附件

「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」

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
金融監督管理委員會 109 年 01 月 02 日
金管銀票字第 1080139395 號函准予備查

一、本指引依「銀行業及其他經金融監督管理委員會指定之金融機構防制洗錢及打擊資恐內部控制與稽核制度實施辦法」訂定，以防制洗錢及打擊資恐為目的，內容涵括我國電子支付機構如何辨識、評估各項業務之洗錢及資恐風險，以及制訂防制洗錢及打擊資恐計畫等面向，作為執行之依據。

二、電子支付機構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。其內容並應包括對洗錢及資恐風險進行辨識、評估、管理與相關書面政策、程序之訂定，以及依據風險評估結果而訂定之防制洗錢及打擊資恐計畫，並定期檢討。

以風險為基礎之方法（risk-based approach）旨在協助發展與洗錢及資恐風險相當之防制與抵減措施，以利電子支付機構決定其防制洗錢及打擊資恐資源之配置、建置其內部控制制度、以及訂定和執行防制洗錢及打擊資恐計畫應有之政策、程序及控管措施。

本指引所舉例之各項說明並非強制性規範，電子支付機構之風險評估機制應與其業務性質及規模相當。對較小型或業務較單純之電子支付機構，簡單之風險評估即足夠；惟對於產品與服務較複雜之電子支付機構、有多家分公司（或子公司）提供廣泛多樣之產品、或其使用者群較多元者，則需進行較高度的風險評估程序。

三、電子支付機構應採取合宜措施以識別、評估其洗錢及資恐風險，並依據所辨識之風險訂定具體的風險評估項目，以進一步管控、降低或預防該風險。

具體的風險評估項目應至少包括地域、使用者、產品及服務、交易或支付管道等面向，並應進一步分析各風險項目，以訂定細部的風險因素。

（一）地域風險：

1、 電子支付機構應識別具較高洗錢及資恐風險的區域。

2、 於訂定高洗錢及資恐風險之區域名單時，電子支付機構得依據其各分公司（或子公司）的實務經驗或參照附錄，並考量個別需求，以選擇適用之參考依據。

（二）使用者風險：

1、 電子支付機構應綜合考量個別使用者背景、職業與社會經濟活動特性、地域、以及非個人使用者之組織型態與架構等，以識別該使用者洗錢及資恐風險。

2、 於識別個別使用者風險並決定其風險等級時，電子支付機構得依據以下風險因素為評估依據：

（1）使用者之地域風險：依據電子支付機構所定義之洗錢及資恐風險的區域名單，決定使用者國籍與居住國家的風險評分。

（2）第三類電子支付帳戶使用者職業與行業之洗錢風險：依據電子支付機構所定義之各職業與行業的洗錢風險，決定使用者職業與行業的風險評分。高風險行業如從事密集性現金交易業務、或屬易被運用於持有個人資產之公司或信託等。

（3）使用者申請註冊之管道。

（4）電子支付帳戶類型之交易限額。

（5）使用者是否有其他高洗錢及資恐風險之表徵，如使用者為未持有居留證之外國人及無戶籍之國民且無法提出合理說明、

使用者為具隱名股東之公司或可發行無記名股票之公司、法人使用者之股權複雜度，如股權架構是否明顯異常或相對其業務性質過度複雜等。

（三）產品及服務、交易或支付管道風險：

1、 應依據個別產品與服務、交易或支付管道的性質，識別可能會為其帶來較高的洗錢及資恐風險者。

2、 應於新產品、新服務或使用通路上線前，進行全面洗錢風險評估，並按照風險控制原則，建立相應風險管理措施以降低所辨識之風險。

3、 個別產品與服務、交易或支付管道之風險因素舉例如下：

（1）不容易追查資金來源或難以做身分辨識。

（2）容易套現程度。

（3）是否為高金額之金錢或價值移轉業務。

（4）匿名交易。

（5）收到款項來自於未知或無關係之第三者。

四、電子支付機構應建立不同之使用者風險等級與分級規則。

就使用者之風險等級，至少應有兩級（含）以上之風險級數，即「高風險」與「一般風險」兩種風險等級，作為加強使用者審查措施及持續監控機制執行強度之依據。若僅採行兩級風險級數之電子支付機構，因「一般風險」等級仍高於本指引第五點與第七點所指之「低風險」等級，故不得對「一般風險」等級之使用者採取簡化措施。

電子支付機構不得向使用者或與執行防制洗錢或打擊資恐義務無關者，透露使用者之風險等級資訊。

五、除外國政府之重要政治性職務人士與受經濟制裁、外國政府或國際洗錢防制組織認定或追查之恐怖分子或團體，及依資恐防制法指定制裁

之個人、法人或團體，應直接視為高風險使用者外，電子支付機構得依自身之業務型態及考量相關風險因素，訂定應直接視為高風險使用者之類型。

電子支付機構得依據完整之書面風險分析結果，自行定義可直接視為低風險使用者之類型，而書面風險分析結果須能充分說明此類型使用者與較低之風險因素相稱。

六、對於新申請註冊的使用者，電子支付機構應在接受註冊後六十天內確定其風險等級。

對於已確定風險等級之既有使用者，電子支付機構應依據其風險評估政策及程序，重新進行使用者風險評估。

雖然電子支付機構在接受註冊時已對使用者進行風險評估，但就某些使用者而言，必須待使用者透過帳戶進行交易，其全面風險狀況才會變得明確，爰此，電子支付機構應依重要性及風險程度，對現有使用者身分資料進行審查，並於考量前次執行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及適時調整使用者風險等級。上開適當時機至少應包括：

（一）使用者申請新增電子支付帳戶時。

（二）依據使用者之重要性及風險程度所定之定期審查時點。

（三）得知使用者身分與背景資訊有重大變動時。

（四）經申報疑似洗錢或資恐交易時，可能導致使用者風險狀況發生實質變化的事件發生時。

電子支付機構應定期檢視其辨識使用者身分所取得之資訊是否足夠，並確保該等資訊之更新，特別是高風險客戶，電子支付機構應至少每年檢視一次。

七、電子支付機構應依據已識別之風險，建立相對應的管控措施，以降低或預防該洗錢風險；電子支付機構應依據使用者的風險程度，決定不

同風險等級使用者所適用的管控措施。

對於風險之管控措施，應由電子支付機構依據其風險防制政策、監控及程序，針對各類型之高風險使用者與具特定高風險因子之使用者採取不同的管控措施，以有效管理和降低已知風險，舉例說明如下：

（一）進行加強使用者審查措施（Enhanced Due Diligence），例如：

1、 取得申請註冊與往來目的之相關資料：如電子支付帳戶用途、預期的使用者交易活動等資料。

2、 取得使用者進一步之商業資訊：瞭解使用者業務往來資訊。

3、 取得將進行或已完成交易之說明與資訊。

4、 依據使用者型態進行實地或電話訪查，以確認使用者之實際營運情形。

（二）取得較高管理階層之核准。

（三）增加進行使用者審查之頻率。

（四）加強之監控機制。

對於低風險情形，得由電子支付機構依據其風險防制政策、監控及程序，採取簡化措施。

八、電子支付機構應建立定期之全面性洗錢及資恐風險評估作業並製作風險評估報告，使管理階層得以適時且有效地瞭解電子支付機構所面對之整體洗錢與資恐風險、決定應建立之機制及發展合宜之抵減措施。

電子支付機構應依據下列指標，建立定期且全面性之洗錢及資恐風險評估作業：

（一）業務之性質、規模、多元性及複雜度。

（二）目標市場。

（三）電子支付機構交易數量與規模：考量電子支付機構一般交易活動與其使用者之特性等。

（四）高風險相關之管理數據與報告：如高風險使用者之數目與比例；

高風險產品、服務或交易之金額、數量或比例；使用者之國籍、註冊地或營業地、或交易涉及高風險地域之金額或比例等。

（五）業務與產品，包含提供業務與產品予使用者之管道及方式、執行使用者審查措施之方式，如資訊系統使用的程度以及是否委託第三人執行審查等。

（六）內部稽核與監理機關之檢查結果。

電子支付機構於進行前項之全面性洗錢及資恐風險評估作業時，除考量上開指標外，建議輔以其他內部與外部來源取得之資訊，如：

（一）電子支付機構內部管理階層（如事業單位主管、使用者關係經理等）所提供的管理報告。

（二）國際防制洗錢組織與他國所發布之防制洗錢及打擊資恐相關報告。

（三）主管機關發布之洗錢及資恐風險資訊。

電子支付機構之全面性洗錢及資恐風險評估結果應做為發展防制洗錢及打擊資恐計畫之基礎；電子支付機構應依據風險評估結果分配適當人力與資源，採取有效的反制措施，以預防或降低風險。

電子支付機構有重大改變，如發生重大事件、管理及營運上有重大發展、或有相關新威脅產生時，應重新進行評估作業。

完成或更新風險評估報告時，電子支付機構應將風險評估報告送金融監督管理委員會（以下稱金管會）備查；兼營電子支付機構應併同本業有關處理之規定辦理。