CCID 赛迪智库 专报

2018 年 1 月 10 日　　第 4 期　　总第 586 期

POS 机诈骗案频发须引起高度重视

【内容提要】 前不久，不断有媒体曝出因 POS 机引发的诈骗案件。刷卡人在改装过的“新 POS 机”上刷卡时，银行卡的所有信息都会被截获，卡内余额会被复制卡全部取走。赛迪智库网络空间研究所认为，POS 机诈骗案折射出的问题是：对 POS 机终端产品监管不严，厂商鱼龙混杂，POS 机安全技术标准滞后，老旧 POS 机终端存量较大。基于此，提出五点建议：加强对 POS 机全生命周期的安全监管；建立部门间协同监管机制；加强 POS 机安全防护技术研发和标准制修订；设定严格的入网及报废机制；做好 POS 机安全宣贯工作。

【关键词】 POS 机改装　银行卡诈骗

近年来，因 POS 机引发的银行卡诈骗案件时有发生。不法分子通过改装 POS 机终端，加装盗取银行卡信息存储的设备到 POS 机内，以低于市场价的价格出售，恶意盗取持卡人信息。前不久，已有不少省市发现这类 POS 机正通过各种渠道流入市场。一些收单机构审批简单，只需身份证、银行卡照片和电话号码就可办理个人对私 POS 机，无疑为这种违法犯罪行为提供了生存空间。针对 POS 机诈骗事件频发提出相应对策，加强对 POS 机发放机构的监管，确保刷卡消费者的合法权益，已是迫在眉睫。

一、POS 机诈骗的特点及危害

（一）POS 机诈骗事件频发

2017 年 6 月，北京朝阳警方破获了多起 POS 机诈骗案，涉案金额 50 余万元。2017 年 8 月，上海市奉贤区警方破获一起特大跨省市系列 POS 机诈骗案件，对商铺店家实行诈骗多达 640 余起，涉案金额 128 万余元。2017 年 8 月，沈阳市公安局浑南分局侦破一起利用 POS 机实施的诈骗案件，被骗商户 178 家，涉案金额 203 万元。2017 年 8 月，云南曲靖警方抓获一诈骗团伙，经侦查对实施的 POS 机金融诈骗事实供认不讳，据交代，该团伙流窜在山东、江西、河

南、贵州、陕西等地，疯狂作案 20 余起，涉案金额 10 万余元。2017 年 8 月，重庆南岸区警局打掉一个利用 POS 机进行诈骗的团伙，短短两个月，该团伙就盗刷近百万元，受害者多达 30 余人。

（二）POS 机诈骗的特点

2017 年以来，媒体曝光的多起通过 POS 机盗刷银行卡诈骗案有以下特点: 一是有组织的团伙犯罪。覆盖了非法改装 POS 机、截获持卡人信息及密码、克隆银行卡并实施异地盗刷的黑色产业链，分工明确，协作周密，作案手法隐秘。二是诈骗团伙学历普遍在高中水平。POS 机诈骗并不需要高深的专业技术，其大多数是通过互联网了解 POS 机结构，并学习改装 POS 机。三是人员流动性强。犯罪嫌疑人主要通过互联网、即时聊天工具等媒介进行线上勾结、策划以及犯罪经验传授，并在各地流窜作案。

（三）POS 机诈骗的危害

一是 POS 机诈骗给持卡人带来了严重的经济损失。近期北京、上海、四川等地连续侦破系列 POS 机诈骗案件，涉案金额近千万元，给受害者造成了难以弥补的经济损失。二是 POS 机诈骗干扰了正常的金融秩序。POS 机诈骗不仅扰乱了金融机构的经营秩序，

还会给金融机构带来潜在的金融风险，尤其是信用卡诈骗，会给银行造成无法挽回的声誉和资金损失。

二、POS 机诈骗案多发的原因

（一）对 POS 机终端产品监管不严

POS 机终端作为重要的金融支付工具，攸关公众财产安全，应定性为面向收单机构的行业产品而非大众消费品。然而，由于产品监管方面存在漏洞，致使 POS 机产品被当作一般性电子消费品，在一些购物网站甚至可以随意购买到 POS 机，极易导致不符合技术标准、被非法改装过的 POS 终端流入市场。不论对购买方还是使用方，都存在信息泄露、资金被盗等风险，为电信网络诈骗开启了方便之门。

（二）POS 机厂商鱼龙混杂

目前，全国有银联认证的 POS 机终端厂商约 95 家，还有众多未经过银联认证的厂商，这些终端厂商资质和技术水平有一定差异，产品质量参差不齐。一方面，一些能力和技术水平差的公司通过挂靠、代理的形式可以生产 POS 机终端，尽管授权符合要求，但在实际生产中偷工减料，产品质量不达标。另一方面，一

些未获得相应资质的 POS 机终端厂商执行生产标准不严，在产品没有通过必要测试和认证的情况下，仅通过第三方收单机构的入网联调，就将不合规的 POS 机产品推向市场。这些都给 POS 机终端的应用埋下了安全隐患。

（三）POS 机安全技术标准滞后，新技术应用推广难度较大

随着信息安全技术的发展，通信传输安全、身份认证技术、数据存储安全、芯片安全、操作系统安全、信息脱密、数据编码、POS 机防拆自毁程序等多种安全技术在金融支付领域得以应用。但是，强制性安全标准规范更新滞后，目前最新的 POS 机终端安全标准还是 2010 年发布实施的《银联卡受理终端 PIN 输入设备安全规范》（Q/CUP 007.6-2010）。此外，由于高安全、高可靠性的 POS 机终端成本较高、系统集成复杂，在没有强制标准制约下应用推广受限；一些掌握更高安全技术的 POS 机终端生产企业迫于成本压力，以及来自低端 POS 机终端生产厂商的竞争压力，不得不放弃对新安全技术的研发生产及应用推广。

（四）老旧 POS 机终端存量较大

目前，市场还存有大量老旧 POS 机终端仍在使用，这些 POS

机终端产品大都存在一定的安全缺陷，并且也超出了厂家维保年限（一般规定为 5 年），其中大部分 POS 机未安装防拆装置，或防拆装置失效，容易被不法分子拆解改装。此外，全国发行的银行卡总量在 65 亿张左右，其中磁条卡存量约 34 亿张，由于读取磁条卡的 POS 机存在设计缺陷，很容易被不法分子通过侧录的方式窃取银行卡信息。此次曝出的被非法改装的 POS 机终端就属于读取磁条卡的老旧机型。

三、遏制利用 POS 机诈骗的措施建议

（一）加强对 POS 机全生命周期安全监管

POS 机终端设计生产和应用环节理应遵循严格的规范要求。依照颁布实施的相关规范，在应用软件开发环节，由金融收单机构下单，POS 机终端厂商根据收单机构的技术标准要求制定研制方案，待通过银行或第三方机构验收后，POS 机终端厂商才能做定制化生产，并且严格按照生产安全流程操作，保证设备终端信息安全。在设计生产环节，遵照金融行业《银联终端产品生命周期安全和质量管理指南》的相关要求，由 POS 机终端厂商进行严格的把关控制，从源头上开始保证安全，从原材料采购到生产整

机入库，对整个过程关键节点都要进行相应的测试与监控。同时，要保证终端整机的安全、可靠，可根据设备序列号实现对批次产品的追溯。在安装应用环节，POS 机终端交付收单机构后，会交由专门的金融主管部门分管，按照资质审查流程和标准，对 POS 机用户进行资质审核和材料审批，内容包括对机具布放市场后的安全和使用安全均由机构负责，银行或机构对采购的机具拥有所有权，杜绝 POS 机生产和流通过程中的安全隐患。

金融主管部门应加强对收单机构的监管。严格禁止非法、违规提供或使用受理设备。如果已造成社会危害和不良影响的，相关机构和单位及个人有权追究其法律责任并要求赔偿。收单机构有责任、有义务给商户提供有合法来源的支付产品；收单支付产品和设备应符合国家相关金融规范及指导标准。在推广和营销各类收单受理工具和设备时，收单机构有义务为使用者说明使用要点，明确违规违法责任。

（二）建立部门间协同监管机制

POS 机终端作为重要的金融支付工具，除了遵循国家金融行业相关规范和设计标准外，还应接受相关行业主管部门的监督管

理。例如，对于受理金融支付的 POS 机，应通过工业和信息化部颁发的入网许可；POS 机终端产品投入市场前，需经过金融主管部门授权许可的银检机构和相应的安全检测认证许可。POS 机终端不同于一般的消费类电子产品，它关乎国家金融秩序的稳定，对此类特殊的行业产品，必须加强监督管理和行业应用的规范化。为此，在应对 POS 机诈骗时，还需根据各部门的职责分工，强化相关主管部门之间的沟通合作，形成高效互动机制，借助联合开展整治非法买卖银行卡信息的专项行动，要加强对 POS 诈骗新型违法犯罪交易风险的研判管理和有效应对。

（三）加强对 POS 机安全防护技术研发和标准的制修订

作为一种特殊的金融支付工具，POS 机首要的功能应是确保持卡人刷卡交易的安全。一方面，要加强安全技术的研发与应用，提升 POS 机应用安全保障能力；另一方面，要及时更新 POS 机终端的安全标准规范，推动新型安全技术的应用。研究制定应对 POS 机诈骗的具体技术标准，应从以下方面展开：一是通过应用新型安全支付标记化技术，对银行卡安全码等信息进行脱敏处理，并通过设置支付标记的交易次数、交易金额、有效期、支付

渠道等域控属性，从源头控制信息泄露和交易风险。二是采用具有信息输入即时数据加密功能的安全控件，防止收单机构及委托代理机构非法采集支付敏感信息。三是加强客户端软件安全管理，确保客户端软件符合国家金融行业相关标准和信息安全要求，提升客户端软件安全防控能力。四是利用大数据分析用户行为建模等手段，建立交易风险监控模型和系统，及时预警异常交易，并采取调查核实、风险提示、延迟结算、附加验证、拒绝请求等措施，应对批量或频繁登录等异常行为。五是强化第三方收单服务平台的安全评估，增加服务器端对接收数据的有效性校验功能，防止客户端提交非法数据及 SQL 注入等攻击。

（四）设定严格的入网及报废机制

POS 机终端作为金融支付工具，应具有严格的入网审查许可。POS 终端厂商通过安全认证后，方可进行产品入网许可申请，保证安全认证产品与入网产品的一致性，并由主管部门进行监管，未获得进网许可证以及进网许可证失效的电信设备不得加贴进网标志。此外，无论从使用期限、硬件老化程度，还是应用环境、行业安全标准更迭来看，电子产品都应当有一定的生命周期和年

限要求。对于 POS 机产品，可以考虑在进网标上加上使用年限字样，约定特殊产品的在网有效期，以规避因技术更新、安全技术等级提高等因素造成原有终端不符合现有安全使用条件，相关部门可进一步研究 POS 机终端报废回收办法。

（五）做好 POS 机安全宣贯工作

引导 POS 机生产企业加强行业自律，利用先进成熟的安全信息、安全技术手段，实现对敏感信息的隔离保护，生产安全可靠的 POS 终端产品。同时，还应加强银行卡互联网支付等交易密码的保护管理和安全宣传和教育，培养收单商户、普通用户的风险防范意识和安全支付习惯，提高安全防范意识，针对犯罪分子典型作案手法，开展安全支付教育工作，通过网站、微博、微信以及网络安全周等不同渠道，及时向商户通报犯罪分子的最新作案手法，提高用户的风险防范意识。

本文作者：工业和信息化部赛迪研究院　　李建武
联系方式：18811593662
电子邮件：lijianwu@ccidthinktank.com

赛迪智库
面向政府 服务决策

思想，还是思想
才使我们与众不同

《赛迪专报》
《赛迪译丛》
《赛迪智库·软科学》
《赛迪智库·国际观察》
《赛迪智库·前瞻》
《赛迪智库·视点》
《赛迪智库·动向》
《赛迪智库·案例》
《赛迪智库·数据》
《智说新论》
《书说新语》

《两化融合研究》
《互联网研究》
《网络空间研究》
《电子信息产业研究》
《软件与信息服务研究》
《工业和信息化研究》
《工业经济研究》
《工业科技研究》
《世界工业研究》
《原材料工业研究》

《财经研究》
《装备工业研究》
《消费品工业研究》
《工业节能与环保研究》
《安全产业研究》
《产业政策研究》
《中小企业研究》
《无线电管理研究》
《集成电路研究》
《政策法规研究》
《军民结合研究》

编 辑 部：赛迪工业和信息化研究院
通讯地址：北京市海淀区万寿路27号院8号楼12层
邮政编码：100846
联 系 人：刘 颖 董 凯
联系电话：010-68200552 13701304215
010-68207922 13910685050
传 真：0086-10-68209616
网 址：www.ccidwise.com
电子邮件：liuying@ccidthinktank.com

报：部领导

送：部机关各司局，各地方工业和信息化主管部门及相关部门

编 辑 部：工业和信息化部赛迪研究院
通讯地址：北京市海淀区万寿路27号院南门8号楼12层
邮政编码：100846
联 系 人：刘颖　董凯
联系电话：010-68200552　13701304215
010-68207922　13910685050
传　　真：010-68200534
网　　址：www.ccidwise.com
电子邮件：liuying@ccidthinktank.com