财经与管理·第 03 卷·第 04 期·2019 年 08 月
DOI: https://doi.org/10.26549/cjygl.v3i4.2008

Analysis on the Causes of Money Laundering Risk, Suspicious Transaction Pattern and Countermeasures of Non-bank Payment Institutions

Zhongyuan Zhang

Operations Office, The People's Bank of China, Beijing, 100045, China

Abstract

In recent years, non-bank payment institutions have developed rapidly due to their convenience, low cost and high efficiency. While bringing convenience to the public, it has gradually become a fertile ground for money laundering crimes due to weak real names and concealment, the particularity of transaction mode, difficulty in tracking funds, and defects in management systems and technology monitoring. With the use of non-bank payment platforms, illegal transfer of funds, fund-raising fraud, fictitious transactions, malicious cash-out, illegal gambling and other illegal activities and cases continue to surge, money laundering techniques emerge in endlessly, which poses a great challenge to the supervision of compliance of non-bank payment institutions. Through the analysis of the money laundering risk and suspicious transaction behavior of payment institutions, this paper puts forward some policy suggestions for the prevention and control of money laundering risk.

Keywords

non-bank payment institution; money laundering risk; suspicious transaction

浅析非银行支付机构洗钱风险成因、可疑交易模式及应对措施

张钟元

中国人民银行营业管理部，中国·北京 100045

摘　要

近年来，非银行支付机构以其方便快捷、低廉高效的特点迅猛发展。其在为社会大众带来便利的同时，也因弱实名性和隐匿性、交易模式特殊性、资金难追踪性以及管理制度和技术监控上的缺陷等原因，逐渐成为洗钱犯罪的沃土。借助非银行支付平台的非法转移资金、集资诈骗、虚构交易、恶意套现、非法博彩等违法行为与案件不断激增，洗钱手法层出不穷，这对非银行支付机构合规监管提出较大挑战。本文通过分析支付机构的洗钱风险和可疑交易行为，为防控洗钱风险提出了政策建议。

关键词

非银行支付机构；洗钱风险；可疑交易

1 非银行支付机构洗钱风险分析

1.1 客户准入门槛低

目前，支付机构的客户准入多依靠线上非面对面形式完成，个人客户在注册互联网支付账户时，往往仅需要提供姓名、证件信息、联系地址、电子邮箱、手机号等简单的身份资料即可成功入网。单位客户、特约商户需要提供营业执照、法人证件信息、联系地址、手机号等信息。而支付机构合规理念尚不健全，客户身份识别基础性工作普遍较差，在以盈利为目的的驱使下，疏于对客户提交信息真实性的核对和审查。多数机构在客户准入方面，违反反洗钱和支付结算有关规定，未按有关程序核实客户信息，与未在工商注册、公司主体已经注销吊销、ICP 无理由不备案等不明身份的客户，或身份异常的客户建立业务关系，并为其提供服务。大量的匿名、假名、身份不明账户的存在，为不法分子利用支付账户进行非法资金转移与清洗提供通道，同时为案件调查、确认身份以及追踪非法资金增大难度，产生严重风险隐患。然而，监管部门也未能全面掌握支付账户开立的情况，支付机构与监管部门

之间没有建立有效的信息沟通机制，造成一定的监管滞后。

1.2 客户管理能力差

与客户建立业务关系后，支付机构疏于对客户的持续管理。存在不能批量查询和核验对公客户和特约商户身份和经营信息，系统无法提示证件有效期，没有有效措施确保客户更新身份信息，商户巡检、回访工作流于形式或只关注经营情况及设备故障等问题，导致大量身份异常的客户在存续期间未得到及时发现和处理，存在较多违规转接口或负面舆情的客户。甚至有的商户的备案网站已成为涉黄、涉毒等明显异常甚至违法的网站，但支付机构并未理睬或发现，大量的投诉举报也从侧面反映了支付机构对客户的风险识别和管控严重缺位。加之目前工商管理部门逐步弱化企业年检、经营范围管理，支付机构对商户的管理更难有效开展。同时，支付机构对持续识别、重新识别、客户风险等级划分等工作的要求不理解，执行不到位，导致其不能将不法分子资金拒之支付渠道外。

1.3 交易真实性难确定

非银行支付交易的载体主要是依托于互联网的应用，它提供了一个虚拟的、非面对面式的交易环境，通过互联网进行的交易，只要买卖双方自愿达成交易即可完成资金往来，不但买卖双方个人信息的真实性无法得知，支付机构在参与支付结算交易时，并不会对交易的背景、目的进行审查，也不对交易的真实性进行核实。因此无法确认是否经历了真实的商品交易，同时也无法验证交易金额与实际商品价值是否相符。

电商平台类客户伪造、变造电商网站及订单或物流等信息的成本很低，支付机构交易真实性审核难度和压力相对较大，从准入到交易的审核过程并不能完全保证交易的真实性。另外在跨境交易中，不收单场景下的购付汇业务是非银行支付平台跨境外汇支付业务的主要收入来源，支付机构可以凭借大量的不收单场景购付汇业务获取高额手续费，而反洗钱违规成本相对较低，这助长了支付机构怠于严格履职。

1.4 账户资金难追踪

作为非金融机构，支付机构打破了传统银行对交易双方资金划拨点对点的模式。支付指令由客户发出后通过支付机构传递给银行，银行收到指令后把客户虚拟账户中的资金划入支付账户，然后通过支付平台账户划入最终目标账户。非银行支付机构作为金融中介，割断了交易双方原本的直接联系，同时又能够整合不同银行之间的支付渠道，资金可以迅速地在不同银行账户之间进行流转[1]，屏蔽了银行对资金来源和去向的辨别。而付款人在支付款项时，显示的收款单位多为支付机构，而非特约商户，可能给付款人造成实际收款人即为支付机构的错觉。同时，网关支付、快捷支付、扫码支付、不记名预付卡支付等模式下，支付机构无法获取付款人姓名、银行账号等基本信息，不利于资金的完整记录和全程追踪，严重削弱监管部门和机构自身对资金的监控。

1.5 交易监测有效性低

可疑交易监测是预防洗钱的重要环节，监测标准的合理有效设计、监测系统的完整准确信息采集和人工的全面深入分析是金融情报是否有价值的重要因素。而支付机构监测标准设置简单、笼统，缺乏有效的指标设计，无法体现符合自身风险和业务特点的个性化要求。可疑交易监测系统未能充分采集各业务系统的交易信息，交易监测标准未能全面、准确通过系统实现或反馈，导致大量符合自定义监测标准的异常交易未被筛选和关注。针对系统筛出的可疑情形，支付机构欠缺专业的人工分析，没能有意识的运用客户身份识别结果，也没有结合客户经营背景判定交易的合理性，导致有关交易应排除未排除、应提交未提交情况的发生。可疑交易监测有效性低，为不法分子提供较多洗钱空间。

1.6 外包商转嫁风险

对于线下银行卡收单业务来说，绝大部分支付机构采用外包模式进行线下商户的拓展，在此过程中，需要由外包服务商对商户实际经营场所进行查访，并对商户的营业执照等资料进行初步识别及核验。部分支付机构的外包服务商还同时需要对商户进行回访及巡检。因此，外包服务商反而承担了客户尽职调查工作。然而，现行法律法规对于外包服务商缺乏相应的监管措施，部分支付机构虽与外包服务商签订履行身份识别等义务的相关协议，但实际操作中，商户实名制难以落实，商户的后续经营情况也难以监控，洗钱风险随义务转移给外包服务提供商，带来较大风险隐患。

1.7 名单监控难执行

支付机构大多都建立有独立的反洗钱黑名单数据库，除

财经与管理·第 03 卷·第 04 期·2019 年 08 月
DOI: https://doi.org/10.26549/cjygl.v3i4.2008

公安部发布的涉恐、红通等名单外，主要纳入的是业务中的违规商户名单，并非真正意义上的反洗钱名单监控。联合国安理会制裁名单获取和实时更新相对复杂，支付机构对名单监控义务尚不清晰，更难积极执行。虽市面上存在专业的反洗钱黑名单库可以购买，由于成本较高，大部分规模较小的支付机构不愿出资购买和维护。面对逐步放开的跨境支付业务，名单监控的疏忽将增大洗钱风险暴露。

2 可疑交易行为分析

支付机构因反洗钱交易监测分析工作起步较晚，与传统金融机构相比，监测指标的有效性不足，导致可疑交易报告上报数量较少、质量不高、成案率低。针对不同的支付业务，常见涉嫌洗钱的可疑交易行为列举如下。

2.1 互联网支付业务

互联网线上支付业务因其非面对面、效率高且无时空限制等交易特点，支付机构实施客户身份识别及尽职调查难度较大，成为了非法集资、网络赌博、电信诈骗等涉众犯罪活动资金快速汇集和转移的重要通道。比较典型的可疑交易方式有：一是虚构交易场景[2]，制作虚假电商购物网站，以“购物付款”方式转移赃款；二是个人购买、盗用他人身份或制作虚假身份开立支付账户，绕开交叉验证，规避交易额度，使不法资金在多个支付账户和银行账户间划转，将资金链条复杂化，b 从而掩盖违法资金去向；三是由于支付机构疏于客户管理，客户违规将支付接口出租借给违法实体，支付接口挪用又很难通过技术手段发现，导致电信诈骗、非法博彩、黄赌毒、非法期货及大宗商品等非法交易场景激增，不知情者认为资金打给支付机构特约商户参与投资，而不法分子跑路后，导致大量上访投诉；知情者以购买“游戏点卡”“虚拟商品”“充值”等为幌子，参与网络赌博等。

2.2 扫码支付业务

二维码支付业务的用户大部分为个人客户及小微商户，使用场景多为 C 扫 B。在此模式下，存在不经过实名认证即开通支付账户的情况以及“一证下机”的违规行为，客户审核不到位。在聚合支付业务中，拥有大量 C 端用户的机构扮演着转接清算机构的角色，存在参与资金流或仅参与信息流的不同情况，有潜在的资金二清风险和信息安全风险。部分非法聚合机构打着低费率旗号骗取社会资金，最终携款跑路。

2.3 银行卡线下收单业务

在银行卡线下收单业务中，移动 POS 机成为电信诈骗和非法集资、信用卡套现的常用工具。银行卡收单业务通常具有以下特点：商户准入门槛较低；商户日常巡检及查访不到位；刷卡资金到账快，目前部分支付机构支持 POS T+0 交易，可实现交易资金实时到账； POS 机具有携带便捷性、交易隐蔽性等特征，使得支付机构 POS 机具容易被非法分子利用。通过支付机构进行信用卡恶意套现费率低，不法分子通过购买闲置信用卡，在注册申领POS机具后，将非法资金注入信用卡，再通过虚构交易套现的方式，将非法资金合法化。除此之外，不法分子还会利用大额借记卡进行转账交易，并谎称为借贷还款等其他解释，进行非法资金的转移。

2.4 预付卡业务

因预付卡购买和兑换的便利性，且存在无需进行客户身份识别的不记名预付卡，也容易成为不法分子转移非法资金的工具。不法分子将违法收益购买大量不记名预付卡，通过黄牛置换成现金或将预付卡内的资金向多个支付账户分散转移，最后通过购买商品或提现完成非法资金的合法化。

3 政策建议

3.1 完善非银行支付机构法律体系

一是在反洗钱领域，虽然非银行支付机构参照金融机构监督管理，但因上位法缺失，其在督促、指导支付机构工作和反洗钱检查监管方面仍面临一定问题，建议值此修改《反洗钱法》契机，将支付机构纳入法律框架，规定相应义务。二是针对各业务细化客户身份识别、交易记录保存制度，对支付业务中的支付机构、外包服务提供商、银行等的各参与方的反洗钱义务加以规范。三是要求支付机构严格保护用户隐私，明确非银行支付机构和用户的权利和义务。四是规范举报通道和流程，保护和奖励检举人的同时抵制惩处恶意举报投诉等行为。

3.2 完善非银行支付机构的账户管理

账户实名制是反洗钱工作的基本要求，但目前大部分支付机构仍无法在业务中落实此项要求。一是因为同一张身份证可以注册多个账户，且每个账户可以绑定名下不同的银行卡，造成支付账户数量多、银行卡账户交错混乱的问题。二是因为支付机构的客户入网时大部分为远程非面对面录入信

息，再通过工商或身份证鉴权等方式即可通过验证，无法确定是否为本人开户。因此落实账户实名制，可以借鉴核实银行结算账户实名的经验，采取上传录音、录像文件的措施，并配合人脸识别软件等生物识别、动态识别工具，确保实名认证。同时也可以利用征信和大数据等手段，探索更加可靠和可信的身份验证手段，既满足账户实名制的要求，也保护客户信息不被泄露。建议公安机关在现有的公民身份信息查询系统基础上，向非银行互联网支付机构开放公民身份信息查询系统，为其提高辨别客户真实性能力提供支持。

3.3 加强非银行支付渠道的资金监测

一是要指导支付机构根据自身业务网络化、账户量众多、交易地区广、新业务层出不穷等特点和各业务洗钱风险环节搭建并完善反洗钱风险监测指标体系，加强资金监测和客户信息的整合，充分利用支付机构较强的大数据分析能力，形成多层次、多品种的监测模型，深度挖掘交易信息，增强数据分析的针对性。二是要指导机构采取有效措施，结合客户身份背景信息等内容开展人工分析、甄别和判断，加大对异常案例的人工审核能力和覆盖面，进一步提升可疑交易分析工作的有效性和报送的时效性。三是充分发挥银联、网联金融枢纽作用，加强基础设施建设，可建立资金交易信息整合、共享和查询机制，解决支付机构和银行端各执部分数据信息的问题，为反洗钱资金监控和案件调查信息的获取提供便利。

3.4 强化支付机构风险防范能力

一是要求机构树立良好的风险防控理念，尤其是董、监、高的反洗钱意识和职责，指导机构正确处理好业务发展和风险防控的关系。二是要求机构加强人才培养，通过吸纳和培养高素质专业人才，提升反洗钱工作水平，为防范洗钱风险提出有针对性的意见和专业的指导。同时通过加大对员工的培训，提高认识，增强其业务能力。三是利用互联网优势，加大普法宣传教育，增强机构对违规行为的敏感性，同时也增强社会公众的反洗钱意识。四是加强对支付机构的监督检查力度，指导机构严格履职，在客户准入环节严格把关，做好客户身份初次识别，从源头上控制洗钱风险，在后续管理中，做好持续识别和重新识别工作，通过技术手段利用大数据分析的优势，多途径验证客户信息的真实性。完善客户风险等级划分依据和流程，按照风险为本原则，合理配置资源，针对不同风险客户采取有针对性的管控措施。五是指导完善支付机构洗钱风险防范技术手段，要求做好反洗钱系统与业务系统的整合与对接，完善可疑交易监测模型和指标体系，按规定及时上报大额交易和可疑交易报告。

3.5 完善支付机构洗钱风险防控体系

建议建立完善以政府监督为主导、支付机构履职为重点、行业自律为依托的全方位监管体系，切实发挥好监管部门、支付机构和行业自律组织在洗钱风险防范中的作用。通过开展积极有效的业务交流、信息共享活动，将客户身份识别、大额可疑交易报告等工作的各个环节落到实处。

3.6 加强支付机构洗钱风险防范国际合作

随着全球化不断推进，跨境支付规模与需求不断增大，支付机构参与跨境活动也呈现上升趋势，欧美等国家互联网支付起步早，制度相对成熟，在充分分析中国国情基础上，制定和完善制度时当可借鉴。建议加强国际监管合作[3]，吸收别国监管经验，拓宽监管信息共享渠道、警务合作协查渠道等，形成全球化跨境网络支付业务管理体系，共同抵制洗钱行为，维护全球支付体系和金融系统稳健发展。

参考文献

[1] 肖邦迪.浅析支付机构洗钱风险—以第三方支付为例[EB/OL].(2018-11-07). http://www.xinjr.com/yinxing/yewudongtai/2018-11-07/615123.html.

[2] 马伟利,许井荣.互联网金融洗钱风险控制研究[J].金融论坛,2015,(4):64-68.

[3] 刘蕙,姚燕莹.第三方支付机构洗钱风险控制研究[J].金融经济,2018,(20):7-9.