

數位發展部數位產業署
提供第三方支付服務之事業或人員落實涉詐客戶認定及控管
措施指引手冊

壹、目的

數位發展部為強化打擊詐欺犯罪與防制洗錢，依詐欺犯罪危害防制條例（以下稱本條例）及第三方支付服務業疑似涉詐客戶認定及控管措施處理辦法（以下稱本辦法），建立提供第三方支付服務之事業或人員（以下稱第三方支付服務業者）落實涉詐客戶認定及控管措施指引手冊（以下稱本指引）。

本指引適用對象為我國境內通過提供第三方支付服務之事業或人員洗錢防制及服務能量登錄之第三方支付服務業者。

本指引為行政指導，旨在使第三方支付服務業者依循本辦法第3條訂定防詐內部措施時參考，確保第三方支付服務業者於訂定疑似涉及詐欺犯罪客戶之態樣、訂定防詐內部措施之預警規範及確認程序時及對高風險業務關係者採取之必要強化管理措施，可切合其防止詐騙之法遵義務，進一步強化第三方支付服務業者管理規範，保障使用者財產安全。

貳、疑似涉詐客戶認定之態樣：

第三方支付服務業者依本辦法第3條第1項第1款規定，綜合考量客戶商業模式、業務規模與交易方式、所屬產業被利用於詐欺之風險及民眾通報可疑交易等因素，訂定疑似涉詐客戶認定之態樣時，應包括但不限於下列態樣：

一、第三方支付服務交易類：

- (一) 第三方支付帳號久未往來，突有異常交易者。
- (二) 第三方支付帳號甫開立後，即有多筆頻繁交易者。
- (三) 第三方支付帳號常有頻繁不正常之退款作業者。
- (四) 經常有買方客戶反應交易糾紛者。

(五) 信用卡爭議款比例過高者。

二、客戶身分資訊及第三方支付帳號類：

(一) 疑似使用匿名、假名、人頭、虛設行號等往來或使用服務者。

(二) 使用他人資訊開立帳號、第三方支付帳號連結他人信用卡、多數帳號連結同一銀行帳戶者。

(三) 賣方客戶提供之商品網頁使用一頁式網頁、或所提供之網頁無商品資訊者。

(四) 帳號持有人短期間內頻繁申請開立第三方支付帳號，且無法提出合理說明者。

(五) 其他經主管機關或第三方支付服務業者透過產業聯防平臺通知為疑似詐欺或顯屬異常交易之賣方客戶。

參、詐欺風險評估及疑似涉詐通報流程

第三方支付服務業者依本辦法第3條第1項第2款規定訂定防詐內部措施之預警規範及確認程序，其內容應包括疑似涉詐客戶之認定標準、預警規範及確認程序、對高風險業務關係者所採取之必要強化管理措施，並應定期檢查執行狀況，作成評估報告。

一、訂定預警規範及確認程序（本辦法第3條第1項第2款）：

第三方支付服務業者應參考本指引有關疑似涉詐客戶認定之態樣，採取適當作為以辨識、評估及了解詐欺風險，至少涵蓋客戶、服務、交易及支付管道，訂定防詐內部措施之預警規範及確認程序。

二、高風險業務關係者必要強化管理措施（本辦法第3條第1項第3款）：

第三方支付服務業者應按前述辨識、評估及了解詐欺風險後，針對高風險客戶採行必要之強化管理措施。

三、強化確認客戶身分及客戶持續審查措施（本辦法第4條）：

第三方支付服務業者就疑似涉詐客戶，應強化確認客戶身分，採行下列之措施：

- (一) 要求客戶提供足資驗證其身分及資金來源之佐證資料。
- (二) 採用實地訪查、視訊或語音通話等方式確認客戶狀態。
- (三) 使用金融機構或其他可信賴來源所提供資訊以交互比對確認客戶身分。

第三方支付服務業者除依上述措施辦理外，並得採取下列措施對客戶身分持續審查：

- (一) 確認客戶所進行之交易內容與其業務相符，必要時並應瞭解其資金來源或確認其交易為實質交易。
- (二) 檢視其辨識客戶身分所取得之資訊是否充足，並確保該等資訊之即時性、真實性及妥適性。
- (三) 持續確認客戶之交易或帳號之運作方式是否有涉及詐欺之虞。

四、拒絕建立業務關係或延後撥款：

第三方支付服務業者就疑似涉詐客戶，如有以下情形之一者，得依本辦法第5條規定拒絕建立業務關係或提供服務：

- (一) 拒絕配合客戶身分確認程序或提供確認客戶身分措施相關文件者。
- (二) 疑似使用匿名、假名、人頭、虛設行號或虛設法人團體名義往來或使用服務者。
- (三) 持用偽、變造身分證明文件者。
- (四) 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者。
- (五) 不尋常拖延應補充之身分證明文件、登記證照或其他核准文件者。

依本辦法第6條規定，若有拒絕配合確認客戶身分程序，或經查證有涉及詐欺犯罪之情事者，第三方支付服務業者得對其帳號內交易款項延後撥款或暫停提供服務。延後撥款或暫停提供服務之期間不得少於二十日。

五、通報司法警察機關及通知同業業者程序（本辦法第7條、第8條）：

第三方支付服務業者認定其客戶疑似涉及詐欺犯罪，並執行上述程序及措施後，得將疑似涉詐客戶相關資料儘速通報該客戶所在地之司法警察機關；並得以書面或電子方式（聯防平臺）通知同業業者。

(一) 通報司法警察機關流程：

1. 郵寄或傳送至司法警察機關指定之收件地址或電子信箱。
2. 使用司法警察機關指定之網站進行通報。

(二) 通知同業業者。

六、通報司法警察機關後之延後撥款及後續控管程序：

第三方支付服務業者對於疑似涉詐客戶延後撥款，並通報司法警察機關之處理方式：

(一) 司法警察機關應於接獲通報後二十日內通知第三方支付服務業者就延後撥款辦理後續控管或解除控管（本辦法第9條第1項）。

(二) 重大緊急案件，司法警察機關得以電話、傳真、電子郵件或其他可行方式先行通知，並應於通知後五個營業日內補辦公文書資料送達第三方支付服務業者（本辦法第9條第2項）。

(三) 第三方支付服務業者依規定辦理後續控管，應依司法警察機關指定二年以下之控管期間，就疑似涉詐客戶之帳戶內交易款項延後撥款，並暫停提供服務（本辦法第9條第3項）。

(四) 第三方支付服務業者接獲司法警察機關之通報，應立即查詢該帳號相關交易，如發現通報之詐欺款項已撥款，應將該筆款項轉出之資料及原通報機關名稱，通知該筆款項之受款銀行及原通報機關。第三方支付服務業者接獲金融機構疑似涉詐帳號之通知者，適用之（本辦法第10條）。

(五) 第三方支付服務業者接獲司法警察機關通報後，應將警示涉詐帳號內交易款項延後撥款或暫停提供服務，控管期限自司

法警察機關通報時起算，逾二年自動失其效力。但有繼續控管之必要者，原通報機關應於期限屆滿前再行通報之，通報延長以一次及一年為限（本辦法第11條）。

七、解除控管之申訴處理程序（本辦法第12條）：

第三方支付服務業者經司法警察機關通報解除控管，或控管期限屆滿者，第三方支付服務業者應解除該帳號之控管。

(一) 第三方支付服務業者之客戶認為其帳號非「警示涉詐帳號」或「帳號涉及詐欺犯罪之情形已不存在時」，得檢具事證以書面向司法警察機關申訴，司法警察機關應將申訴處理結果通知申請人，並副知第三方支付服務業者。

(二) 第三方支付服務業者之客戶認為其帳號非「疑似涉詐帳號」或「帳號涉及詐欺犯罪之情形已不存在時」，得檢具事證以書面向第三方支付服務業者申訴，第三方支付服務業者查證屬實，應通報司法警察機關建議解除控管。

肆、涉及詐欺犯罪客戶確認身分資料及交易紀錄保存（本辦法第13條）

第三方支付服務業者就其客戶疑似涉及詐欺犯罪，執行以上程序及措施後，應將疑似涉詐客戶其確認身分程序所得資料及交易紀錄予以保存。

一、所有交易紀錄（至少保存五年。法律有較長保存期間規定從其規定）

(一) 網路實質交易相關資訊（交易日期、交易類型、金額與種類）。

(二) 付款方與受款方之身分資訊。

(三) 代理收付資金之存入及撥款方式。

(四) 身分驗證之方式。

(五) 對疑似涉詐客戶與其可疑交易進行通知及通報之相關紀錄。

二、客戶資料（至少保存至與客戶結束業務關係後五年）

- (一) 確認客戶身分所取得之所有紀錄。
- (二) 帳戶、帳號資料、支付證明或契約文件檔案等。
- (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及分析資料。

保存之交易紀錄應能重建個別交易，而客戶資料之紀錄足資辨識該客戶之所有資訊，以備作為認定詐欺犯罪之證據；另對主管機關要求提供代理收付之紀錄及確認客戶身分等相關資訊時，應確保即時提供，不得以隱碼之方式遮蔽相關資訊。