

中華民國銀行公會

電子支付機構防制洗錢及打擊資恐注意事項範本

金融監督管理委員會 104 年 07 月 03 日
金管銀票字第 10400111140 號函准予備查
金融監督管理委員會 106 年 09 月 30 日
金管銀票字第 10600225010 號函准予備查

第一條

本範本依「洗錢防制法」、「資恐防制法」、「金融機構防制洗錢辦法」及「銀行業及電子支付機構電子票證發行機構防制洗錢及打擊資恐內部控制要點」規定訂定，以防制洗錢及打擊資助恐怖主義（以下簡稱防制洗錢及打擊資恐）為目的。

第二條

依「電子支付機構內部控制及稽核制度實施辦法」第三十三條規定建立之風險控管機制或內部控制制度，應經董（理）事會通過；修正時，亦同。其內容應包括下列事項：

- 一、依據「電子支付機構評估洗錢及資恐風險及訂定相關防制計畫指引」（附件），訂定對洗錢及資恐風險進行辨識、評估、管理之相關政策、程序。
- 二、依該指引與風險評估結果及業務規模，訂定防制洗錢及打擊資恐計畫，以管理及降低已辨識出之風險，並對其中之較高風險，採取強化控管措施。
- 三、監督控管防制洗錢及打擊資恐法令遵循及防制洗錢及打擊資恐計畫執行之標準作業程序，並納入自行查核及內部稽核項目，且於必要時予以強化。

前項第一款洗錢及資恐風險之辨識、評估及管理，應至少涵蓋使用者、地域、產品及服務、交易或支付管道等面向，並依下列規定辦

理：

一、應製作風險評估報告。

二、應考量所有風險因素，以決定整體風險等級，及降低風險之適當措施。

三、應訂定更新風險評估報告之機制，以確保風險資料之更新。

四、應於完成或更新風險評估報告時，將風險評估報告送金融監督管理委員會（以下簡稱金管會）備查。

第一項第二款之防制洗錢及打擊資恐計畫，應包括下列政策、程序及控管機制：

一、確認使用者身分。

二、使用者之姓名及名稱檢核。

三、帳戶及交易之持續監控。

四、紀錄保存。

五、一定金額以上通貨交易申報。

六、疑似洗錢或資恐交易申報及依據資恐防制法之通報。

七、指定防制洗錢及打擊資恐專責主管負責遵循事宜。

八、員工遴選及任用程序。

九、持續性員工訓練計畫。

十、測試防制洗錢及打擊資恐系統有效性之獨立稽核功能。

十一、其他依防制洗錢及打擊資恐相關法令及金管會規定之事項。

具國外分公司（或子公司）之電子支付機構，應訂定集團層次之防制洗錢與打擊資恐計畫，於集團內之分公司（或子公司）施行。其內容除包括前項政策、程序及控管機制外，另應在符合我國及國外分公司（或子公司）所在地資料保密規定之情形下，訂定下列事項：

一、為確認使用者身分與洗錢及資恐風險管理目的所需之集團內資訊分享政策及程序。

二、為防制洗錢及打擊資恐目的，於有必要時，依集團層次法令遵

循、稽核及防制洗錢及打擊資恐功能，要求國外分公司（或子公司）提供有關使用者、帳戶及交易資訊。

三、對運用被交換資訊及其保密之安全防護。

電子支付機構應確保其國外分公司（或子公司），在符合當地法令情形下，實施與總公司（或母公司）一致之防制洗錢及打擊資恐措施。
當總公司（或母公司）及分公司（或子公司）所在國之最低要求不同時，分公司（或子公司）應就兩地選擇較高標準者作為遵循依據，惟就標準高低之認定有疑義時，以電子支付機構總公司（或母公司）所在國之主管機關之認定為依據；倘因外國法規禁止，致無法採行與總公司（或母公司）相同標準時，應採取合宜之額外措施，以管理洗錢及資恐風險，並向金管會申報。

在臺外國金融機構集團分公司或子公司就第一項第一款及第二款應依據「電子支付機構評估洗錢及資恐風險及訂定相關防制計畫指引」訂定之洗錢及資恐風險辨識、評估、管理相關政策、程序，及防制洗錢及打擊資恐計畫所須包括之政策、程序及控管機制，若母集團已建立不低於我國規定且不違反我國法規情形者，在臺分公司或子公司得適用母集團之規定。

電子支付機構之董（理）事會對確保建立及維持適當有效之防制洗錢及打擊資恐內部控制負最終責任。董（理）事會及高階管理人員應瞭解其洗錢及資恐風險，及防制洗錢及打擊資恐計畫之運作，並採取措施以塑造重視防制洗錢及打擊資恐之文化。

第三條

本範本用詞定義如下：

- 一、一定金額：指新臺幣五十萬元（含等值外幣）。
- 二、通貨交易：單筆現金收或付之交易（在會計處理上，凡以現金收支傳票記帳者皆屬之）。
- 三、建立業務關係：係指電子支付機構接受使用者申請註冊時。

- 四、電子支付機構：指專營之電子支付機構及兼營電子支付機構業務之銀行、中華郵政股份有限公司及電子票證發行機構。
- 五、電子支付帳戶：指電子支付機構接受使用者開立記錄資金移轉或儲值情形之網路帳戶。
- 六、使用者：指於電子支付機構註冊及開立電子支付帳戶，利用電子支付機構所提供服務進行資金移轉及儲值者。
- 七、個人使用者：指自然人之使用者，包括外國自然人及大陸地區自然人。
- 八、非個人使用者：指我國政府機關、法人、行號、其他團體及外國法人與大陸地區法人之使用者。
- 九、實質受益人：指對使用者具最終所有權或控制權之自然人，或由他人代理交易之自然人本人，包括對法人或法律協議具最終有效控制權之自然人。
- 十、風險基礎方法：指電子支付機構應確認、評估及瞭解其暴露之洗錢及資恐風險，並採取適當防制洗錢及打擊資恐措施，以有效降低此類風險。依該方法，電子支付機構對於較高風險情形應採取加強措施，對於較低風險情形，則可採取相對簡化措施，以有效分配資源，並以最適當且有效之方法，降低經其確認之洗錢及資恐風險。

第四條

確認使用者身分措施，應依下列規定辦理：

一、有以下情形之一者應予以婉拒建立業務關係或交易：

(一) 疑似使用匿名、假名、人頭、虛設行號或虛設法人團體。

(二) 使用者拒絕提供審核使用者身分措施相關文件，但經可靠、獨立之來源確實查證身分屬實者不在此限。

(三) 對於由代理人辦理註冊電子支付帳戶或交易之情形，且查證代

理之事實及身分資料有困難。

(四) 持用偽、變造身分證明文件。

(五) 臨櫃申請時，出示之身分證明文件均為影本。但依規定得以身分證明文件影本或影像檔，輔以其他管控措施辦理之業務，不在此限。

(六) 提供文件資料可疑、模糊不清，不願提供其他佐證資料或提供之文件資料無法進行查證。

(七) 使用者不尋常拖延應補充之身分證明文件、登記證照或相關核准文件。

(八) 建立業務關係之對象為資恐防制法指定制裁之個人、法人或團體，以及外國政府或國際組織認定或追查之恐怖分子或團體。但依資恐防制法第六條第一項第二款至第四款所為支付不在此限。

(九) 對於已提供用於身分確認之同一金融支付工具，遭不同使用者重複提供用於身分確認。

(十) 經相關機關通報該使用者有非法使用金融機構存款帳戶或電子支付帳戶之紀錄。

(十一) 其他經主管機關規定應拒絕申請註冊之情形。

二、確認使用者身分時機：

(一) 電子支付機構與使用者建立業務關係時。

(二) 辦理達一定金額以上之通貨交易時。

(三) 電子支付機構於執行持續審查機制時，如有下列情形，應再次進行確認身分程序：

1、個人使用者與非個人使用者分別申請變更「電子支付機構使用者身分確認機制及交易限額管理辦法」第七條與第十一條之基本身分資料。

2、使用者電子支付帳戶之交易出現異常情形。

- 3、使用者於註冊時提供之身分證明文件或登記證照等相關文件疑似偽造或變造。
- 4、使用者交易時距前次交易已逾一年。
- 5、同一行動電話號碼遭不同使用者用於身分確認程序。
- 6、發現疑似洗錢或資恐交易時，或自洗錢或資恐高風險國家或地區存入款項之交易時。
- 7、對於所取得使用者身分資料之真實性或妥適性有所懷疑時。
- 8、電子支付機構依明顯事證認有必要再行確認使用者身分之情形。

三、確認使用者身分應採取下列方式辦理：

- (一) 電子支付機構與使用者建立業務關係時，應依「電子支付機構使用者身分確認機制及交易限額管理辦法」相關規定辦理。
- (二) 對於由代理人建立業務關係者，應確實查證代理之事實，並依前目方式辨識及驗證代理人身分，並保存該身分證明文件影本或予以記錄。
- (三) 針對第三類電子支付帳戶之非個人使用者為法人時，確認使用者之實質受益人，並以合理措施驗證其身分，包括使用可靠來源之資料或資訊。
- (四) 確認使用者身分措施，應包括瞭解建立業務關係之目的，並視情形取得相關資訊。
- (五) 再次識別及確認使用者身分資料，除核對身分證明文件及登記證照等相關文件方式外，得以下列方式辦理：
 - 1、要求使用者補充其他身分資料。
 - 2、以電話、電子郵件信箱或書面方式聯絡使用者。
 - 3、實地查訪使用者。
 - 4、向相關機構查證。

(六) 對於未能配合第二款第三目及前目規定再次進行識別及確認身分之使用者，應依契約約定暫停其交易功能。

四、第三款規定於使用者為非個人時，應瞭解使用者之業務性質及境外非個人使用者往來目的。

五、於申請第三類電子支付帳戶之非個人使用者為法人時，應瞭解下列資訊以確認其實質受益人：

(一) 具控制權之最終自然人身分（如姓名、出生日期、國籍及身分證明文件號碼等）。所稱具控制權係指持有該法人股份或資本超過百分之二十五者。

(二) 如未發現具控制權之自然人，或對具控制權自然人是否為實質受益人有所懷疑時，應徵詢有無透過其他方式對使用者行使控制權之自然人。必要時得取得使用者出具之聲明書確認實質受益人之身分。

(三) 如依前二小目規定均未發現具控制權之自然人時，應採取合理措施，確認擔任高階管理職位（如董事或總經理或其他具相當或類似職務之人）之自然人身分。

(四) 使用者或具控制權者為下列身分者，除有第六條第一項第三款但書情形者外，得不適用上開應辨識及確認實質受益人身分之規定：

- 1、我國政府機關。
- 2、我國公營事業機構。
- 3、外國政府機關。
- 4、我國公開發行公司或其子公司。
- 5、於國外掛牌並依掛牌所在地規定，應揭露其主要股東之股票上市、上櫃公司，或其子公司。
- 6、受我國監理之金融機構及其管理之投資工具。
- 7、設立於我國境外，且所受監理規範與防制洗錢金融行動工作

組織（FATF）所定防制洗錢及打擊資恐標準一致之金融機構，及該金融機構管理之投資工具。電子支付機構對前開金融機構及投資工具需留存相關文件證明（如公開資訊查核紀錄、該金融機構防制洗錢作業規章、負面資訊查詢紀錄、金融機構聲明書等）。

六、依據電子支付機構洗錢及資恐風險評估相關規範辨識為高風險或具特定高風險因子之使用者，應以加強方式執行驗證，例如：

（一）取得寄往使用者所提供住址之使用者本人/法人或團體之有權人簽署回函或辦理電話訪查。

（二）取得法人、團體資金來源及去向之佐證資料，如主要供應商名單、主要使用者名單等。

（三）實地訪查。

七、依據電子支付機構洗錢及資恐風險評估相關規範辨識為高風險或具特定高風險因子之使用者，電子支付機構於確認使用者身分時，應利用電子支付機構自行建置之資料庫或外部之資訊來源查詢使用者及其實質受益人、高階管理人員是否為現任或曾任國內外政府或國際組織之重要政治性職務人士：

（一）使用者或其實質受益人若為現任國外政府之重要政治性職務人士，應將該使用者直接視為高風險使用者，並採取第六條第一項第一款各目之強化確認使用者身分措施。

（二）使用者或其實質受益人若為現任國內政府或國際組織之重要政治性職務人士，應於與該使用者建立業務關係時，審視其風險，嗣後並應每年重新審視。對於經電子支付機構認定屬高風險業務關係者，應對該使用者採取第六條第一項第一款各目之強化確認使用者身分措施。

（三）使用者之高階管理人員若為現任國內外政府或國際組織之重要政治性職務人士，電子支付機構應考量該高階管理人員對

該使用者之影響力，決定是否對該使用者採取第六條第一項第一款各目之強化確認使用者身分措施。

(四) 對於非現任國內外政府或國際組織之重要政治性職務人士，電子支付機構應考量相關風險因子後評估其影響力，依風險基礎方法認定其是否應適用前三目之規定。

(五) 前四目規定於重要政治性職務人士之家庭成員及有密切關係之人，亦適用之。前述家庭成員及有密切關係之人之範圍，依洗錢防制法第七條第四項後段所定辦法之規定認定之。

(六) 第五款第四目第一小目至第三小目所列對象，其實質受益人或高階管理人員為重要政治性職務人士時，不適用本款第一目至第五目之規定。

八、確認使用者身分其他應遵循之事項：

(一) 在不違反相關法令情形下，電子支付機構如果得知或必須假定使用者往來資金來源自貪瀆或濫用公共資產時，應不予接受或斷絕業務往來關係。

(二) 電子支付機構在與使用者建立業務關係或懷疑使用者資料不足以確認身分時，應從政府核發或其他辨認文件確認使用者身分並加以記錄。

(三) 對採委託授權建立業務關係或建立業務關係後始發現有存疑之使用者應以電話、書面或實地查訪等方式確認。

(四) 電子支付機構對於無法完成確認使用者身分相關規定程序者，應考量申報與該使用者有關之疑似洗錢或資恐交易。

(五) 電子支付機構懷疑某使用者或交易可能涉及洗錢或資恐，且合理相信執行確認使用者身分程序可能對使用者洩露訊息時，得不執行該等程序，而改以申報疑似洗錢或資恐交易。

(六) 其他建立業務關係應注意事項悉依電子支付機構內部作業規定辦理。

九、有以下情形得依契約約定為下列之處理：

- (一) 對於第一款第八目情形，電子支付機構得暫停其使用電子支付機構業務服務或終止與其之契約。
- (二) 對於不配合確認或重新確認身分者、拒絕提供實質受益人或對使用者行使控制權之人等資訊、對交易之性質與目的或資金來源不願配合說明等使用者、或有相當事證足認有利用電子支付帳戶從事詐欺、洗錢等不法行為或疑似該等不法行為者，電子支付機構得暫停其使用電子支付機構業務服務之全部或一部；其情節重大者，應立即終止與其之契約。

十、對於有第一款第八目所述建立業務關係或交易對象情形，電子支付機構應依洗錢防制法第十條申報疑似洗錢或資恐交易，如該對象為資恐防制法指定制裁之個人、法人或團體，電子支付機構並應於知悉之日起不得有資恐防制法第七條第一項行為，及依資恐防制法規定辦理通報（格式請至法務部調查局網站下載）。電子支付機構若於前述對象受制裁指定前已有資恐防制法第六條第一項第三款及第四款情事，則應依資恐防制法相關子法向資恐審議會申請許可。

第五條

電子支付機構確認使用者身分措施，應包括對使用者身分之持續審查，並依下列規定辦理：

- 一、應對使用者業務關係中之交易進行詳細審視，以確保所進行之交易與使用者及其業務、風險相符，必要時並應瞭解其資金來源。
- 二、應定期檢視其辨識使用者及實質受益人身分所取得之資訊是否足夠，並確保該等資訊之更新，特別是高風險使用者，應至少每年檢視一次，除前述使用者外，應依風險基礎方法決定檢視頻率。
- 三、對使用者身分辨識與驗證程序，得以過去執行與保存資料為依

據，無須於使用者每次從事交易時，一再辨識及驗證使用者之身分。但電子支付機構對使用者資訊之真實性或妥適性有所懷疑、發現使用者涉及疑似洗錢或資恐交易，或使用者之交易或帳戶之運作方式出現與該使用者業務特性不符之重大變動時，應依第四條規定對使用者身分再次確認。

第六條

第四條第三款及第五條規定之確認使用者身分措施及持續審查機制，應以風險基礎方法決定其執行強度，包括：

一、對於高風險情形，應加強確認使用者身分或持續審查措施，其中至少應額外採取下列強化措施：

(一) 在建立或新增業務往來關係前，電子支付機構應取得依內部風險考量，所訂核准層級之高階管理人員同意。

(二) 在進行持續審查措施時，針對第三類電子支付帳戶使用者應採取合理措施以瞭解使用者財富及資金來源。其中資金來源係指產生該資金之實質來源（例如薪資、投資收益、買賣不動產等）。

(三) 對於業務往來關係應採取強化之持續監督。

二、對於來自洗錢或資恐高風險國家或地區之使用者，應採行與其風險相當之強化措施。

三、對於較低風險情形，得採取簡化措施，該簡化措施應與其較低風險因素相當。但有下列情形者，不得採取簡化確認使用者身分措施：

(一) 使用者來自未採取有效防制洗錢或打擊資恐之高風險國家或地區，高風險國家或地區係指金管會函轉國際防制洗錢組織所公告防制洗錢與打擊資恐有嚴重缺失之國家或地區。

(二) 足資懷疑該使用者或交易涉及洗錢或資恐。

電子支付機構得採行之簡化確認使用者身分措施如下：

一、降低使用者身分資訊更新之頻率。

二、降低持續性監控之等級，並以合理的金額門檻作為審查交易之基礎。

三、從交易類型或已建立業務往來關係可推斷其目的及性質者，得無須再蒐集特定資訊或執行特別措施以瞭解業務往來關係之目的及其性質。

電子支付機構應依重要性及風險程度，對現有使用者進行使用者審查，並於考量前次執行使用者審查之時點及所獲得資料之適足性後，在適當時機對已存在之往來關係進行審查。

第七條

電子支付機構確認使用者身分作業應自行辦理，如法令或主管機關另有規定電子支付機構得依賴第三方執行辨識及驗證使用者本人或代表人身分、代理人身分、實質受益人身分或業務關係之目的及性質時，該依賴第三方之電子支付機構仍應負確認使用者身分之最終責任，並應符合下列規定：

一、應能立即取得確認使用者身分所需資訊。

二、應採取符合電子支付機構本身需求之措施，確保所依賴之第三方將依電子支付機構之要求，毫不延遲提供確認使用者身分所需之使用者身分資料或其他相關文件影本。

三、確認所依賴之第三方受到規範、監督或監控，並有適當措施遵循確認使用者身分及紀錄保存之相關規範。

四、確認所依賴之第三方之所在地，其防制洗錢及打擊資恐規範與防制洗錢金融行動工作組織所定之標準一致。

第八條

電子支付機構對使用者之姓名及名稱檢核，應依下列規定辦理：

一、應依據風險基礎方法，建立使用者之姓名及名稱檢核政策及程序，以偵測、比對、篩檢使用者、第三類電子支付帳戶非個人使用者之高階管理人員或第三類電子支付帳戶非個人使用者實質受益人是否為資恐防制法指定制裁之個人、法人或團體，以及外國政府或國際組織認定或追查之恐怖分子或團體。

二、電子支付機構就第四條第一款第一目之確認方式，應對於使用者於建立業務關係時自行填寫之姓名欄位，進行輸入資料之系統檢核，如有符號、數字、連續三疊字或特殊關鍵字等，應進一步採取身分確認檢核措施，以防止使用者使用假名。

三、使用者之姓名及名稱檢核政策及程序，至少應包括比對與篩檢邏輯、檢核作業之執行程序，以及檢視標準，並將其書面化。

四、執行姓名及名稱檢核情形應予記錄，並依第十三條規定之期限進行保存。

本檢核機制應予測試，且依據測試結果確認是否仍能妥適反映風險並適時修訂。

第九條

電子支付機構對帳戶或交易之持續監控，應依下列規定辦理：

一、逐步以資訊系統整合公司使用者之基本資料及交易資料，進行基於防制洗錢及打擊資恐目的之查詢，以強化其帳戶或交易監控能力。對於各單位調取及查詢使用者之資料，應建立內部控制程序，並注意資料之保密性。

二、依據風險基礎方法，建立帳戶或交易監控政策與程序，並利用資訊系統，輔助發現疑似洗錢或資恐交易。

三、依據防制洗錢與打擊資恐法令規範、其使用者性質、業務規模及複雜度、內部與外部來源取得之洗錢與資恐相關趨勢與資訊、電子支付機構內部風險評估結果等，檢討其帳戶或交易監控政策及程序，並定期更新之。

四、電子支付機構之帳戶或交易監控政策及程序，至少應包括完整之監控型態、參數設定、金額門檻、預警案件與監控作業之執行程序與監控案件之檢視程序及申報標準，並將其書面化。

五、前款完整之監控型態參附錄所示。電子支付機構就電子支付帳戶間款項移轉，應將收受兩端之所有資訊納入監考量，以判定是否申報疑似洗錢或資恐交易。

六、電子支付機構對於前款規定之監控型態或其他經認定有疑似洗錢或資恐交易者，不論交易金額多寡，均應向法務部調查局申報。交易未完成者，亦同。

七、電子支付機構自發現並確認疑似洗錢或資恐交易之日起十個營業日內，向法務部調查局辦理申報。

八、執行帳戶或交易持續監控之情形應予紀錄，並依相關法令規定之期限進行保存。

疑似洗錢或資恐交易申報程序：

一、各單位承辦人員發現異常交易，應立即陳報督導主管。

二、督導主管應儘速裁決是否確屬應行申報事項。如裁定應行申報，應立即交由原承辦人員填寫申報書（格式請至法務部調查局網站下載）。

三、將申報書呈經單位主管核定後轉送專責人員。

四、由專責人員簽報專責主管核定後，立即向法務部調查局申報。

五、如屬明顯重大緊急之疑似洗錢或資恐交易案件之申報，應立即以傳真或其他可行方式儘速向法務部調查局申報，並立即補辦書面資料。但經法務部調查局以傳真資料確認回條（格式請至法務部調查局網站下載）確認收件者，無需補辦申報書。電子支付機構並應留存傳真資料確認回條。

防止申報資料及消息洩露之保密規定：

一、依前項規定申報之事項，各級人員應保守秘密，不得任意洩露。

二、本申報事項有關之文書，均應以機密文件處理，如有洩密案件應依有關規定處理。

三、專責人員及主管、法令遵循單位人員或稽核單位人員為執行職務需要，得即時取得使用者資料與交易紀錄，惟仍應遵循保密之規定。

第十條

對與境外機構合作或協助境外機構於我國境內從事電子支付機構業務相關行為者，應訂有一定政策及程序，至少包括：

一、蒐集足夠之可得公開資訊，以充分瞭解該境外機構之業務性質，並評斷其商譽及管理品質，包括是否遵循防制洗錢及打擊資恐之規範。

二、評鑑該境外機構對防制洗錢及打擊資恐具備相當之控管政策及執行效力。

三、電子支付機構在與境外機構合作或協助境外機構於我國境內從事電子支付業務相關行為前，應先取得內部業務主管層級人員核准後始得辦理。

四、以文件證明各自對防制洗錢及打擊資恐之責任作為。

第十一條

電子支付機構於推出新產品或服務或辦理新種業務（包括新支付機制、運用新科技於現有或全新之產品或業務）前，應進行產品之洗錢及資恐風險評估，並建立相應之風險管理措施以降低所辨識之風險。

第十二條

對達一定金額以上之通貨交易，應依下列規定辦理：

一、應確認使用者身分並留存相關紀錄憑證。

二、電子支付機構確認使用者身分措施，應依下列規定辦理：

(一) 憑使用者提供之身分證明文件或護照確認其身分，並將其姓名、出生年月日、電話、交易帳戶號碼、交易金額及身分證明文件號碼等事項加以記錄。但如能確認使用者為交易帳戶本人者，可免確認身分，惟應於交易紀錄上敘明係本人交易。

(二) 交易如係由代理人為之者，應憑代理人提供之身分證明文件或護照確認其身分，並將其姓名、出生年月日、電話、交易帳戶號碼、交易金額及身分證明文件號碼等事項加以記錄。

三、應於交易完成後五個營業日內以媒體申報方式（格式請至法務部調查局網站下載），向法務部調查局申報。無法以媒體方式申報而有正當理由者，得報經法務部調查局同意後，以書面（格式請至法務部調查局網站下載）申報之。

四、向調查局申報資料及相關紀錄憑證之保存，應依第十三條規定辦理。

第十三條

電子支付機構應以紙本或電子資料保存與使用者往來及交易之紀錄憑證，並依下列規定辦理：

一、對國內外交易之所有必要紀錄之保存應至少保存五年。但法律另有較長保存期間規定者，從其規定。前述必要紀錄應依「電子支付機構使用者身分確認機制及交易限額管理辦法」第二十一條規定留存。

二、對達一定金額以上通貨交易，其確認紀錄及申報之相關紀錄憑證，以原始方式至少保存五年。確認使用者程序之紀錄方法，由電子支付機構依本身考量，根據全公司一致性做法之原則，選擇一種紀錄方式。

- 三、對疑似洗錢或資恐交易之申報，其申報之相關紀錄憑證，以原始方式至少保存五年。
- 四、下列資料應保存自電子支付帳戶終止或一定金額以上通貨交易結束後，至少五年。但法律另有較長保存期間規定者，從其規定：
- (一) 確認使用者身分所取得之所有紀錄，如護照、身分證、駕照或類似之官方身分證明文件影本或紀錄。
 - (二) 電子支付帳戶檔案。
 - (三) 業務往來資訊，包括對複雜、異常交易進行詢問所取得之背景或目的資訊與分析資料。
- 五、電子支付機構保存之交易紀錄應足以重建個別交易，以備作為認定不法活動之證據。
- 六、電子支付機構對權責機關依適當授權要求提供交易紀錄及確認使用者身分等相關資訊時，應確保能夠迅速提供。

第十四條

專責主管及專責人員：

- 一、專營之電子支付機構應依其規模、風險等配置適足之防制洗錢及打擊資恐專責人員及資源，並由董（理）事會指派高階主管一人擔任專責主管，賦予協調監督防制洗錢及打擊資恐之充分職權，及確保該等人員及主管無與其防制洗錢及打擊資恐職責有利益衝突之兼職。
- 二、前款專責主管掌理下列事務：
 - (一) 督導洗錢及資恐風險之辨識、評估及監控政策及程序之規劃與執行。
 - (二) 協調督導全面性洗錢及資恐風險辨識及評估之執行。
 - (三) 監控與洗錢及資恐有關之風險。
 - (四) 發展防制洗錢及打擊資恐計畫。

(五) 協調督導防制洗錢及打擊資恐計畫之執行。

(六) 確認防制洗錢及打擊資恐相關法令之遵循，包括所屬金融同業公會所定並經金管會准予備查之相關範本或自律規範。

(七) 督導向法務部調查局進行疑似洗錢及資恐交易申報及資恐防制法指定對象之財物或財產上利益及其所在地之通報事宜。

三、第一款專責主管應至少每半年向董（理）事會及監察人（監事、監事會）或審計委員會報告，如發現有重大違反法令時，應即時向董（理）事會及監察人（監事、監事會）或審計委員會報告。

四、專營之電子支付機構國外營業單位應綜合考量在當地之分公司家數、業務規模及風險等，設置適足之防制洗錢及打擊資恐人員，並指派一人為主管，負責防制洗錢及打擊資恐之協調督導事宜。

五、專營之電子支付機構國外營業單位防制洗錢及打擊資恐主管之設置應符合當地法令規定及當地主管機關之要求，並應具備協調督導防制洗錢及打擊資恐之充分職權，包括可直接向第一款專責主管報告，且除兼任法令遵循主管外，應為專任，如兼任其他職務，應與當地主管機關溝通，以確認其兼任方式無利益衝突之虞，並報金管會備查。

六、兼營之電子支付機構對於涉及專責主管及專責人員相關規定，應依本業有關之規定辦理。

第十五條

防制洗錢及打擊資恐內部控制制度之執行、稽核及聲明：

一、專營之電子支付機構國內外營業單位應指派資深管理人員擔任督導主管，負責督導所屬營業單位執行防制洗錢及打擊資恐相關事宜，及依「電子支付機構內部控制及稽核制度實施辦法」相關規定辦理自行查核之情形。

二、專營之電子支付機構內部稽核單位應依「電子支付機構內部控制

及稽核制度實施辦法」規定辦理下列事項之查核，並提具查核意見：

- (一) 洗錢及資恐風險評估與防制洗錢及打擊資恐計畫是否符合法規要求並落實執行。
- (二) 防制洗錢及打擊資恐計畫之有效性。

三、專營之電子支付機構內部稽核單位之職責：

(一) 應依據所訂內部管制措施暨有關規定訂定查核事項，定期辦理查核，並測試防制洗錢及打擊資恐計畫之有效性及風險管理品質。

(二) 查核方式應涵蓋獨立性交易測試，包括就電子支付機構評估之高風險產品、使用者及地域，篩選有關之交易，驗證已有效執行防制洗錢及打擊資恐相關規範。

(三) 發現執行該項管理措施之疏失事項，應定期簽報專責主管陳閱，並提供員工在職訓練之參考。

(四) 查獲故意隱匿重大違規事項而不予揭露者，應由總公司權責單位適當處理。

四、專營之電子支付機構總經理應督導各單位審慎評估及檢討防制洗錢及打擊資恐內部控制制度執行情形，由董（理）事長（主席）、總經理、稽核人員、防制洗錢及打擊資恐專責主管聯名出具防制洗錢及打擊資恐之內部控制制度聲明書，並提報董（理）事會通過，於每會計年度終了後三個月內將該內部控制制度聲明書內容揭露於電子支付機構網站，並於金管會指定網站辦理公告申報。

五、兼營之電子支付機構對於涉及內部控制制度之執行、稽核及聲明相關規定，應依本業有關之規定辦理。

第十六條

員工任用及訓練：

一、專營之電子支付機構應建立審慎適當之員工遴選及任用程序，包括檢視員工是否具備廉正品格，及執行其職責所需之專業知識。

二、專營之電子支付機構之防制洗錢及打擊資恐專責主管、專責人員及國內營業單位督導主管應於充任後三個月內符合下列資格條件之一，電子支付機構並應訂定相關控管機制，以確保符合規定：

(一) 曾擔任專責之法令遵循或防制洗錢及打擊資恐專責人員三年以上者。

(二) 參加金管會認定機構所舉辦二十四小時以上課程，並經考試及格且取得結業證書者。但已符合法令遵循人員資格條件者，經參加金管會認定機構所舉辦十二小時防制洗錢及打擊資恐之教育訓練後，視為具備本目資格條件。

(三) 取得金管會認定機構舉辦之國內或國際防制洗錢及打擊資恐專業人員證照者。

三、前款人員於中華民國一百零六年六月三十日前充任者，依下列各目之一符合所列資格條件，視為符合資格：

(一) 於一百零六年六月三十日前符合前款第一目或第三目資格條件。

(二) 於下列期限內符合前款第二目資格條件：

1、電子支付機構防制洗錢及打擊資恐專責主管、專責人員於一百零六年十二月三十一日前。

2、電子支付機構之國內營業單位督導主管於充任後一年內。

四、專營之電子支付機構之防制洗錢及打擊資恐專責主管、專責人員及國內營業單位督導主管，每年應至少參加經第十四條第一款專責主管同意之內部或外部訓練單位所辦十二小時防制洗錢及打擊資恐教育訓練，訓練內容應至少包括新修正法令、洗錢及資恐風險趨勢及態樣。當年度取得金管會認定機構舉辦之國內或國際防制洗錢及打擊資恐專業人員證照者，得抵免當年度之訓練時數。

五、專營之電子支付機構國外營業單位之督導主管與防制洗錢及打擊資恐主管、人員應具備防制洗錢專業及熟知當地相關法令規定，且每年應至少參加由國外主管機關或相關單位舉辦之防制洗錢及打擊資恐教育訓練課程十二小時，如國外主管機關或相關單位未舉辦防制洗錢及打擊資恐教育訓練課程，得參加經第十四條第一款專責主管同意之內部或外部訓練單位所辦課程。

六、專營之電子支付機構董（理）事、監察人、總經理、法令遵循人員、內部稽核人員及業務人員，應依其業務性質，每年安排適當內容及時數之防制洗錢及打擊資恐教育訓練，以使其瞭解所承擔之防制洗錢及打擊資恐職責，及具備執行該職責應有之專業。

員工有下列情形之一者，應對其經辦事務予以抽查，必要時可洽請稽核單位協助：

一、員工奢侈之生活方式與其薪資所得顯不相當。

二、員工已排定休假而無故不休假。

三、員工無法合理解釋其自有帳戶之大額資金進出。

員工有下列對防制洗錢或打擊資恐有功之具體事蹟者，應給予適當獎勵：

一、員工發現有疑似洗錢或資恐案件，並依據洗錢防制相關規定申報，對檢警單位防範或偵破犯罪有貢獻者。

二、員工參加國內外防制洗錢或打擊資恐相關業務講習，成績優良或蒐集國外法令研提對防制洗錢或打擊資恐活動具有價值之資料者。

職前及在職訓練得採下列方式辦理：

一、職前訓練：新進員工訓練至少應安排若干小時以上有關洗錢防制、資恐防制法令及金融從業人員法律責任訓練課程，使新進員工瞭解相關規定及責任。

二、在職訓練：

(一) 初期之法令宣導：於洗錢防制法、資恐防制法施行或修正後，應於最短期間內對員工實施法令宣導，介紹洗錢防制法、資恐防制法及其有關法令，並講解電子支付機構之相關配合因應措施，有關事宜由專責主管負責規劃後，交由員工訓練單位負責辦理。

(二) 平時之在職訓練：

- 1、員工訓練部門應每年定期舉辦有關之訓練課程提供員工研習，以加強員工之判斷力，落實防制洗錢及打擊資恐之功能，並避免員工違法，本訓練得於其他專業訓練班中安排適當之有關課程。
- 2、有關訓練課程除由電子支付機構培訓之講師擔任外，並得視實際需要延聘學者專家擔綱。
- 3、訓練課程除介紹相關法令之外，並應輔以實際案例，使員工充分瞭解洗錢及資恐之特徵及類型，俾助於發覺「疑似洗錢或資恐之交易」。
- 4、專責主管應定期瞭解員工參加訓練之情形，對於未曾參加者，應視實際需要督促其參加有關之訓練。
- 5、除內部之在職訓練外，電子支付機構亦得選派員工參加外部訓練機構所舉辦之訓練課程。

三、專題演講：為更充實員工對洗錢防制法及資恐防制法令之認識，電子支付機構得舉辦專題講座，邀請學者專家蒞公司演講。

四、兼營之電子支付機構對於涉及員工任用及訓練相關規定，應依本業有關之規定辦理。

第十七條

其他應注意事項：

一、使用者有下列情形應婉拒服務，並報告直接主管：

- (一) 當被告知依法必須提供相關資料確認身份時，堅不提供相關資料。
- (二) 使用者強迫或意圖強迫電子支付機構員工不得將交易紀錄或申報表格建檔。
- (三) 意圖說服員工免去完成該交易應填報之資料。
- (四) 探詢逃避申報之可能性。
- (五) 使用者之描述與交易本身顯不吻合。
- (六) 意圖提供利益於員工，以達到電子支付機構提供服務之目的。

二、專營之電子支付機構兼營其他業務時，該兼營部門亦應適用與該業務有關之防制洗錢及打擊資恐注意事項範本，如電子支付機構兼營電子票證業務，該電子票證部門即應適用電子票證發行機構防制洗錢及打擊資恐注意事項範本。

第十八條

電子支付機構應參酌本範本訂定其注意事項，經電子支付機構董（理）事會通過後實施，並呈報金管會備查；並應每年檢討。修正時亦同。

第十九條

本範本應經本會理事會議通過，及報奉金管會備查後實施；修正時，亦同。