼搭配指定之硬體設備產生一次性密碼或第四款『兩項以上技術』等安全設計進行身分確認，於交易時應採用第七條第三款密碼搭配指定之硬體設備產生一次性密碼或第四款『兩項以上技術』進行身分確認」，其提款金額應符合第四條第一款第二目低風險交易之限額規定，且與晶片金融卡之提款限額併計。	2、進行消費扣款之入帳帳戶，事業單位應指定一用於款項收取作業之活期性存款帳戶，客戶無需輸入該存款帳戶以避免遭竄改，另以行動 APP 進行每筆達等值新臺幣五千元以上之消費扣款時，應以簡訊、APP 推播、電子郵件或其他方式通知，若無法及時通知，應於如對帳單上提示請客戶提供及時聯繫管道，以利後續帳務通知，確保客戶權益，另金融機構得採用第七條第二項第一款、第三款、第四款之任一款安全設計進行客戶身分確認後提供取消通知機制。 3、 客戶辦理事業單位或金融機構發動交易指示之扣款約定時，扣款金融機構應採用第七條第二項第一款至第四款之任一款安全設計進行客戶身分確認。 5、 客戶向事業單位或金融機構終止扣款約定後，無需承擔遭冒用之損失，金融機構或事業單位應於十四日內返還帳款，客戶應配合協助後續調查作業。 (二) 辦理ＡＴＭ無卡提款業務，於申請時應採用第七條第二項第一款硬體憑證簽章、第二款晶片金融卡、第三款密碼搭配指定之硬體設備產生一次性密碼或第四款『兩項以上技術』等安全設計進行身分確認，於交易時應採用第七條第二項第三款密碼搭配指定之硬體設備產生一次性密碼或第四款『兩項以上技術』進行身分確認」，其提款金額應符合第四條第一款第二目低風險交易之限額規定，且與晶片金融卡之提款限額併計。	丁。 三、第二款第五目之4調整為三百萬元，係比照財金公司之「金融資訊系統自動化服務機器共用業務參加單位作業手冊」第一篇第一章第二節第三點一般轉帳之規定，調整為每戶每日最高可轉出之限額為新台幣三百萬元整。 四、第二款第五目之4提供可確認交易內容及防止內容被竄改之防護措施案例供參，惟金融機構仍應自行確認所採用之機制有效性並依據金管會檢查局 110 年 8 月 18 日檢局(地)字第 1100606104 號函辦理，明訂應留存該防護措施之評估紀錄。 五、第二款第五目之5明定指定照會人員之方式與要求。

(三) 個人辦理實體ＡＴＭ轉帳業務，每筆達等值新臺幣一萬元(含)以上時，應以簡訊、APP 推播、電子郵件或其他方式通知，若無法及時通知，應於如對帳單上提示請客戶提供及時聯繫管道，以利後續帳務通知，確保客戶權益，另金融機構得採用第七條第一款、第三款、第四款之任一款安全設計進行客戶身分確認後提供取消通知機制。	(三) 個人辦理實體ＡＴＭ轉帳業務，每筆達等值新臺幣一萬元(含)以上時，應以簡訊、APP 推播、電子郵件或其他方式通知，若無法及時通知，應於如對帳單上提示請客戶提供及時聯繫管道，以利後續帳務通知，確保客戶權益，另金融機構得採用第七條第二項第一款、第三款、第四款之任一款安全設計進行客戶身分確認後提供取消通知機制。	
(四) 辦理「結構型商品交易」應遵循下列要求： １、 交易及扣款帳戶以同一統一編號為限。 ２、 限非首次辦理之同類型結構型商品交易。 ３、 金融機構應提供交易內容供客戶確認，並考量電子交易風險承受度，單筆交易超過等值新臺幣一仟萬、每日累計交易金額超過等值新臺幣三仟萬以上之交易應採用第七條第一款高風險交易之安全設計進行客戶身分確認，以防止交易糾紛。 ４、 金融機構應留存客戶辦理交易指示及確認風險揭露相關紀錄（如:日期、同意內容或版本及身分驗證結果等）。	(四) 辦理「結構型商品交易」應遵循下列要求： １、 交易及扣款帳戶以同一統一編號為限。 ２、 限非首次辦理之同類型結構型商品交易。 ３、 金融機構應提供交易內容供客戶確認，並考量電子交易風險承受度，單筆交易超過等值新臺幣一仟萬、每日累計交易金額超過等值新臺幣三仟萬以上之交易應採用第七條第二項第一款高風險交易之安全設計進行客戶身分確認，以防止交易糾紛。 ４、 金融機構應留存客戶辦理交易指示及確認風險揭露相關紀錄（如:日期、同意內容或版本及身分驗證結果等）。	
(五)辦理「非約定轉入帳戶」應遵循下列要求： １、ATM、POS 等之低風險性交易，其限額應符合現行 ATM 作業及 POS 作業相關規定。 ２、網際網路之低風險性交易，以每一帳戶每筆不超過等值新臺幣五萬元、每天累	第四條　電子銀行業務之交易類別及風險 一、電子轉帳及交易指示類 (二)交易指示 ２、低風險交易： （１０）非約定轉入帳戶 甲、ATM、POS 等之低風險性交易，其限額應符合現行 ATM 作業及 POS 作業相關規定。	

積不超過等值新臺幣十萬元、每月累積不超過等值新臺幣二十萬元為限。 3、透過網站、行動 APP、電子郵件、傳真、FTP 或 AP2AP 等方式傳送且未經金融機構人工確認客戶身分與指示內容者，其交易限額同前一子目要求。 4、若採用之技術防護措施（如憑證簽章、晶片金融卡、非簡訊傳送之一次性密碼、視訊會議、第三人覆核、簡訊簡碼回傳、直接人臉辨識軌跡等），提供客戶確認該筆交易內容並能防止身分確認資料與交易內容被竄改者，該筆非約定轉入帳戶之轉帳限額，可由個別金融機構視其風險承擔之能力斟酌予以適當提高，最高該轉出帳號不超過當日累計等值新臺幣三佰萬元為限，並留存該技術評估紀錄。 5、若經客戶事先以臨櫃或視訊會議申請指定照會人員且由金融機構人工確認其指定人員之身分與指示內容者(如電話照會)，其交易限額由雙方依據風險承受度約定之。	乙、網際網路之低風險性交易，以每一帳戶每筆不超過等值新臺幣五萬元、每天累積不超過等值新臺幣十萬元、每月累積不超過等值新臺幣二十萬元為限。 丙、透過網站、行動 APP、電子郵件、傳真、FTP 或 AP2AP 等方式傳送且未經金融機構人工確認客戶身分與指內容者，其交易限額同(１０)之乙要求。 丁、配合採用各種嚴密之技術防護措施（如簡訊簡碼回傳），提供客戶確認該筆交易內容並能防止身分確認資料與交易內容被竄改者，該筆非約定轉入帳戶之轉帳限額，可由個別金融機構視其風險承擔之能力斟酌予以適當提高，最高不超過當日累計等值新臺幣二佰萬元為限;若經客戶事先申請且由金融機構人工與客戶確認其指定人員之身分與指示內容者(如電話照會)，其交易限額由雙方依據風險承受度約定之。	
第八條 交易類別之安全設計 三、「電子轉帳及交易指示類」之申請指示 （一)辦理存款業務應採用第七條第一款至第七款之任一款安全設計，但辦理下列業務，應遵循下列要求：	第八條 交易類別之安全設計 三、「電子轉帳及交易指示類」之申請指示服務 (一)辦理存款業務應採用第七條第二項第一款至第七款之任一款安全設計，但辦理下列業務，應遵循下列要求：	一、明定辦理「電子轉帳及交易指示類」之申請指示應遵循之安全設計。 二、新增第一目第４子目之（３），係自

1、臨櫃開立存款帳戶之存戶得線上首次申請晶片金融卡並親赴銀行櫃檯確認身分後辦理領卡。 2、辦理已持有晶片金融卡舊戶申請補換發晶片金融卡者，客戶應先登入網路銀行、行動銀行或網路 ATM 並採用第七條第三款一次性密碼或第四款「兩項以上技術」之安全設計進行身分確認、再郵寄至原留存通訊住址、客戶須透過該銀行 ATM 以舊卡啟用新卡並以系統驗證新舊卡內帳戶號碼係為一致。(如有一晶片金融卡設定多個帳戶號碼之情形，應以該卡片之主要帳戶號碼做驗證。) 3、辦理申請網路銀行或晶片金融卡之非約定轉帳功能應採用第七條第一款至第五款任一款進行設定，惟排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計。 4、辦理申請約定非同一統一編號之約定轉入帳戶，須透過線上逐筆採用第七條第一款至第五款任一款進行設定，並排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計設定，並應遵循下列要求： (1)首次設定非同一統一編號帳戶者須先經臨櫃或採用第七條第五款視訊會議確認身分後方可為之。 (2)電話語音或網路銀行之新約定帳戶應於申辦日後次一日始生效，惟同一統一編號帳戶經評估並無遭詐騙損失之虞者除外。	1、臨櫃開立存款帳戶之存戶得線上首次申請晶片金融卡並親赴銀行櫃檯確認身分後辦理領卡。 2、辦理已持有晶片金融卡舊戶申請補換發晶片金融卡者，客戶應先登入網路銀行、行動銀行或網路 ATM 並採用第七條第二項第三款一次性密碼或第四款「兩項以上技術」之安全設計進行身分確認、再郵寄至原留存通訊住址、客戶須透過該銀行 ATM 以舊卡啟用新卡並以系統驗證新舊卡內帳戶號碼係為一致。(如有一晶片金融卡設定多個帳戶號碼之情形，應以該卡片之主要帳戶號碼做驗證。) 3、辦理申請網路銀行或晶片金融卡之非約定轉帳功能應採用第七條第二項第一款至第五款任一款進行設定，惟排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計。 4、辦理申請約定非同一統一編號之約定轉入帳戶，須透過線上逐筆採用第七條第二項第一款至第五款任一款進行設定，並排除軟體 OTP 或透過簡訊傳送 OTP 之安全設計設定。 (1)首次設定非同一統一編號帳戶者須先經臨櫃或採用第七條第二項第五款視訊會議確認身分後方可為之。 (2)電話語音或網路銀行之新約定帳戶應於申辦日後次一日始生效，惟同一統一編號帳戶經評估並無遭詐騙損失之虞者除外。	第四條第一款第二目第二子目之(6)目移入。 三、新增第一目第7子目辦理晶片金融卡解鎖作業之安全設計。

（３）約定轉入帳戶之設定，其交易限額同第八條第二款第五目之２要求，若配合採用各種嚴密之技術防護措施，提供客戶確認設定內容並能防止或偵測設定內容被竄改，其限額可由個別金融機構 視其風險承擔之能力斟酌予以適當提高。 ７、辦理晶片金融卡密碼解鎖作業，應採用第七條第一款至第三款任一款安全設計，惟排除以數位存款帳戶之安全設計解鎖臨櫃帳戶之晶片金融卡、以第三類數位存款帳戶之安全設計解鎖第一類及第二類數位存款帳戶之晶片金融卡、以第二類數位存款帳戶或第一類低風險數位存款帳戶之安全設計解鎖第一類高風險數位存款帳戶之晶片金融卡並排除軟體 OTP 與簡訊 OTP，且應於發卡行之端末設備(如 ATM、POS、VTM 等)進行，並針對解鎖用之敏感資料採用符合第五條訊息隱密性要求，進行端點對端點加密防護。	原第四條第一款第二目第二子目之(６) （６）約定轉入帳戶之設定，其交易限額同(１０)之乙要求，若配合採用各種嚴密之技術防護措施，提供客戶確認設定內容並能防止或偵測設定內容被竄改，其限額可由個別金融機構 視其風險承擔之能力斟酌予以適當提高。 <新增>	
第八條 交易類別之安全設計 三、「電子轉帳及交易指示類」… （二）辦理個人授信業務應採用第七條第一款至第七款之任一款安全設計，但辦理下列業務，應遵循下列要求： １、辦理本行個人新戶(含借款人及保證人)同意金融機構查詢聯徵中心信用資料(申請階段)，應採用第七條第一款憑證簽章之安全設計，但如為他行既有非數位存款客	第八條 交易類別之安全設計 三、「電子轉帳及交易指示類」… （二）辦理授信業務應採用第七條第二項第一款至第七款之任一款安全設計，但辦理下列業務，應遵循下列要求： １、辦理本行新戶(含借款人及保證人)同意金融機構查詢聯徵中心信用資料(申請階段)，應採用第七條第二項第一款憑證簽章之安全設計，但如為他行既有非數位存	一、酌修文字。 二、第三款第二目增加「個人」二字，以釐清應用範圍。 三、調整第三款第二目之２(２)、２(３)、２(４)、３(５)係依據國發會 110 年 6 月 10 日「紓

戶，得採用下列任一方式之安全設計： （1）採用第七條第一款憑證簽章之安全設計。 （2）採用第七條第五款視訊會議之安全設計，上傳身分證影像檔，並搭配第七條第二款非數位存款帳戶晶片金融卡進行身分確認。 （3）採用第七條第八款存款帳戶之安全設計並上傳身分證影像檔，其中採用無卡方式核驗以簡訊或推播方式發送一次性密碼者，應依據客戶本人留存於非數位存款帳戶銀行的手機號碼進行發送。 （4）採用第七條第十款電信認證之安全設計，上傳身分證影像檔，並搭配第七條第五款視訊會議或第八款存款帳戶之財金公司之「跨行金融帳戶資訊核驗」進行身分確認，並視風險評估決定是否強化控管措施(如：確認門號使用電信業者服務已超過半年且近6個月內繳款正常並沒有停話紀錄等)。 2、辦理本行個人既有數位存款帳戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計： （1）本行既有第一類適用高風險交易之數位存款帳戶或第二類數位存款帳戶	款客戶，得採用下列任一方式之安全設計： （1）採用第七條第二項第一款憑證簽章之安全設計。 （2）採用第七條第二項第五款視訊會議之安全設計，上傳身分證影像檔，並搭配第七條第二項第二款非數位存款帳戶晶片金融卡進行身分確認。 （3）採用第七條第二項第八款存款帳戶之安全設計並上傳身分證影像檔，其中採用無卡方式核驗以簡訊或推播方式發送一次性密碼者，應依據客戶本人留存於非數位存款帳戶銀行的手機號碼進行發送。 （4）採用第七條第二項第十款電信認證之安全設計，上傳身分證影像檔，並搭配第七條第二項第五款視訊會議或第八款存款帳戶之財金公司之「跨行金融帳戶資訊核驗」進行身分確認，並視風險評估決定是否強化控管措施(如：確認門號使用電信業者服務已超過半年且近6個月內繳款正常並沒有停話紀錄等)。 2、辦理本行既有數位存款帳戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計： （1）本行既有第一類適用高風險交易之數位存款帳戶或第二類數位存款帳戶	困平台」會議決議銀行於疫情期間就既有數三帳戶或數一低風險帳戶得採用財金公司2566機制核身，並搭配電話知識詢問照會機制或上傳身分證影像檔、金管會110年8月13日金管銀國字第1100138025號函同意放寬既有數三客戶申辦個人貸款相關規範及110年9月29日授信業務委員會召開「銀行辦理線上貸款相關議題」專案小組第7次專案會議決議修正放寬既有數三客戶、既有數一適用低風險交易客戶及既有信用卡戶貸款契約對保之安全設計機制。

者，應採用第七條第一款至第七款之任一款安全設計方式辦理簽約對保。	者，應採用第七條第二項第一款至第七款之任一款安全設計方式辦理簽約對保。	
（2）本行既有第一類適用低風險交易之數位存款帳戶，辦理簽約對保應採用下列任一方式之安全設計： 甲、採用第七條第一款之硬體憑證簽章安全設計。 乙、採用第七條第八款存款帳戶之財金公司「跨行金融帳戶資訊核驗」，並搭配第七條第六款知識詢問或上傳身分證影像檔之安全設計機制辦理簽約對保者，得將款項撥入本人非數位存款帳戶。 丙、採用第七條第四款包含生物特徵之「兩項以上技術」搭配第九條第一款第一目第三子目軟體C3憑證簽章或第七條第六款知識詢問辦理簽約對保，得將款項撥入本人存款帳戶，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)。	（2）本行既有第一類適用低風險交易之數位存款帳戶，應採用第七條第二項第一款之硬體憑證簽章辦理簽約對保。	
（3）本行既有第三類數位存款帳戶，辦理簽約對保應採用下列任一方式之安全設計： 甲、採用第七條第一款硬體憑證簽章	（3）本行既有第三類數位存款帳戶，如採第七條第二項第五款視訊會議辦理簽約對保者，限將款項撥入本人非數位存款帳戶，如採用第七條第二項第一	

安全設計。 乙、採用第七條第五款視訊會議辦理簽約對保者，限將款項撥入本人非數位存款帳戶。 丙、採用第七條第八款存款帳戶之財金公司「跨行金融帳戶資訊核驗」，並搭配第七條第六款知識詢問或上傳身分證影像檔之安全設計機制辦理簽約對保者，得將款項撥入本人非數位存款帳戶。 丁、採用第七條第四款包含生物特徵之「兩項以上技術」搭配第九條第一款第一目第三子目軟體 C3 憑證簽章或第七條第六款知識詢問辦理簽約對保，得將款項撥入本人存款帳戶，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)。 (4)本行既有第三類數位存款帳戶，經確認資金使用於特定目的用途且借款人同意貸款款項直接撥入第三方公司之實體帳戶者，如採第七條第四款包含生物特徵之「兩項以上技術」及第七條第一款硬體憑證簽章辦理簽約對保者，得將款項撥入他行第三方公司之實體帳戶。	款之硬體憑證簽章，得撥入本人存款帳戶。	

3、辦理本行個人既有信用卡客戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計： （1）採用第七條第一款憑證簽章及第七條第五款視訊會議。 （2）採用第七條第三款一次性密碼，得將款項撥入本人非數位存款帳戶、第一類適用高風險交易之數位存款帳戶或第二類數位存款帳戶。 （3）採用第七條第三款一次性密碼及第七條第五款視訊會議，得將款項撥入本人第一類適用低風險交易之數位存款帳戶及第三類數位存款帳戶。 （4）採用第七條第四款包含生物特徵之「兩項以上技術」，得將款項撥入本人非數位存款帳戶、第一類適用高風險交易之數位存款帳戶或第二類數位存款帳戶。 （5）採用第七條第四款包含生物特徵之「兩項以上技術」搭配第九條第一款第一目第三子目軟體C3憑證簽章或第七條第六款知識詢問辦理簽約對保，得將款項撥入本人存款帳戶，並視貸款金額大小、貸款撥入帳戶為實體或數位帳戶等風險評估因素，決定是否強化控管措施(如：增加視訊會議或其他安全設計)。	3、辦理本行既有信用卡客戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計： （1）採用第七條第二項第一款憑證簽章及第七條第二項第五款視訊會議。 （2）採用第七條第二項第三款一次性密碼，得將款項撥入本人非數位存款帳戶、第一類適用高風險交易之數位存款帳戶或第二類數位存款帳戶。 （3）採用第七條第二項第三款一次性密碼及第七條第二項第五款視訊會議，得將款項撥入本人第一類適用低風險交易之數位存款帳戶及第三類數位存款帳戶。 （4）採用第七條第二項第四款包含生物特徵之「兩項以上技術」，得將款項撥入本人非數位存款帳戶、第一類適用高風險交易之數位存款帳戶或第二類數位存款帳戶。 <新增>	

（6）依「長期使用循環信用持卡人轉換機制」申辦信用貸款方案者，採用第七條第一款至第七款之任一款安全設計。 4、辦理本行個人新戶之貸款契約或保證人保證契約成立，簽約對保方式應採用下列任一方式之安全設計： （1）採用第七條第一款硬體憑證簽章之安全設計，得將款項撥入本人存款帳戶。 （2）採用第七條第八款存款帳戶之安全設計並上傳身分證影像檔，其中採用無卡方式核驗以簡訊或推播方式發送一次性密碼者，應依據客戶本人留存於非數位存款帳戶銀行的手機號碼進行發送，得將款項撥入本人存款帳戶。 （3）採用第七條第十款電信認證之安全設計者，上傳身分證影像檔，且限將款項撥入本人非數位存款帳戶，並視風險評估決定是否強化控管措施(如：確認門號使用電信業者服務已超過半年且近 6 個月內繳款正常並沒有停話紀錄、人工照會)。 5、辦理「個人貸款」及「房貸及車貸原抵押權擔保範圍內」之增貸，對原保證人增貸保證契約成立，簽約對保方式應採用第七條第一款至第五款之任一款安全設計。	（5）依「長期使用循環信用持卡人轉換機制」申辦信用貸款方案者，採用第七條第二項第一款至第七款之任一款安全設計。 4、辦理本行新戶之貸款契約或保證人保證契約成立，簽約對保方式應採用下列任一方式之安全設計： （1）採用第七條第二項第一款硬體憑證簽章之安全設計，得將款項撥入本人存款帳戶。 （2）採用第七條第二項第八款存款帳戶之安全設計並上傳身分證影像檔，其中採用無卡方式核驗以簡訊或推播方式發送一次性密碼者，應依據客戶本人留存於非數位存款帳戶銀行的手機號碼進行發送，得將款項撥入本人存款帳戶。 （3）採用第七條第二項第十款電信認證之安全設計者，上傳身分證影像檔，且限將款項撥入本人非數位存款帳戶，並視風險評估決定是否強化控管措施(如：確認門號使用電信業者服務已超過半年且近 6 個月內繳款正常並沒有停話紀錄、人工照會)。 5、辦理「個人貸款」及「房貸及車貸原抵押權擔保範圍內」之增貸，對原保證人增貸保證契約成立，簽約對保方式應採用第七條第二項第一款至第五款之任一款安全設	

6、辦理個人購屋貸款依「個人購屋貸款定型化契約應記載事項」第十三條及個人購車貸款依「個人購車貸款定型化契約應記載事項」第十二條（擔保物權連結條款）借款人或第三人提供擔保物設定抵押權予金融機構時，該抵押權擔保範圍僅限本貸款契約之債務，借款人因未來需求，需經擔保物提供人另以書面同意時，應採用第七條第一款硬體憑證簽章之安全設計。	計。 6、辦理法人戶同意金融機構查詢聯徵中心信用資料應採用第七條第二項第一款之安全設計。 7、辦理個人購屋貸款依「個人購屋貸款定型化契約應記載事項」第十三條及個人購車貸款依「個人購車貸款定型化契約應記載事項」第十二條（擔保物權連結條款）借款人或第三人提供擔保物設定抵押權予金融機構時，該抵押權擔保範圍僅限本貸款契約之債務，借款人因未來需求，需經擔保物提供人另以書面同意時，應採用第七條第二項第一款硬體憑證簽章之安全設計。	
第八條 交易類別之安全設計 三、「電子轉帳及交易指示類」… （三）辦理法人授信業務應遵循下列要求： 1、辦理本行既有法人客戶及法人新戶同意金融機構查詢聯徵中心信用資料，應採用下列安全設計機制： （1）採用第七條第一款硬體憑證簽章之安全設計。 （2）法人戶之負責人或保證人或依信保基金規定應查詢之關係人(如配偶)同意金融機構查詢聯徵中心信用資料之安全設計，應比照個人授信案件有關本行新戶同意金融機構查詢聯徵中心信用資料之安全設計。	<新增>	一、新增第三款第三目法人授信業務係依據金管會110年6月2日金管銀國字第1100271627號函同意既有法人戶線上貸款契約成立及110年7月23日金管銀國字第11001381351號函同意法人新戶線上貸款契約成立辦理。 二、新增第三款第六目信託業務，以配合第四條第一款第一目

2、辦理本行既有法人客戶之貸款契約成立，簽約對保方式應採用下列任一方式之安全設計： （1）採用第七條第一款硬體憑證簽章之安全設計。 （2）透過本行法人戶申請平台驗證檢核既有客戶事先以授權書方式授權原留存印鑑之安全設計。上述檢核流程應透過公司負責人進行線上身分驗證後傳送印鑑，公司負責人身分驗證須依第八條第三款第二目第一子目個人貸款身分確認機制，相關檢核及驗證軌跡、紀錄等應比照第九條第七款規定辦理。 3、辦理3位以下本國籍自然人股東之法人新戶(不包括有法人股東之公司)之貸款契約成立，簽約對保方式應採用第七條第一款硬體憑證簽章之安全設計。 4、辦理法人戶之負責人或保證人契約成立之簽約對保方式，應採用下列任一方式之安全設計： （1）採用第七條第一款硬體憑證簽章之安全設計。 （2）採用第七條第五款視訊會議，並搭配第七條第八款存款帳戶之財金公司「跨行金融帳戶資訊核驗」。 5、法人戶徵授信相關文件之上傳，應採用法		第二子目之(6)並得同財富管理業務採用第七條第一款至第七款之任一款安全設計進行身分確認。 三、依金管會111年5月16日金管銀國字第1110205052號函示，有關銀行檢核印鑑係客戶以線上方式提供，須由公司負責人進行線上身分驗證後傳送印鑑，故指示本會增列公司負責人身分驗證方式及相關檢核及驗證軌跡、紀錄等規定以供日後查驗。爰於第三款第三目第二子目之(2)增訂相關規範文字。 四、依金管會111年5月16日金管銀國字第1110205052號函示，如非屬3位以下本國籍自然人股東之法人新戶無法線上申請貸款及同意金融機構查詢聯徵中心信用

人戶及其負責人貸款契約成立之安全設計機制。 (四)信用卡業務除辦理新戶申辦信用卡業務應採用第七條第一款、第八款、第九款或第十款之任一款安全設計，其中採用第十款電信認證者，應視風險評估決定是否強化控管措施(如：確認門號使用電信業者服務已超過半年且近6個月內繳款正常並沒有停話紀錄、人工照會)；辦理其他信用卡業務應採用第七條第一款至第七款之任一款安全設計。 (五)辦理財富管理業務應採用第七條第一款至第七款之任一款安全設計，但本基準另有限制者，從其規定。 (六)辦理信託業務應採用第七條第一款至第七款之任一款安全設計，但本基準另有限制者，從其規定。	(三)信用卡業務除辦理新戶申辦信用卡業務應採用第七條第二項第一款、第八款、第九款或第十款之任一款安全設計，其中採用第十款電信認證者，應視風險評估決定是否強化控管措施(如：確認門號使用電信業者服務已超過半年且近6個月內繳款正常並沒有停話紀錄、人工照會)；辦理其他信用卡業務應採用第七條第二項第一款至第七款之任一款安全設計。 (四)辦理財富管理業務應採用第七條第二項第一款至第七款之任一款安全設計，但本基準另有限制者，從其規定。 <新增>	資料，不利線上業務發展，爰於第四條授信業務服務項目中刪除法人新戶係指3位以下本國籍自然人股東之公司，不包括有法人股東之公司等相關文字，並將該等文字調整增列於本條第三款第三目第三子目有關法人新戶貸款契約成立、簽約對保之安全設計規範中。
第九條 交易面之介面安全設計具體要求 一、採用第七條第一款憑證簽章，應遵循下列安全設計： (一)應採用經本會認可之憑證機構…。 1、採用經本會核可之金融FXML憑證得辦理非電子轉帳及交易指示類、電子轉帳及交易指示類之高風險和低風險交易。 2、採用內政部簽發之自然人憑證或經濟部簽發之工商憑證僅能應用於非電子轉帳及交易指示類、電子轉帳及交易指示類之申請指示服務。 3、採用經密碼保護之臺灣網路認證公司簽發第三級商務EC+憑證、第三級商務XML憑證或中華	第九條 交易面之安全設計 一、採用第七條第二項第一款憑證簽章之安全設計 (一)應採用經本會認可之憑證機構…。 1、採用經本會核可之金融憑證得辦理非電子轉帳及交易指示類、電子轉帳及交易指示類之高風險和低風險交易。 2、採用內政部簽發之自然人憑證或經濟部簽發之工商憑證僅能應用於非電子轉帳及交易指示類、電子轉帳及交易指示類之申請指示服務。 3、採用臺灣網路認證公司簽發且經密碼保護之第三級商務EC+憑證或商務XML憑證僅能應用於	一、本條配合第七條項次調整由二項改為一項，刪除所有「第二項」文字。 二、第一款第一目之1明訂金融憑證係指本會之金融FXML憑證。 三、第一款第一目之3新增中華電信Public CA憑證，係依據本技術分組110

電信公司簽發第三級 Public CA 憑證。上述 C3 憑證僅能應用於非電子轉帳及交易指示類服務、電子轉帳及交易指示類之申請指示服務，如若以臨櫃或第七條第一款至第五款之任一款安全設計進行身分確認者，方能辦理不涉及非約定轉入帳戶轉帳之低風險交易，惟金融機構應確保金鑰儲存安全。 (六)應用於高風險交易或開立第一類適用高風險交易之數位存款帳戶進行身分驗證者，憑證私鑰應儲存於經第三方認證之硬體裝置。	非電子轉帳及交易指示類、電子轉帳及交易指示類之申請指示服務。如又採用臨櫃親辦或第七條第二項第一款至第四款之任一款安全設計進行憑證申請之身分確認者，得辦理不涉及非約定轉入帳戶轉帳之低風險交易，惟金融機構應確保金鑰儲存安全。 (六)應用於高風險交易或依據「銀行受理客戶以網路方式開立數位存款帳戶作業範本」開立第一類帳戶並採用高風險之介面安全設計進行身分驗證者，憑證私鑰應儲存於經第三方認證之硬體裝置。	年 7 月 1 日會議紀錄並新增第七條第五款得辦理不涉及非約定轉入帳戶轉帳之低風險交易。 四、第一款第六目酌修文字。
第九條 交易面之介面安全設計具體要求 二、採用第七條第二款晶片金融卡，應遵循下列安全設計： 三、採用第七條第三款一次性密碼，應遵循下列安全設計： (二)採用簡訊傳送 OTP 時，應遵循下列安全設計： 1、應用於電子轉帳交易指示類時，應與發送行銷廣告之門號有所區隔。 2、應用於電子轉帳交易指示類並以簡訊傳送 OTP 重新設定固定密碼或重新綁定兩項以上技術時應加強防護機制(如交易密碼驗證、設備指定、推播確認、遞延交易並可偵測阻擋、降低額度、OTP 綁交易、語音 OTP、SIM 卡認證、錄影存證、雙向簡訊並可辨識來源電話、採用非交易設備確認交易	第九條 交易面之安全設計 二、採用第七條第二項第二款晶片金融卡之安全設計 三、採用第七條第二項第三款一次性密碼之安全設計 (二)採用簡訊傳送 OTP 時，應遵循下列安全設計： 1、應與發送行銷廣告之門號有所區隔。 2、採用固定密碼或兩項以上技術並應用於電子轉帳交易指示類者，如以簡訊傳送 OTP 重新設定該固定密碼或重新綁定該兩項以上技術時應加強防護機制，該機制應排除固定密碼或電子郵件認證。	一、配合第七條項次調整由二項改為一項，刪除所有「第二項」文字。 二、第三款第二目之 1 補充說明應用範圍，與信用卡業務區隔。

內容或依金融機構風險評估至少具相同安全強度之安全機制，並應留存評估紀錄及核決層級)，該機制應排除固定密碼或電子郵件認證。 3、應用於非約定轉入帳戶轉帳交易時… (2)考量客戶交易使用之電腦或行動裝置，可能遭植入惡意程式竊取 OTP 等敏感資料，應加強防護機制(如交易密碼驗證、設備指定、推播確認、遞延交易並可偵測阻擋、降低額度、OTP 綁交易、語音 OTP、SIM 卡認證、錄影存證、雙向簡訊並可辨識來源電話、採用非交易設備確認交易內容或依金融機構風險評估至少具相同安全強度之安全機制，並應留存評估紀錄及核決層級)。 4、應用於開立第二類數位存款帳戶時，手機號碼之設定應於臨櫃辦理，另異動應採用臨櫃或第七條第一款至第五款任一款進行設定，惟排除透過軟體 OTP 或簡訊傳送 OTP 之安全設計。	3、應用於非約定轉入帳戶轉帳交易時… (2)考量客戶交易使用之電腦或行動裝置，可能遭植入惡意程式竊取 OTP 等敏感資料，應加強防護機制(如交易密碼驗證、設備指定、推播確認、遞延交易並可偵測阻擋、降低額度、OTP 綁交易、語音 OTP、SIM 認證、錄影存證、雙向簡訊並可辨識來源電話、採用非交易設備確認交易內容等)。 4、應用於開立第二類數位存款帳戶時，手機號碼之設定應於臨櫃辦理，另異動應採用臨櫃或第七條第二項第一款至第五款任一款進行設定，惟排除透過軟體 OTP 或簡訊傳送 OTP 之安全設計。	
第九條 交易面之介面安全設計具體要求 四、採用第七條第四款「兩項以上技術」，應遵循下列安全設計： (一) 採用直接驗證生物特徵技術者… (二) 採用間接驗證生物特徵技術者…	第九條 交易面之安全設計 四、採用第七條第二項第四款生物特徵之安全設計 (一) 採用直接驗證生物特徵技術者… (二) 採用間接驗證生物特徵技術者…	刪除第二項及酌修文字

五、採用第七條第五款視訊會議之安全設計應確認真人(Liveness Detection)、本人(Biorecognition)辦理，以防止透過科技預先錄製影片、製作面具或模擬影像等機制偽冒身分。	五、採用第七條第二項第五款視訊會議之安全設計應確認真人(Liveness Detection)、本人(Biorecognition)辦理，以防止透過科技預先錄製影片、製作面具或模擬影像等機制偽冒身分。	
第九條 交易面之安全設計具體要求 六、採用第七條第六款知識詢問或第七條第七款固定密碼之安全設計時，僅限應用於辦理非電子轉帳及交易指示類及下列電子轉帳及交易指示類之業務： (四)財富管理業務 １、非首次之認識客戶作業。 ２、非首次之客戶風險承受度測驗。 ３、同意第二條第二十款第一目結構型商品業務之推介或終止推介。 (五)信託業務 １、非首次之認識客戶作業。 ２、非首次之客戶風險承受度測驗。 ３、信託業推介及終止推介同意書。 ４、同意簽署為專業投資人。 ５、專業投資人聲明表示已充分審閱而無須適用審閱期之規定。 (六)共同行銷業務。 (七)不涉及帳務通知或交易指示之個人資料異動。 (八)協助電子支付機構確認客戶身分。	第九條 交易面之安全設計 六、採用第七條第二項第六款知識詢問或第七條第二項第七款固定密碼之安全設計時，僅限應用於辦理非電子轉帳及交易指示類及下列電子轉帳及交易指示類之業務： (四)財富管理業務 １、非首次之認識客戶作業。 ２、非首次之客戶風險承受度測驗。 ３、信託業推介及終止推介同意書。 ４、同意結構型商品業務之推介或終止推介。 <新增> (五)共同行銷業務。 (六)不涉及帳務通知或交易指示之個人資料異動。 (七)協助電子支付機構確認客戶身分。	一、第六款第四目之３明定財富管理業務之結構型商品業務係指第二條第二十款第一目。 二、新增第六款第五目信託業務，原於財富管理業務與信託業務重疊之非首次認識客戶作業及非首次客戶風險承受度測驗複製至(五)信託業務之１、２；原於財富管理業務所列之信託業推介及終止推介同意書移至(五)信託業務之３。 三、新增第六款第五目之４～５係考量同意簽署為專業投資人、專業投資人聲明表示已充分審閱而無須適用審閱期之規定

		所涉風險較小，得採用第七條第六款或第七款固定密碼之安全設計進行身分確認。 四、配合新增第六款第五目信託業務，調整原第五目至第七目為第六目至第八目。
第九條 交易面之安全設計具體要求 八、個人資料顯示應採取隱碼機制。但如系統已對客戶進行身分確認者(如簽入作業)， 得不隱碼其帳號及確認交易之必要資訊，或已採取本基準第七條第一款至第四款之任一款安全設計者，變更個人資料欄位得不予隱碼處理。 九、應用於法人客戶之高風險交易且未能使用符合我國電子簽章法之數位簽章者，應遵循下列必要措施： (一)應針對金融機構本身及客戶進行風險評估，訂定交易額度與管控機制，並提報董(理)事會或經其授權之經理部門核定，但外國銀行在臺分行，得由總行授權之人員為之。 (二)應提供客戶交易再確認機制，並確保在安全實體環境下交付給客戶(如雙通道啟用)，客戶端應於每筆交易須經由至少兩人以上進行交易內容再確認，包含一位交易建檔人員及一位以上授權人員。 (三)交易再確認機制應採用非我國憑證機構通過WebTrust 或 ETSI 認可具密碼保護且可應用於	第九條 交易面之安全設計 八、個人資料顯示應採取隱碼機制。但如系統已對客戶進行身分確認者(如簽入作業)， 得不隱碼其帳號及確認交易之必要資訊，或已採取本基準第七條第二項第一款至第四款之任一款安全設計者，變更個人資料欄位得不予隱碼處理。 九、應用於法人客戶之高風險交易且未能使用符合我國電子簽章法之數位簽章者，應遵循下列必要措施： (一) 應針對金融機構本身及客戶進行風險評估，訂定交易額度與管控機制，並提報董(理)事會或經其授權之經理部門核定，但外國銀行在臺分行，得由總行授權之人員為之。 (二) 應提供客戶交易再確認機制，並確保在安全實體環境下交付給客戶(如雙通道啟用)，客戶端應於每筆交易須經由至少兩人以上進行交易內容再確認，包含一位交易建檔人員及一位以上授權人員。 (三) 交易再確認機制應採用非我國憑證機構通過WebTrust 或 ETSI 認可具密碼保護且可應用	刪除第二項

法人金融交易簽章之憑證、第七條第二款或第三款安全設計，並使用安全元件(Secure Element)、可信賴執行環境(Trusted Execution Environment)、安全載具(如動態密碼產生器)或增強防護機制之行動裝置應用程式軟硬體，以保護敏感資料，並遵循下列安全設計：	於法人金融交易簽章之憑證、第七條第二項第二款或第三款安全設計，並使用安全元件(Secure Element)、可信賴執行環境(Trusted Execution Environment)、安全載具(如動態密碼產生器)或增強防護機制之行動裝置應用程式軟硬體，以保護敏感資料，並遵循下列安全設計：	
第十條 交易面之應用系統之安全設計： 一、提供網際網路應用系統，應遵循下列必要措施： (七)採用固定密碼進行網路銀行身分確認者，應加強下列安全機制： 2、針對固定密碼應提供端點對端點加密機制。係指於客戶端(如瀏覽器)輸入資料後立即加密，傳送至金融機構可信任網段(如經兩道防火牆隔離之獨立網段)於符合 FIPS 140-2 Level 3 以上之硬體安全模組(如 HSM)內進行解密，並於硬體安全模組內或於無洩漏解密資料疑慮之安全環境進行驗證；如用戶代號為個人統一編號者，其使用者代號仍應加強防護(如雜湊、加密、混淆)。 (八)應提供客戶安全教育宣導，強化風險認知與交易確認。 二、提供客戶端電腦應用程式，應遵循…措施： (一) 可執行程式(如 EXE, COM 等)應採用被作業	第十條 交易面之應用系統之安全設計： 一、提供網際網路應用系統，應遵循下列必要措施： (七)應偵測網頁與程式異動時，進行紀錄與通知措施。(刪除) (八)採用固定密碼進行網路銀行身分確認者，應加強下列安全機制： 2、提供端點對端點加密機制。係指於客戶端(如瀏覽器)輸入資料後立即加密，傳送至金融機構可信任網段(如經兩道防火牆隔離之獨立網段)於符合 FIPS 140-2 Level 3 以上之硬體安全模組(如 HSM)內進行解密，並於硬體安全模組內或於無洩漏解密資料疑慮之安全環境進行驗證。 (九)應提供客戶安全教育宣導，強化風險認知與交易確認。 二、提供使用者端電腦應用程式，應遵循…措施： (一)應採用被作業系統認可之數位憑證進行程式碼簽	一、刪除第一款第七目，係因與第十一條第二款第一目第二子目之(一)重複，調整相關條次。 二、第一款第七目之2係依據金管會 110 年 11 月 23 日金管銀國字第 11002231191 號函辦理，新增個人戶如以統一編號登入電子銀行時，應依第七條第七款增設使用者代號且該使用者代號應加強防護。 二、第二款第一目新增於客戶端安裝電腦應用程式時，避免於安裝過程出現憑證相關安全警告。

系統認可之數位憑證進行程式碼簽章(CodeSign)且安裝過程不應出現憑證相關安全警告。 三、透過 QR Code 進行資料傳輸，應遵循下列必要措施： (一)QR Code 表示的資料應為辦理該業務所需最小化為原則。 (二)應用於電子轉帳及交易指示類時，應設計合理使用時效，且在時效內以使用一次為限 (三)所產生之 QR Code，如具客戶個人資料應符合訊息隱密性、如應用於電子轉帳及交易指示類時，應符合訊息完整性、訊息來源辨識性與訊息不可重複性。 (四)應針對解析 QR Code 後進行格式檢查，如為網站連接應進行網站合法性檢查。 四、提供行動裝置應用系統，應遵循「金融機構提供行動裝置應用程式作業規範」。	章(CodeSign)。 <新增> 三、提供行動裝置應用系統，應遵循「金融機構提供行動裝置應用程式作業規範」。	三、新增第三款 QRCode 相關要求，係依據金管會 110 年 11 月 23 日金管銀國字第 11002231191 號函、金管會檢查局 110 年 8 月 18 日檢局(地)字第 1100606104 號函辦理並調整相關條次。
第十四條 其他 一、電子銀行業務倘與第三方(含金控及其子公司)進行資料傳輸或服務委外時，除應符合訊息來源辨識外，簽訂相關契約，明訂其須符合本基準之相關規定及雙方責任。	第十四條 其他 一、電子銀行業務倘與第三方進行資料傳輸或服務委外時，除應符合訊息來源辨識外，簽訂相關契約，明訂其須符合本基準之相關規定及雙方責任。	第一款新增第三方應包含金控及其子公司。