中国刑警学院学报
Journal of Criminal Investigation Police University of China

电信网络新型犯罪防控体系研究

林　伟

（福建警察学院　福建　福州　350007）

摘　要：电信网络新型犯罪是伴随社会信息化而滋生的一类犯罪，其核心是电信诈骗，具有向网络盗窃转型的趋势。针对目前诈骗方式结合通信、金融技术发展不断更新升级，非法获取公民个人信息后骗盗结合手段突出。分析电信网络犯罪的发展趋势，探讨打击治理面临的困境，提出以技术与管理相结合的方式构建警企联动、行业担责、全民参与的防控电信网络违法犯罪体系。

关键词：电信网络犯罪　个人信息安全　防控体系

中图分类号：D924　　**文献标识码**：A　　**文章编号**：2095-7939(2016)04-0032-04

DOI：10.14060/j.issn.2095-7939.2016.04.006

随着我国金融、电信和互联网的发展，电信网络新型诈骗迅速在我国产生并蔓延。通过侵害公民个人信息以及非法生产、销售和使用“伪基站”、窃听窃照专用器材、手机恶意程序、无线屏蔽器、“黑广播”等电信网络新型犯罪来势凶猛、愈演愈烈，严重危害人民群众财产安全，扰乱正常生产生活秩序，已成为影响社会稳定的突出犯罪问题。因此，分析电信网络新型犯罪的发展趋势，构建针对此类犯罪的防控体系具有重要的现实意义[1]。

1　电信网络新型犯罪发展趋势

1.1　诈骗手段升级

当前，电信诈骗犯罪经历了传统的“漫天撒网”、“盲目扫描”、“情报导骗”等阶段[2]发展演变后，已开始向骗盗结合、窃取信息后盗窃银行客户存款犯罪升级。特别是随着网上银行与第三方支付业务快速发展，针对网银电子支付工具与业务验证漏洞出现的新型电信诈骗、网络盗窃犯罪问题日益突出，近年常见的形式就有虚构涉案审查诈骗升级版的“假通缉令诈骗”[3]、骗取公民个人及账户信息后盗取存款的“各类恶意链接陷阱”、“虚假网银升级”、“虚构代办高额度信用卡”以及虚假网络投资诈骗等。

诈骗分子通常编造各种理由，骗取受害人银行卡账户信息和短信验证码或按指令操作登陆网银的电脑和加密工具，常见手法有：一是发送各类隐含恶意链接的短信，如假冒电子请贴、怀旧、亲情照片、要事通知、网银加密工具升级等，诱骗事主点击，窃取信息后盗窃手机关联账户存款。二是在预先获取客户身份证信息、手机号、银行卡、网上营业厅登录密码后，再借助 10086 网上营业厅、139 邮箱短信骗取客户校验码，完成自助换手机卡后盗取相关银行账户存款。三是电话谎称某地警方发现事主涉嫌洗钱或涉毒品案件需当地协助办案为由需核查资金，电话联系过程中先引导事主通过 114 查号台核对来电显号（实为虚拟号）系公安机关号码，之后要求登录指定网址查看假“通缉令”，让事主轻信涉案被通缉。接着引导事主操作电脑下载安装远程控制软件，并操作账户网银加密工具，盗取存款。四是以提供无息低息贷款为诱饵，以办卡、多次存取钱刷交易流水记录为幌子，要求事主去银行办理关联操作，其目的不是方便贷款，而是直接将事主的银行卡与嫌犯的银行卡进行关联。按照这种“关联”业务规定，一方的钱，在不用确认的情况下，可被另外一方直接扣走。五是谎称可代办高额度信用卡，要求事主先开一张储蓄卡，预留事主手机和对方手机号，并存入一定数额的资金。之后将身份证号、账号告知对方。当事主问为何还要预留对方手机号，则谎称便于和银行沟通联系办高额度信用卡。当事主按对方要求开户并存款后，诈骗分子即利用冒名注册第三方支付快捷支付功能将账户内资

收稿日期：2016-11-03

基金项目：福建省法学会 2015 年度研究课题（编号：FLS(2015)D09）。

作者简介：林伟(1983-)，男，福建莆田人，福建警察学院侦查系讲师，主要从事信息化侦查研究。

金转走。六是架设虚假农产品现货交易平台，当事人通过第三方支付将账户资金投入诈骗分子设立的交易平台进行交易，其行情指数却不受现实价格影响，而由嫌疑人随意通过反向操作控制行情走势，致客户资金亏损、爆仓，骗盗资金。

1.2 个人信息安全问题日益突出

随着互联网的发展及大数据时代的到来，数据技术通过深度挖掘和分析向我们提供进一步的信息和服务，然而技术给我们提供很多便利的同时，亦丰富了公民个人信息泄露的渠道。如 12306 订票官网流出的 13 万用户数据，其中就包含用户姓名、身份证、手机号、电话等敏感信息；支付宝前技术人员非法贩卖他人信息达 20 多 G；淘宝后台的重大安全漏洞致使黑客无需账户密码即可登录账号，获取用户余额、收货地址、姓名、手机号等隐私信息；再到快递公司公开出售快递信息、快捷酒店系统存在安全隐患、多家航空公司的“泄露门”事件，公民信息泄露的隐患堪忧[4]。同样，掌握大量数据资源的企业网络一旦出现非法采集、窃取、贩卖和利用网络个人信息的客户个人隐私泄露，将对公民的人身财产安全构成严重威胁。有了这些真实的个人信息，骗子即可轻易骗取受害人的信任，继而开始实施诈骗、网络盗窃，如社保卡停用、机票改签、邮包藏毒等骗局。

1.3 反侦查手段升级

利用跨区域、跨境侦查障碍，逃避打击。同时又利用国际化通信、金融服务快捷实施犯罪，主要表现在以下三个方面：其一团伙结构设置及成员分布跨区域、跨境化。诈骗分子通常分布在不同的区域及国家，因各国司法制度等方面的差异而存在种种障碍，增加侦查成本[5]。其二紧随科技潮流增加信息化侦查障碍。其表现为跨境使用 VOIP 电话任意透传号码技术，无线上网操作网上银行转账，话务、转取款多设在境外或异地[6]。其三利用金融业务发展设置资金流侦查障碍。洗钱方式由购买游戏币、电话卡、网络支付等方式进一步升级，已出现嫌犯利用境外赌盘，以“左手倒右手”的方式通过“输家”将骗得汇款注入赌盘，“赢家”则从赌盘取出洗白赃款，从而形成“水池洗钱效应”。

2 打击治理面临的困境

2.1 侦查障碍多，消耗资源大

电信网络犯罪作为一种新型犯罪形式，往往因为办案队伍的专业侦查能力差距、侦查资源的限制、异地协作不畅、重要信息查询速度慢等因素迟滞侦查，给打击工作造成很大困难。主要表现为：其一，涉案账户和联络信息虚假。诈骗分子绝大多数使用的手机、银行卡无记名或为冒用他人身份登记开户的“人头”卡，网站是虚假资料登记或者租用境外服务器，并用无线上网技术维护网站。其二，分散隐蔽作案。诈骗团伙一般分为幕后操纵指挥、发短信、接听电话、取款等几个相对独立的单元分散作案，作案手机与生活手机严格分开。甚至内部联系机与个人生活机分开，并经常更换。还有的将接听电话窝点设置在山区、高楼层等侦控定位难的地点，以逃避打击。近期，还发现话务部分拆分一线与二、三线并分别设窝点。其三，利用跨境屏障。诈骗团伙在境外设置相对独立跨多国的分支、窝点，并由在境外的团伙头目统一指挥，故难以打全，亦多因取证问题难以处理或降格处理。其四，及时毁灭证据或适时转移“高危窝点”。每骗到一笔巨额汇款（约 20 万以上）即转移话务窝点，遣散部分成员，转移异地再重组，或每隔一段时间即转移话务窝点。电信诈骗在取证过程中往往仅获取到现案证据、并且获取的证据数量缺失多。近年来出现的新型的诈骗犯罪类型，认定数额多低于实际发生数额、职业犯重罪轻判亦较多。

2.2 银行、通信行业社会安全责任不落实

因电信网络新型犯罪案件的非接触性，诈骗分子主要利用通信工具或者互联网实施诈骗，再通过银行卡或者第三方支付将钱转移，此过程涉及到金融、通信行业。

2.2.1 银行业责任不落实的主要体现

（1）各商业银行账户开户泛滥、存在审核漏洞。绝大多数银行仍使用柜员的人眼识别身份证照片与开户人容貌的方式，识别率不够高，并易受个体能力影响。

（2）安全论证不足，多种新增功能成为翻新诈骗、盗窃手段的载体，“亡羊补牢”严重滞后问题依然突出；售后安全服务长期不足，客户使用支付工具时缺乏安全知识；重利轻安式的发展风险由客户“买单”。

（3）银行与第三方支付的协议存在降低安全等级问题；高加密级的网银用户（U 盾用户）被冒名注册第三方支付账户后成为低密级账户（手机验证码用户），直至存款被盗。

（4）依法给警方提供查询工作比较滞后，影响侦查进度。

2.2.2 通信行业责任不落实的体现

手机卡开户泛滥（实名制后仍存在套开人头卡问题），固定电话、宽带安装、手机补卡审核均存在漏洞；安全论证不足，新功能易成为翻新诈骗手段的载体，“亡羊补牢”严重滞后等问题同样突出；境外透传改号网络电话呼入量巨大,封堵严重不足;依法给警

方提供查询工作比较滞后，特别是异地 400、一号通、商务号、网络传真，以及 170、171 开头号段等查询困难。

综上，发案居高不下的问题之所以长期未能根本改观，主要原因之一就是银行、通信行业社会安全责任不落实，至今仍有大量的使用他人身份开户的银行账户、手机卡、网络电话线路继续流入市场为犯罪所用。

2.3 群众防范意识和能力滞后

随着“互联网 +”进程的全面推进，电信网络新型犯罪中的电信诈骗与互联网快速融合，诈骗手段的不断变换，群众相关知识空白或者不足，必然会遇到安全知识新盲点问题，新政策的推广、公民个人信息泄露的扩大、金融系统新的安全漏洞，都让诈骗分子有机可乘。而公安机关阶段性的宣传只局限于已发生的诈骗形式，受众面覆盖范围的不完全，群众素质高低的不同，都使得宣传效果打了折扣，群众防范意识和能力不足仍普遍存在，对身份证和银行卡的安全意识有待提升。

3 防控体系建设

电信网络新型犯罪活动的猖獗，诈骗分子反侦查能力的增强，非接触性和隐蔽性等特点使得群众财产安全受到严重威胁。全社会的合力与公安机关高强度的打击势在必行，只有防治结合，才能真正切断电信网络新型违法犯罪的“根”。

3.1 警银联动构建资金流防护网

警银联合打击关联洗钱犯罪，银行加强监管资金流动的入口、过程、出口等各个环节，警银协作阻截犯罪产业链，根治此类犯罪赖以生存的土壤。

（1）联合加强开户身份验证基础措施，把好开户准入关。银行首先要加强开户审核，从根源上解决“人头卡”问题，从证件认证，向实人认证发展。一是柜员比对开户人像与身份证照片，如发现嫌疑，后台人员再识别。如福建平潭招商银行案例，留存开户人高清照片，后台人像比对，发现嫌疑，现场控制，协助公安机关破获一特大妨碍信用卡管理案件。二是开户必须备份高清照片，保存开户人开户行为的重要证据。三是推广应用机器识别辅助手段。柜员借助电脑识别软件识别开户人像照片与身份证照片，现有成熟技术识别率已达 98%，远高于人眼识别。四是阻断丢失、被盗的二代身份证被犯罪利用的通道。我国每年丢失、被盗的二代身份证数量巨大，大多被不法分子非法收集，在网络黑市公然叫卖。几经倒手后，这些身份证或被用于冒名开银行卡牟利，或被用于掩护诈骗犯罪。公安机关应提供补办身份证信息查询条件。

（2）警银合作加强风险控制信息化建设，立足银行大数据实现高效技术对抗，保护客户正当权益，限制违法犯罪活动。警银合作开展事中干预，推进涉案账户及灰名单账户预警管控机制。例如，工商银行自 2013 年建成《外部欺诈风险信息系统》运行以来，已阻拦涉案赃款数亿元，成效显著。

（3）建立反诈骗中心，公安、银行、通信分工协作，做好出口端的防控及快速止损。福建省厦门市反诈骗中心成立后，群众一旦遭遇诈骗需要求助，只要通过正常拨打 110 进行报警，接警员会第一时间将警情转到反诈骗中心。反诈骗中心接警席向报警人问清诈骗电话号码、涉案银行账号、转账银行、转账方式等详情，并同步录入反诈骗接处警平台，需紧急处置的经接警组长审核后，即通过反诈骗接处警平台直接推送至处置席的金融电信点对点查控系统，再由处置席通过该系统分别向银行提请资金查询冻结，向通信运营商提请电话停机（针对本地诈骗电话）、拦截（针对外地诈骗电话）和封堵（针对虚拟诈骗电话），之后，再由研判打击组分析数据，作为警方后续追踪、打击犯罪的线索，取得良好成效。

3.2 警通联动构建通讯网络信息流防火墙

警通联合从电话、网络信息传输的各个环节封堵漏洞，压缩此类犯罪生存空间。通信企业加强开办手机卡审核措施，加强屏蔽机制，拦截诈骗信息，禁止任意显话务流量随意外包，建立严控 VOIP 的准入机制。警通协作严打严防冒用他人身份开卡、补卡，进而实施电话诈骗窃取个人账密信息、盗窃存款犯罪。警通联合构建智能全网拦截平台，合力开展源头拦截，对具有被叫用户按键转接“人工服务”的电话、回呼不通的境内隐藏号码或改号电话以及通过“诈骗关键词”语音识别出的境内群呼电话等即时切断。

3.3 落实金融、通信与互联网行业社会责任

打击治理电信网络新型违法犯罪必须从落实金融、通信行业社会安全责任入手，加强行业安全生产监管，明确相关法律责任，实现标本兼治。

（1）加强网银客户售后安全服务及终端设备的安全措施，若因银行管理或技术上问题导致客户资金损失，应按相关法律法规落实银行的经济赔偿责任。例如，2014 年 6 月 12 日，福建漳州龙海一客户发现手机里有多条短信，提示银行卡里的 3 万多元被人分 8 次支取，交易点在汕头市一家银行的 ATM 机。该客户第一时间向银行客服投诉，持银行卡打印出交易清单，并申请冻结了银行卡存款，向警方报案，经警方查证取款人并非客户本人。该客户将银行告上法庭，最终法院判银行负全责，赔偿全部损失 3.6 万余元。

（2）应建立有效的行业监管和惩罚机制，避免出现无法可依、有法不依等现象，决不放任通信行业一味追求企业利益而抛弃社会安全责任的行为,对违法违规运营造成客户个人信息被窃、账户资金损失的，应依法追究相应法律责任。

（3）应完善金融行业互联网支付法律制度，包括支付协议的相关问题，树立金融消费者保护和违约追责赔损理念，加强保护信息安全措施，加强银行、第三方支付开户身份验证基础措施，加强交易过程的安全提示，快速冻结止付，及时挽损。

3.4 公安、银行、通信合力提高安全服务水平，有效帮助群众加强防范能力

（1）公安机关通过设立警方防骗咨询热线，为群众提供安全防范服务。通过做好安全咨询服务工作，方便遇到疑问的群众及时报警和举报，切实提高群众的防范意识和个人信息安全意识。同时，及时向银行、通信企业通报新型犯罪警情及手段变换特点，适时联合银行、通信开展针对性防范宣传活动，通过制作宣传展板、传单、动画等群众喜闻乐见的形式，及时公布最新的诈骗手段和预警信息，扫除安全盲点，填补相关安全知识的不足。

（2）银行、通信企业要切实做好产品售后安全服务，按照营业规则、合同约定，认真履行向客户销售产品附带传输安全使用常识的责任。要综合利用业务短信、网页、账单、终端显示屏、营业网点设施做足防范提醒和警示， 努力提升客户端防范能力。

（3）公安、银行、通信建立联合服务社会安全的长效机制，致力解决社会大众防范滞后问题，最大程度地节约社会成本，提高防控工作效率。警银通应加强在信息检索、调取证据、快速冻结赃款等方面协作能力。首先，银行、通信应加强其内部系统建设，完善信息目录建设合理化、科学化以提高信息检索精确率、效用率；信息化的建设不仅提高企业自身安全系数，避免犯罪分子利用其漏洞实施犯罪行为，而且利于在事发后帮助警方实现由案到人的精确打击，实现警企联动共同维护用户权益。

其次，警方为侦查需要应深入挖掘相关犯罪嫌疑人交易记录、相关开户信息、视频监控等信息，而银行、通信是这些信息的持有者和提供者，应简化查询、冻结的审批手续，建立便捷反应机制，提高案件侦破效率。

电信网络新型犯罪不是单纯的犯罪问题，近年来境内外经验（中国台湾、日本、韩国、东南亚等国家地区）证明，仅靠警方的打防控工作显然不足以遏制此类犯罪的发展蔓延。需争取从政府层面调动金融、通信行业投入，不断完善相关社会管理制度以跟进社会信息化发展[7]，并从法制层面落实相关行业的社会安全责任，警银、警通联合构建多元立体化防控体系，有力遏制此类犯罪。

参考文献:

[1] 胡向阳,刘祥伟,彭巍.电信诈骗犯罪防控对策研究[J].中国人民公安大学学报,2010(5):90-98.

[2] 李恒,王刚.网络电信诈骗犯罪案件特点及侦防对策研究[J].净月学刊,2014(5):33-39.

[3] 王晓伟.打击电信诈骗犯罪理念转变与机制创新[J].人民论坛,2016(1):42-44.

[4] 陶茂丽,王泽成.大数据时代的个人信息保护机制研究[J].情报探索,2016(1):12-19.

[5] 李维强.电信诈骗的规律特点及治理对策研究[D].兰州:兰州大学,2012:9.

[6] 李超峰.跨国电信诈骗犯罪惩治与防范[J].社会科学家,2014(3):94-98.

[7] 李双其.再论公安侦查机制改革[J].中国人民公安大学学报,2015(3):54-60.

（责任编辑：孟凡骞）