风险防控视角下商业银行预防电信诈骗难点及对策研究——以中国工商银行十堰分行为例

宋磊

湖北汽车工业学院 汽车商学院，湖北省十堰市，442002；

中国工商银行股份有限公司十堰分行，湖北省十堰市，442000；

摘要：数字化背景下，基于风险防控视角探究商业银行预防电信诈骗的难点及其对策研究具有重要的现实意义。电信诈骗对全社会造成的损失和影响不断扩大，其犯罪手段不断进化，并已发展出一条成熟的非法产业链，而诈骗行为也呈现出线上线下相融合、跨机构、甚至跨国界作案的新趋势。在预防电信诈骗过程中，存在场景不断增多、受害群体年轻化和手段快速变化等难点，这不仅给商业银行等金融机构开展风险防控工作带来更大的难度，也为商业银行带来了声誉风险、经济损失风险、法律风险等多重风险的影响。因此，商业银行可以通过多维资源整合、开发预警系统、建立反诈数据模型、加强反诈宣传、完善银行内部制度管理等方式来解决电信诈骗中的难点问题。

关键词：商业银行；电信诈骗；反欺诈；风险防控

DOI：10.69979/3041-0673.25.12.075

引言

在移动互联网、大数据等高新技术的助力下，兼具便捷与低成本特点的电子渠道支付交易方式逐渐替代了传统的现金支付方式，形成了市场交易支付的新形态。这为消费者提供了更高效、便捷的金融服务。“互联网+金融”在为商业银行与消费者提供方便的同时，许多潜在的网络安全监管问题为商业银行的健康发展以及用户的财产安全带来了巨大隐患：多渠道多形式的电信诈骗铺天盖地席卷中国金融市场，以伪基站、钓鱼网站、手机木马病毒为主要犯罪工具的电信诈骗分子，不断变换着身份和方式对商业银行以及用户安全问题带来威胁。这使得反欺诈工作面临严峻挑战，电信诈骗已发展成具有严密组织、明确分工的黑色产业链，使客户和金融机构遭受了沉重损失。不仅给数字金融行业的普惠目标和创新发展带来了负面影响，同时也给金融机构和金融科技公司的风险控制带来了沉重的挑战。商业银行是金融机构之一，预防电信诈骗是银行防范操作风险和声誉风险的现实需要，正确并有效地防范金融风险是银行工作的重中之重。所以商业银行预防电信诈骗具有极大的现实意义，尤其是在风险难以控制、客户维权意识逐渐增强的大背景下，明确电信诈骗方式手段并制定安全有效的风险防范策略已经迫在眉睫。

1 文献综述

现有的研究主要是从银行账户风险管理、账户交易的特征和反电信网络诈骗的路径等方面展开分析，并提出相应措施。

1.1 防范电信网络诈骗银行面临的风险

张敏[1]（2023）从银行账户风险管理的角度，通过文献研究法、定性分析法、案例分析法和访谈记录法分析研究了 Y 银行当前账户管理存在制度、操作、管理上的风险，制度风险主要是存在银行业绩考核制度设置不科学、银行的投诉分析处理机制不健全的情况，操作风险主要是存在掩盖真实账户用途，提供虚假资料，存量客户出租、出借银行账户，账户异常交易监测不及时，银行工作人员风险识别能力低的情况，管理风险主要是存在账户准入成本低，智慧机具存在风险，存量账户存在潜在风险的情况，最终得出了有效打击防范电信网络诈骗，缓解当前 Y 银行面临的严峻形式，需要完善监管体系，强化信息沟通，提升人员素质，提高技术水平，加强存量账户管理，优化内部考核制度，加大宣传力度。

1.2 电信网络诈骗犯罪账户交易特征

关于账户交易特征的研究。蔡宁伟和张凯[2]（2021）通过分析常见犯罪账户交易特征，提出电信诈骗个人账户具有交易对手在反电信网络诈骗资金流环节，银行机构承担着重要任务。王大开[3]（2023）通过案例分析法，分析了新型电信网络诈骗犯罪账户主要有跨境、跨区域作案， 隐蔽性强、取证困难，作案方式更新换代快，作案前多进行数据分析定位，受害人群年龄呈现两极化分布的交易特点，明确我国目前打击电信诈骗犯罪面临的困境，最终建议我国应采取完善法律法规、保护公民个人信息、开展事先反诈防范及协同作战的打防方式。陶冶[4]（2023）使用样本分析法，认为电信网络诈骗犯

罪账户有三个交易特征，一是分散转入集中转出 ：三个及三个以上交易对手连续转入后，接着资金转出；二是集中转入分散转出：一个交易对手汇入后，连续向三个及三个以上交易对手转出；三是快进快出：一个或两个交易对手汇入后，接着发生资金转出或多笔多渠道连续资金转出。无论犯罪分子采取何种方式洗钱，资金都会保持一定的完整性，要么化零为整，要么化整为零或整体转移，账户交易明细也就会呈现以上三种基本特征，并且这三种特征的交易一般都是在很短的时间内完成，这是因为诈骗资金很容易被冻结，为了确保“资金安全”，犯罪分子多会采取的策略。

1.3 银行机构反电信网络诈骗路径分析

陶冶[4]（2023）从银行机构反电信网络诈骗路径分析的角度，通过对 200 个样本涉案账户进行分析，思考涉案账户流水特征的背后逻辑，得出了银行机构反电信诈骗的四个有效途径，一是加强对出租出借出售银行卡行为的处罚力度，二是实行智能化管控与人工审核相结合，建立高精度监测模型，实行智能管控，瞬时阻断犯罪交易进行，三是建立受害挽救机制，四是采用生物识别技术。

同时还有对管理机制方面展开研究的。苏如飞[5]（2021）认为可借鉴英国银行业反诈实践，将反电信诈骗纳入银行审慎经营规划中，力促银行强化对消费者利益的保护，同时探索反电信诈骗保险机制，以缓释银行与消费者风险。占再清等[6]（2021）、刘闽浙[7]（2018）等强调银行通过对账户开户的管控、宣传教育、部门协同等建立反诈机制。相关研究也已经出现了具体的技术应用，比如建设银行智慧性交易管控机制，工商银行的大数据外部欺诈系统等。

以上的文献在多方面对预防电信诈骗进行研究，详细地分析了原因，并给出了实用性很强的措施，具有较强的借鉴意义。但是，现有的研究中还没有对银行整体风险防控视角下商业银行预防电信诈骗难点及对策的研究情况，这一领域的研究成果还比较少，对电信诈骗的分类还不够全面。本文分析了电信诈骗各个情况银行面临的风险，详细地罗列了十种类型电信诈骗，具有较强的警示教育意义。

2 电信诈骗的类型及特征

一是刷单返利。骗子通过群发短信、招聘平台、QQ 微信等渠道发布广告，以高额佣金为诱饵吸引事主上钩，要求事主先行垫付保证金、培训费；或者要求事主刷单，先以小额返利为诱饵，诱骗事主投入大量资金后，再把事主拉黑实施诈骗。

二是虚假投资理财。骗子通过网络社交工具、短信、网页发布推广股票、外汇、期货、虚拟货币等投资理财的信息。在与事主取得联系后，通过聊天交流投资经验、拉入投资群聊、听取“投资专家”、“导师”直播课等多种方式，以有内幕消息、掌握漏洞、回报丰厚等谎言骗取事主的信任，诱导事主在其提供的虚假网站、APP 投资，初步小额投资试水，回报利润很高，取得进一步信任，诱导事主加大投入。当事主在投入大量资金后，发现无法提现或全部亏损，与对方交涉时，发现被拉黑或投资理财网站、APP 无法登录。

三是冒充“熟人”或领导。骗子通过非法渠道获取事主的手机通讯录和相关信息，冒充“熟人”主动添加好友，一翻暖心关怀，降低事主的戒备心后，编造各种理由提出转账要求从而骗取钱财。

四是冒充“公检法”。骗子冒充公检法工作人员拨打事主电话，以事主身份信息被盗用、涉嫌洗钱等理由，对事主进行威逼、恐吓，要求将其所有资金转入所谓的“安全账户”配合调查，从而达到诈骗目的。

五是虚假退款。骗子冒充电商平台客服拨打电话或者发送短信谎称事主拍下的货品缺货或产品有质量问题，需要退款赔偿，诱导购买者提供银行卡号、密码等信息，实施诈骗。

六是虚假网络购物。骗子开设虚假购物网站或淘宝店铺，一旦事主下单购买商品，便称系统故障，订单出现问题，需要重新激活。随后，通过 QQ 发送虚假激活网址，事主填写好淘宝账号、银行卡号、密码及验证码后，卡上金额即被划走。

七是网络贷款。骗子会以“无抵押”、“无担保”、“秒到账”、“不查征信”、“月息低”等幌子，吸引事主下载虚假贷款 APP 或登录虚假贷款网站。一旦事主信以为真，骗子即以预付利息、保证金、手续费、刷流水、解冻费等名义实施诈骗。当骗子收钱，便会关闭诈骗 APP 或网站，并将事主拉黑。

八是婚恋交友。骗子伪装为成功人士，通过交友婚介网站、社交平台发布条件优越的虚假征婚交友信息，主动联系社交平台中的异性。取得联系后，以甜言蜜语攻势迷惑事主，取得事主信任后建立所谓的“网恋关系”，甚至以“结婚”为幌子，伺机骗财。骗子往往以“细水长流”的方式行骗，为试探事主的经济实力，提出不同理由、借口，屡次索取不等金额的各种费用。一旦被事主发现戳穿，便立即将事主拉黑，消失无踪。

九是网络游戏。骗子在社交平台发布买卖游戏装备、游戏账号的广告信息，诱导事主在虚假游戏交易平台进行地交易，让事主以“注册费、押金、解冻费”等名义支付各种费用。当事主支付大额费用后，再联系对方时，才发现已被对方拉黑。

十是虚假网站。虚假网站主要是指通过伪造一些合法的网站信息其实是非法牟利的网站。犯罪分子利用伪

基站向广大群众发送网银升级、10086 移动商城兑换现金的虚假链接，一旦事主点击后便在其手机上植入获取银行账号、密码和手机号的木马，从而进一步实施犯罪。

表 1：电信诈骗方式一览表

编号	诈骗方式	诈骗特征
1	刷单返利诈骗	高额佣金
2	虚假投资理财	通过互联网发布投资理财信息
3	冒充“熟人”或领导	非法渠道获取被诈骗人信息
4	冒充“公检法”	要求将资金转入“安全账户”
5	虚假退款	冒充电商平台工作人员实施诈骗
6	虚假网络购物	开设虚假购物网站或淘宝店铺
7	网络贷款	诱导下载虚假贷款 APP 或登录虚假贷款网站
8	婚恋交友	通过交友婚介网站、社交平台发布条件优越的虚假征婚交友信息
9	网络游戏	以“注册费、押金、解冻费”等名义要求支付各种费用
10	虚假网站	犯罪分子利用伪基站向广大群众发送虚假链接

3 电信诈骗对银行风险防控的影响—以中国工商银行十堰分行为例

3.1 电信诈骗对银行产生的风险

近年来，随着客户维权意识不断增强，银行作为金融服务业，其社会地位逐渐下降。客户遇到电信诈骗会投诉银行，造成银行的声誉风险。银行为了避免后续复杂的客户纠纷，达到安抚客户、保障银行声誉的目的，对一些客户进行了直接赔付，这会导致商业银行无可奈何地出现合规风险。直接赔付行为直接导致后来别的被诈骗的客户都认为银行可以赔偿损失，便对银行进行诉讼，追索损失，造成银行的法律风险。这样的处理方式既对银行正面处理电信诈骗问题造成了不利的影响，同样也不利于电信诈骗案件得到真正妥善的处理，给犯罪分子提供了诈骗的土壤，形成了恶性循环。近两年商业银行因防范电信诈骗大面积对风险账户进行管控的问题引发了社会舆情事件，引起国务院、监管机构的高度重视，会给商业银行造成舆情风险。表 2 是工行十堰分行 2023 年统计的主要情况对商业银行造成的风险。

表 2：电信诈骗各种情况对商业银行造成的风险

编号	情况说明	产生的风险	占比
1	客户遇到电信诈骗会投诉银行	声誉风险	79.23%
2	对客户直接进行赔付	经济损失风险	10.34%
3	客户诉讼商业银行	法律风险	3.26%
4	大面积风险账户管控问题引发社会舆情事件	舆情风险	0.23%
5	如果银行在反诈骗方面的措施不到位，可能会面临监管部门的处罚和法律责任	合规风险	0.20%
6	电信诈骗可能导致银行内部控制系统的漏洞被利用，增加操作风险	操作风险	0.16%
7	电信诈骗可能导致客户的个人信息泄露，银行需要加强账户开立管理和个人信息安全保护，以维护与客户的良好关系。	客户关系风险	0.18%
8	大规模的电信诈骗可能会导致银行短期内出现资金流动性问题	流动性风险	0.08%
9	随着诈骗手段的不断升级，银行需要不断提升技术手段来防范和应对电信诈骗，这要求银行在信息技术安全方面进行持续投入	技术安全风险	6.32%
合计			100%

数据来源：中国工商银行十堰分行

3.2 商业银行处理电信诈骗的难点分析

电信诈骗手段随数字化技术的进展不断提升。电信诈骗的方式也从原来的的盗号、盗刷等低级手段渐渐演变成目前的真实场景化行为，数字化电信诈骗渗透的业务环节多，手段新颖，具有很强的隐蔽性及危害性。数字电信诈骗的目标也从一家公司到多家公司进而扩展到多个行业。2023 年，公安部针对缅北电诈团伙开展专项打击治理行动，累计移交电诈分子 4.4 万人，成效明显。但根据公安通报，犯罪团伙境外流窜，柬埔寨、老挝、菲律宾、阿联酋等地逐渐成为新的电诈重灾区。因此反欺诈系统一方面需要各行各业的联动，相互之间增强数据、内容的交流共享，打破屏障；另一方面也需要各监管部门联合行动建立完整的治理体系。

3.2.1 场景不断增多

数字电信诈骗行为呈现场景化，且场景不断增多。常见的数字电信诈骗场景包括网络借贷、网络支付、消费金融和供应链金融四个方面。在网络借贷、网络支付和消费金融场景中，电信诈骗行为一般会发生在账户注

册、激活、登录、交易、信息修改等各个环节。在供应链金融场景下，隐瞒企业经营信息来达到偷税漏税，骗取信贷补助的行为比较常见。

3.2.2 受害群体年轻化

随着科技发展和互联网的普及，我国网民人数不断增多，特别是后疫情时代，互联网已经成为重要的工作、学习和生活的途径，这给了诈骗分子扩大受骗用户接触面和提升诈骗手法提供可乘之机，导致电信诈骗风险呈上升态势。

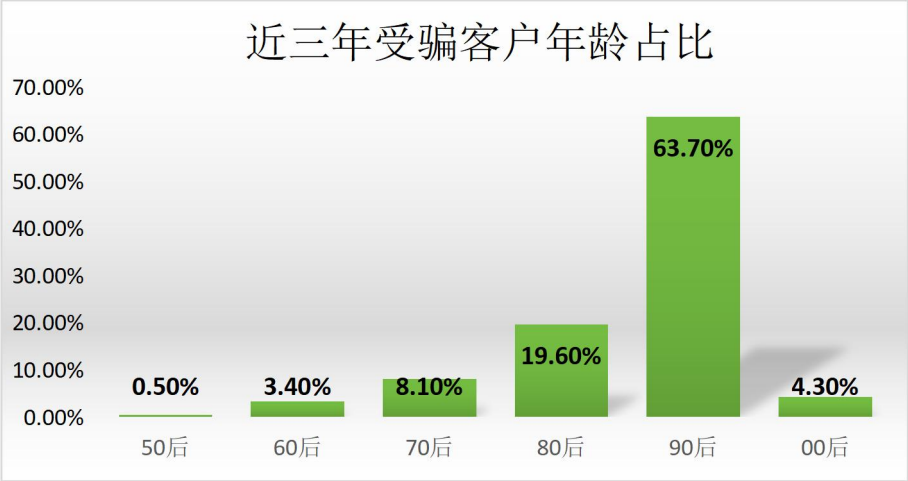

图 1 近三年十堰数字电信诈骗受骗用户年龄占比

图 1 为近三年十堰数字电信诈骗受骗用户年龄占比（数据来源：中国工商银行十堰支行），由图 1 可以看出，90 后已经成为诈骗分子重点诈骗对象，受骗人数已经超过表中其他人数总和，占比高达 63.7%；同时 00 后受骗用户也在上升，达到 4.3%，上述数据反映出诈骗分子的狩猎目标正逐步转向防范意识较差的年轻群体。

3.2.3 手段快速变化

随着互联网的高速发展，目前形成了十类诈骗手段，并且诈骗手段仍在持续快速地更新和发展。刷单返利、虚假网络投资理财、冒充电商物流客服、虚假征信、虚假网络贷款五大高发类案件突出，共计占比 72%。当前科技欺诈手段呈现七种发展趋势。一是覆盖面更广。犯罪分子在实施犯罪的过程中通过电话、短信、社交平台、网络等手段地毯式给群众发布虚假信息，造成较大范围的损害。二是手段更新更快。诈骗分子的犯罪手段层出不穷，通过互联网网站、网络链接、手机病毒、二维码等高科技手段实施犯罪。三是犯罪团伙反侦查的能力更强。在真实的诈骗案件中，他们往往通常采取远程的非接触式的诈骗，根据犯罪需要分饰不同角色、承担不同的分工。四是隐蔽更深。随着国内打击力度加大，部分犯罪分子隐匿在国外，租用服务器通过网络、电话对国内民众实施诈骗。五是抓捕难度更大。黑色产业团伙逐渐专业化、组织化，黑色产业团队内部分工明确，核心成员利用远程操作、不定期更换窝点等手段摆脱执部门的追踪和抓捕，导致执法机构无法做到全链条打击和抓捕。六是追赃更难。诈骗分子在成功骗取资金后，会在短时间内快速通过多种途径进行洗钱，给追讨诈骗资金增加较大难度。

面对发展迅猛的黑产团伙和黑产技术，科技反欺诈行动和技术都面临空前巨大的压力。迫切需要有关部门积极利用基于大数据、云计算、区块链等技术的金融科技手段，提高跨行业、跨市场交叉性金融风险防控能力，为金融反欺诈提供有力支持。

3.3 商业银行做好风险管理的意义

银行风险管理是当银行识别或者预估到风险时采取必要措施而减少或者避免经济损失，保障经营资金运行安全的行为。银行风险管理的措施包括风险预防，风险规避，风险分散，风险转嫁，风险抑制，风险补偿。银行监管机构银保监会从成立开始，借鉴国际经验，出台相关的监管指引，推动银行风险管理的快速发展。同时，随着市场化透明度越来越高，银行定期对外披露相关信息，或者接受会计事务所的审计等，资本市场会对同业经营业绩比较，这也对银行的风险管理发展起到了推动作用。同时银行自身暴露出来的风险点是促使银行进行风险管理的内生动力。银行在市场中承担着重要的角色，重视风险管理不仅能够使银行取得长足发展，树立良好形象，在同业竞争中取得优势，同时，只有重视银行风险管理，才能保障公众财产不受损失，才能维持金融市场的稳定，才能稳定社会经济发展[1]。

4 商业银行预防电信诈骗对策

在金融科技创新的驱动下，银行业正在演变成智能、开放和生态的发展模式。随着数字化银行的高速发展，以便为客户提供卓越的服务体验，银行的经营方式变得更加灵活和开放，然而也逐渐成为网络黑灰产业的主要目标。商业银行预防电信诈骗是防范风险的需要，是践

行社会责任的需要，是保护客户资金安全的需要，更是维护社会和谐稳定的需要，所以一直是各商业银行的重点工作。商业银行预防电信诈骗主要有以下五个对策。

4.1 多维资源整合

商业银行依托大数据技术，对海量数据源进行分析整合，消除不同地域、领域、部门间资源无法共享的劣势，对资源和数据进行充分利用。资源整合主要包括数据资源与计算资源两种形式的整合。数据资源的整合包括对海量不同数据源的捕捉汇总，寻找不同数据之间的关联性，进行合理的存储结构设计，按照预先设定好的主题与维度结构化存储，把杂乱无章的数据规范化。计算资源整合主要利用分布式计算、性能计算、负载均衡的并行计算、网络存储、冗余热备份和虚拟化等计算机技术，来达到对计算资源的有效分配。

4.2 开发预警系统

借助当前的大数据技术的资源整合优势，开发数据预警系统，实现对大量数据的实时抓取和计算，并及早发现潜在风险并做出预警。数据预警系统的作用是在收集合理的数据资源并进行计算资源整合后，充分有效的利用服务器，将海量数据实时计算的压力分摊减小，使得系统可以在最短的时间内，实时地对发生的行为数据做出决策，分批次、分阶段生产预警信息，使得场景不再局限于单纯的流式计算，实现微批处理的实时性，并在实时计算中，加入复杂的关联条件，使得决策信息多样化，显著提高预警精准性。

4.3 建立反诈数据模型

精准而科学的数据模型需要强大的基础数据积累与优质的资源整合。在基础数据积累方面，由于反欺诈场景的多样性与复杂性，单一的反欺诈，模型应对不同的欺诈场景处理能力有限。因此，应结合实时数据和非实时数据两种方式对客户行为进行采集，其中，实时数据主要针对客户单一交易行为进行预警，非实时数据主要针对客户一段时间内累积的历史交易情况进行预警。在优感资源整合方面，基于面向主题的数据仓库对采集数据进行存储，将海量数据组织汇总为较高层次的主题，将相关主题集成归并为主题域，实现对数据的高效操作与处理。依托于优质的计算资源实现强大的分析计算能力，构造针对不同场景的海量模型，同时将海量模型集成整合心形成一个完善而科学的反欺诈数据模型系统。

4.4 重视阶段反诈

在事前阶段，传统方式是借助新型身份验证技术工具，提升金融业务稳健性。随着金融业务的快速发展，商业银行现有的 U 盾、密码器等传统认证手段，虽然安全性较强，但使用过程繁琐，实用性不高，逐渐导致产品实用性和安全性出现不平衡的情况。可以通过建立交易认证安全基线，并引入设备指纹、移动网关等身份认证增强技术，提升金融业务实用性，规范各认证手段使用场景，强化金融业务对电信诈骗的抵御能力。

在事中阶段，使用覆盖各种通道的创新抗击模式，以增强实时防御效应。而作为银行最常见且欺诈率最高的转账汇款业务，它涉及多个通道，如柜台、ATM 机、智能设备、网络银行和手机银行，以及多个业务部门。银行各个部门积极配合，共同讨论并施行流程改进策略和系统阻挡方法，实现系统与欺诈账户的连结和自动阻断。创立防欺诈风险管理平台，自动与业务系统相连，构建覆盖所有通道、全天候电信诈骗抗击体系，对转账汇款交易实时筛查和预警控制。

在事后阶段，强化警方与银行的信息协作，共同创建联合防控的机制。通过使用欺诈账户作为入口，与公安部门实现信息互通，在全局及地区层面上构建出一个欺诈账户的共享和协作机制。

4.5 加强反诈宣传

一方面是提高宣传频率。银行网点是接触客户频率最高的地方，也是客户最信任银行的地方。客户走进银行网点，在与工作人员沟通过程中，工作人员可以将反诈知识及时传递给客户。在客户等待办理业务过程中，通过播放反诈宣传视频，银行工作人员反诈知识小课堂，或者是讲解真实的案例，用通俗易懂的方式将反诈知识传递给大众。同时，走进银行网点的客户，地域、年龄分布广，在银行网点讲解反诈知识，受众群体广，效果好。进而将电信诈骗等违法犯罪手段方式，以及违规使用银行账户，出租出借银行账户的危害性和相关的法律责任都给客户普及到，起到真正的宣传效果。另一方面是针对特定人群进行宣传。根据数据显示，涉及电信诈骗的账户多为老人，村民，学生等特定群体。商业银行通过走进社区，走进校园，走进村庄等形式，对特定人群普及电信网络诈骗案例，将电信诈骗的手段方式以及出租出借银行账户的风险和危害以及违法应承担的相关法律责任向特定人群进行说明，让群众对电信诈骗和合法使用账户有更加深刻的认识。

4.6 完善银行内部制度管理

一方面是制定责任追究制度。银行设置有关账户的考核指标是银行现阶段发展的趋势。银行在设置考核项时应该将账户开立之后的风险考虑进去。或者在账户开立时，如果是为了完成考核指标而进行的批量账户开立，在账户开立的最初，就将营销人进行登记，贯彻“谁的客户谁负责”原则。如果账户后续出现风险事件，将对营销人采取一定的惩罚措施。强化员工的责任意识和风险意识。日常柜面和智慧机具的账户开立，贯彻“谁开

户谁负责”，对于智慧机具谁授权谁负责。不管是在日常银行内部检查，还是银行上级机构检查的时候，针对排查出来的风险账户，严肃追责账户开立人员，以此来加强全员的对于电信诈骗账户风险管理意识[17]。

另一方面是严格贯彻落实合规制度。树立“合规从高层做起”的理念，银行的高管人员不仅要成为合规文化的倡议者，同时也要成为合规文化的践行者，这样才能以上率下；员工要把“合规文化人人有责”内化于心，外化于行，不管什么岗位要确保行为“时时合规”，同时要在发展业务时，思考合规文化如何建设的更好，成为合规文化的献言者。要明确导向。使合规文化发挥最大的作用，就要树立将短期整改转化为长效机制建设理念，要树立事前防控大于事后补救的观念，将合规文化内化为管理动力。要形成合力。合规不是一个部门的事情 ，也不是几个部门的事情，而是需要所有部门之间沟通协作，明确各岗位职责，相互监督，相互制约。同时合规管理部门牵头进行合规检查，及时开展合规风险自查，及时评估合规管理的有效性，发现问题，及时纠正。要突出重点。首先对内部现有的规章，制度，业务流程进行有效梳理，发现合规漏洞，及时查漏补缺；开展新业务，合规审查在前，实施在后，实施过程中，做好合规评估，发现违规及早制止，及早制定相关措施；针对重点岗位，重点业务，重点环节，加大合规管理力度，紧盯内控合规薄弱环节。要强化监督问责。首先是优化全面的监督问责制度，树立起违规必究的警戒线。发生违规问题，不仅要处理不严格执行相关制度的直接责任人，同时管理责任人也要追究，也要追究高管的失职责任，也要追究对于检查不到位，监督不到位的合规部门的相关人员和其他相关部门的人员；六要加强保障支撑。设立合理的考核机制和考核办法，既能起到约束的作用，又能起到激励的作用；提高合规人才的技能，加大合规人才培养力度，培养专业复合型人才，不仅能够精通业务，同时能够对合规管理发挥促进作用；加强合规系统建设，为高效科学的合规管理保驾护航。七要细化合规管理，落实合规制度，形成合规管理长效机制。合规管理要做到不走过场，真正将制度落实到实际工作中，自查工作全覆盖，违规操作深究原因，源头治理，整改工作做到回头看，让合规文化根植基层，从根本上减少账户发生风险。

参考文献

[1]张敏.基于防范电信网络诈骗的银行账户风险管理及对策研究[D].山西财经大学,2024.DOI:10.27283/d.cnki.gsxcc.2023.000123.
[2]蔡宁伟和张凯,2021,《可疑交易分析中常见类罪的交易特征》,《金融会计》第 5 期,第 40～46 页。
[3]王大开.新型电信网络诈骗案件特征及治理对策[J].互联网天地,2023(12):39-43.
[4]陶冶.银行机构反电信网络诈骗路径分析——基于涉案账户流水[J].金融会计,2023(07):68-74.
[5]苏如飞,2021,《英国银行业反电信诈骗实践及启示》,《中国信用卡》第 6 期,第 66～69 页。
[6]占再清、向圣俊、冯安宁、邓凤姣、王欣和马洁,2021,《深化银行账户管理从源头治理违法犯罪行为》,《金融会计》第 1 期,第 60～63 页。
[7]刘闽浙,2018,《金融机构防范电信诈骗现状、问题与对策》,《武汉金融》第 7 期,第 78～80 页。
[8]周影.从三起电信诈骗案看Ⅱ类Ⅲ类个人银行账户管理[J].现代商业银行,2023,(23):41-43.
[9]本刊编辑部.银行是防止电信诈骗的重要防线——金融消费者权益保护典型案例四则[J].中国银行业,2023,(08):91-93.
[10]仇兆燕.电信诈骗套路多年轻人切莫“孤注一掷”[N].中国银行保险报,2023-09-26(005).DOI:10.28049/n.cnki.ncbxb.2023.003496.
[11]李颖超,杜晓彤.电信网络诈骗花样不断翻新金融反诈行动升级[N].证券时报,2022-11-11(A05).DOI:10.38329/n.cnki.nzjsb.2022.003789.
[12]家俊辉.电信诈骗“资金链”治理步入深水区：攻防对抗升级部分诈骗资金利用虚拟货币规避监测[N].21 世纪经济报道,2022-04-15(007).DOI:10.28723/n.cnki.nsjbd.2022.001389.
[13]刘金林.对电信诈骗损失，银行、电信企业或担责[N].检察日报,2016-09-28(003).
[14]办理网络电信诈骗案件如何破解证据难题[N].检察日报,2016-07-31(003).
[15]徐德高,聂彭飞.电信诈骗犯罪呈现四个新动向[N].检察日报,2016-04-06(008).
[16]陈磊.电信诈骗为何猖獗[N].法制日报,2015-11-16(008).
[17]刘闽浙，金融机构防范电信网络诈骗现状、问题与对策[J]，武汉金融，2018，No.223(07):80-82.

作者简介：宋磊，（1996.7-），女，河南光山县人，硕士研究生，研究方向：金融风险管理。