

防范身边的洗钱风险 | 警惕利用聚合收款码进行违法洗钱

对利用聚合收款码进行违法洗钱说“不”

聚合收款码作为经济社会数字化、数智化发展历程中的一项数字化产物，因其快捷和低成本等优势在扫码支付业务中占据了重要地位。然而，这一便捷性也伴随着洗钱风险。

01 什么是聚合收款码

聚合收款码是一款可支持多个平台（支付宝、微信、云闪付、翼支付等）扫描付款的二维码，当顾客扫码时，系统通过识别应用程序类型，自动跳转至相应的支付页面，适用于各种商业场景，方便商家收款。



02 什么是聚合收款码洗钱

聚合收款码洗钱是一项非法活动，犯罪分子通过虚假交易、虚构贸易背景等手段，利用聚合收款码进行可疑资金划转操作，旨在掩盖或混淆资金的真实来源与性质，进而隐匿其非法的资金流动轨迹，以此协助实施洗钱等违法犯罪活动。



03 典型案例

案例一 利用商户收款码进行信用卡套现



2020年9月，杨某“上线”告诉杨某只需要办理商户收款码，进行信用卡套现就可以获利，杨某同意后共办理商户收款码三个，并将办理好的收款码提供给“上线”。“上线”联系需要进行信用卡套现的持卡人，成功套现后，杨某按照一定比例收取手续费。半年间，在并无真实业务交易的情况下，杨某帮助“上线”进行信用卡套现5000余万元，获利5万余元。本案中，杨某作为“中间人”为他人提供信用卡套现服务，以虚构交易的方式，实现了信用卡所属银行与套现客户之间的资金转移，在过程中收取手续费，从中牟利。经人民检察院立案监督后依法提起公诉，法院以非法经营罪判处杨某有期徒刑二年，缓刑考验期二年，并处罚金人民币5.1万元。

案例二 通过手机店等聚合收款码过渡大额资金



2023年10至11月，三名犯罪嫌疑人在明知帮助他人提供手机店聚合收款码收取违法违规手机店铺的情况下，仍以营利为目的，通过寻找手机店铺并谎称采购手机名义，将手机店内聚合收款码拍下，并通过“飞机”软件发送给诈骗嫌疑人，在收取二码收款码支付凭证后，犯罪嫌疑人将手机收取后低价卖出并将售卖手机的非法所得兑换为“U币”帮助诈骗嫌疑人转移资金。犯罪嫌疑人已主动帮助诈骗嫌疑人转移资金59万余元。经人民检察院提起公诉，法院以掩饰、隐瞒犯罪所得罪依法判处三名被告人有期徒刑三年到三年九个月不等，并分别处罚金人民币1万元。

案例三 鲜花店、蛋糕店聚合收款码被用于取现



2024年3月，某鲜花店A、鲜花店B及某蛋糕店工作人员均收到订购要求，一个微信自称“王某某”的人要求订购放置现金2万元的鲜花礼盒、蛋糕礼盒。鲜花店和蛋糕店工作人员均按照“王某某”的要求向该人提供了各自的收款码用于接收钱款。收到钱款后，两家鲜花店及蛋糕店的工作人员分别取出2万元用于放置在鲜花、蛋糕礼盒内。经警方核实，鲜花店和蛋糕店收到用于鲜花、蛋糕礼盒的资金，实际上是电信网络诈骗罪的赃款。当日，被告人李某在明知放置在鲜花及蛋糕礼盒内共计6万元系犯罪所得的情况下，仍欲取走上述礼盒，现场被民警抓获。最终经人民法院审理，判决被告人李某犯掩饰、隐瞒犯罪所得罪，判处有期徒刑八个月，并处罚金人民币1万元。

04 防范措施

措施一

金融机构需规范对商户的客户身份核实、资料保存、交易监控以及尽职调查等程序，一旦识别出可疑活动，应迅速提交可疑交易报告，并对收款码实施相应的管理措施。此外，金融机构应承担起社会责任，积极开展反洗钱培训和宣传，增强全体员工的反洗钱意识和能力，确保国家经济和金融市场的稳定。



措施二

商户应熟悉并严格遵守国家的反洗钱法律法规，妥善保管自己的聚合收款码，规范收取付款码，拒绝不明资金，尽量选择当面交易，对付款客户身份进行详尽核实，做好大额订单的实名登记，安装高质量的视频监控设备，留存清晰的面部信息以备监管检查，避免成为洗钱活动的“工具人”或“替罪羊”，保障自身业务的合法性与安全性。



措施三

公众应提升对洗钱活动的认识，深刻理解其带来的危害及表现特征，尤其是跑账与同城闪送等订单人员需对提供高额报酬以委托接收货物的订单保持高度警觉，一旦察觉到洗钱行为，应积极向执法部门举报，共同营造全民参与反洗钱的积极氛围，助力构建一个更加公正与透明的社会。

