

关于《中华人民共和国反电信网络诈骗法》银行业金融机构作为与不作为法律解读与风险提示

◆金 霁

(中国农业银行股份有限公司广州分行内控与法律合规部, 广东 广州 510623)

【摘要】对于银行业金融机构来讲,必须及时地对各种法律法规进行深入的研究,只有这样才能有效地规避各种法律风险带来的损失。本文主要就针对《中华人民共和国反电信网络诈骗法》中关于银行业金融机构作为与不作为的内容进行解读,希望可以帮助银行业金融机构有效地规避相应的法律风险。

【关键词】银行业金融机构;不作为;法律风险;《中华人民共和国反电信网络诈骗法》

电信网络诈骗案件近年来呈现高发态势,对社会经济产生了影响。《中华人民共和国反电信网络诈骗法》(以下简称《反电信网络诈骗法》或《本法》)已于2022年9月2日公布,2022年12月1日实施。此法总共有七章内容,从电信、金融、互联网三个领域规定了反电信网络诈骗的具体措施及法律责任。本文将根据总则内容,解读金融治理篇、综合措施篇、法律责任篇,重点阐述银行业金融机构在反电信网络诈骗案件当中要采取哪些举措?哪些规矩又是应当遵守不能逾越的?

一、总则规定

(一)反电信网络诈骗宗旨

《反电信网络诈骗法》规定了反电信网络诈骗工作的宗旨。其第四条还规定了反电信网络诈骗治理的基本原则,坚持“十六字”方针,强化“系统思维”“法治观念”,做到“齐抓共管”“群防群治”。精准防治,保护大众的财产安全和合法权益不受侵犯,保障人们正常生产经营活动和生活便利。

(二)案件管辖范围

《反电信网络诈骗法》第三条规定了案件管辖原则,分别是第一类属地原则,在我国境内实施;第二类属人原则,犯罪主体为我国公民;第三类保护原则,保护原则侵犯的仍然是我国领土安全和公民的合法权益。此三类电信网络诈骗活动均适用《本法》。

(三)反电信网络诈骗主体

反电信网络诈骗主体包括国务院及各级地方政府、公检法机关、电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者。各级公安机关牵头反电信网络诈骗工作,与以往对比,公安机关对电信诈骗行为具有治安处罚权。法院依然行使审判职能,检察机关可针对特定受害人提起公益诉讼。

(四)电信诈骗受害者

跟《反洗钱法》没有明确的被害人对比,《反电信网络诈骗法》有明确的被害人。电信诈骗受害人群比较多的是老年人及青少年群体。根据《反电信网络诈骗法》及最高人民法院关于反电信网络诈骗刑事案件的相关司法解释规定,法律将诈骗老年人及青少年群体、残疾人以及丧失劳动能力人的财物作为从重处罚情节。电信网络诈骗花样层出不穷,弱势群体不懂得甄别,容易上当受骗。

(五)注重个人信息保护

《中华人民共和国民法典》出台已将个人信息保护内容作为独立章节规定,《个人信息保护法》也已颁布实施。《反电信网络诈骗法》也将个人信息保护作为单独条款进行规范,包括国家公权力机关,法院,检察院,公安机关,金融机构,电信、网信、市场监管等有关部门在本领域进行反电信网络诈骗活动中都要高度重视个人信息保护,对个人信息处理建规立制。部门、单位对可疑交易信息、贷款信息予以重点保护,推动个人信息保护举措,以防止公安机关根据个人信息来源追究相关单位责任。

(六)法律适用

反电信网络诈骗工作所涉及的相关法律依据,同时适用《网络安全法》《个人信息保护法》《反洗钱法》等相关法律规定。

二、金融治理规定

《反电信网络诈骗法》的出台对银行业金融机构产生了较大的影响。《反电信网络诈骗法》第十五条至第二十条作为第三章金融治理篇、综合措施篇。该法也规定了银行业金融机构、非银行支付机构在反电信网络诈骗工作当中应当采取的措施,下面仅从银行业金融机构阐述,非银行支付机构参照执行。

(一)银行业金融机构建立反电信网络诈骗必要机制

(1)建立客户尽职调查制度。当前我国银行业金融机构普遍已根据反洗钱工作要求建立了客户尽职调查制度,与反

洗钱工作要求对比,《反电信网络诈骗法》规定了尽职调查的具体措施。《反电信网络诈骗法》要求银行机构对企业账户建立开立企业账户相关信息共享查询系统,提供联网核查服务。过去十几年,银行出现的伪卡损失赔偿案件或者第三方支付案件,因系统内从总行到下属分支机构的由上而下、横向贯穿的联动核查机制尚未建立,犯罪分子在全国多个营业网点将涉案资金短期内转入转出,为诈骗行为提供了转账渠道,司法实践当中银行根据注意义务承担了较重的损害赔偿赔偿责任。《本法》出台对银行机构在全国范围内建立联动核查机制提供了法律依据。(2)建立完善符合电信网络诈骗活动特征的异常账户和可疑交易监测机制。国内银行业金融机构已在近些年反洗钱工作中开展了异常账户核查和可疑交易监测,《反电信网络诈骗法》对异常账户和可疑交易监测规定了更加详细的监测举措。对异常账户和可疑交易,银行金融机构应采取必要的防范管控措施,管控措施包括核实交易、重新核验身份、中止有关业务等,如银行对异常开户情形可以拒绝开户或者加强核查。如跨行开户,客户拒绝提供真实材料的加强核查。中国人民银行可以通过互联网企业收集异常客户必要的交易信息、设备位置信息。银行需确保交易信息的真实、完整和支付流程的一致性,并注意留存被害人的相关交易证据资料,确保证据资料的真实性、完整性和合法性。比如,对客户账户的审查有无明显可疑特征,账户是否为客户本人使用,账户开立后有无立即开展核查,且及时进行管控改进措施,如触发如法定代表人失联等预警信号,客户有无通过威胁投诉等提升账户额度,一旦发现账户异常,有无马上进行核查,对涉案特征明显且当事人失联的账户马上进行账户管控。(3)配合公安部门办理查询、止付、冻结、解冻和资金返回等救济措施。(4)对从业人员和用户开展反电信网络诈骗宣传。《本法》第三十条规定,银行业金融机构应当对从业人员和用户开展反电信网络诈骗宣传。具体宣传方式包括:将反电信网络诈骗培训贯穿于从业人员的日常培训当中;将防范电信网络诈骗措施落实到有关业务活动中;对新型电信网络诈骗方式作案手段及时向用户作出提醒,对非法买卖、出租、出借个人账户被用于电信网络诈骗的需承担的法律后果进行警示教育。(5)银行业金融机构违反《反电信网络诈骗法》等相关法律法规规定,承担的责任包括刑事、行政以及民事责任。如果说,《刑法》对反电信网络诈骗活动是事后补救作用,则《反电信网络诈骗法》的出台,则是前端预防作用。

上述第1、2、3项举措是银行业金融机构开展反电信网络诈骗工作的必备措施。根据《本法》第二十八条规定,金融部门依照职责对银行业金融机构落实《本法》规定情况进行监督检查。《本法》第四十条规定,未按照规定落实上述第1、2、3项举措,有一项未落实的,视情节轻重需承担

相应法律责任,行政处罚措施包括警告、通报批评、罚款,罚款金额最高达到500万元。情节严重的,可责令吊销许可证或营业执照,对直接主管人员和其他直接责任人员处以罚款,罚款金额最低一万元、最高二十万元。

(二)银行业金融机构竞业禁止规定

(1)不得为他人实施电信网络诈骗活动出售、提供个人信息。参见《本法》第二十五条第一款规定,第四十二条对违反第二十五条第一款规定确定了法律责任,法律责任是没收违法所得,由公安机关或有关主管部门处罚款;情节严重的,由公安机关并处十五日以下拘留。(2)不得非法买卖、出租、出借银行账户,不得提供实名核验帮助;不得假冒他人身份或虚构代理关系开立银行账户等。参见《本法》第三十一条规定,第四十四条规定,违反第三十一条规定的,没收违法所得,由公安机关处以罚款;情节严重的,并处十五日以下拘留。银行对客户开立账户要进行客户身份识别,近年出现过因系统内一级分行因未对客户开立账户进行身份识别而被人民银行处罚的案例。另外,建议将第三十一条规定纳入到员工行为排查当中,以清除行业“内鬼”。明知他人实施电信网络诈骗犯罪而为其提供信用卡、资金支付结算账户的,按照共同犯罪处理。(3)限制开立银行账户的数量,开立银行账户的数量不得超过我国有关规定。《反电信网络诈骗法》第十五条、第十六条、第十七条都是开户的规定,目前公安部门要求个人开户控制开户的数量,但是人民银行对开户数量的上限尚无明示。据了解,人民银行正在授权中国银联建立跨行核查系统,比如,以后在各大银行开户的总数量会有限制。以后在身份证核查基础上,还会增加跨行开户数量核验功能。(4)对经识别存在异常开户情形的,银行业金融机构有权加强核查或拒绝开户。银行从业人员要树立反诈观念,反诈权力要用好用足,该拒绝开户就拒绝,不要害怕投诉,敢于向电信网络诈骗活动说“不”。

(三)外部协助银行业金融机构推行反诈活动机制

(1)电信业务经营者、互联网服务提供者对提供支付结算服务从事涉诈支持活动进行监测识别和处置。参见《本法》第二十五条第二款规定,第四十三条针对违反本条第二款规定的也作出了没收违法所得,处以罚款;情节严重的,给予拘留的处罚规定。有的科技互联网公司既做反诈,又将技术卖给诈骗团伙,黑白通吃。(2)对涉诈违法犯罪线索风险信息,互联网服务提供者如有发现应移送公安、金融、电信网信等部门,有关部门应建立完善反馈机制。现在洗钱手段变化多端,方式多元,新的黑灰产业链不断滋生。互联网时代来临,给反诈侦查带来了新的考验,很多犯罪方法都离不开互联网,互联网服务提供者如发现相关网络电信诈骗线索,应及时移交公安机关或相关主管部门。

(四)公权力机关建立反电信网络诈骗机制

《反电信网络诈骗法》注重综合治理,反诈职能由公安主抓变为多元共治。如工商部门依法核验企业实名登记履行身份信息职责。金融监管部门统筹负责本行业领域反制技术措施建设。通过国家网络身份认证公共服务,银行业金融机构对存在涉诈异常的银行账户用户身份重新进行核验。需要重点提及的是公安机关的反诈措施,还有针对电信网络诈骗重灾区,国务院有权采取临时管控措施。

(1)公安机关会同金融部门组织、银行业金融机构建立预警劝阻系统,完善涉案资金处置制度。反诈机制的建立依赖于“警银协作”,具体参见《本法》第三十四条。公安机关依照国家侦查权,以往对不构成刑法犯罪的反电信网络诈骗活动,公安机关只能进行批评教育,现根据《反电信网络诈骗法》规定,公安机关可以对实施电信诈骗活动行为人进行治安处罚。比如,对银行开立账户审核不严又涉及电信网络诈骗的,公安机关有权对银行从业人员进行拘留或者治安处罚。对从事反电信网络诈骗活动的单位,公安机关既可以罚机构,又可以罚个人,惩戒纳入个人银行征信范围。对从事过反电信网络诈骗的个人,规定不能从事金融业,这对尚未参加工作的学生从事电信网络诈骗活动具有惩戒意义。

(2)针对电信网络诈骗活动严重的“重灾区”,国务院可采取临时风险防范措施。我国福建安溪县电信网络诈骗活动猖獗,我国可依据《本法》的规定对该县从互联网、电信、金融机构三大领域制定相关的风险防范措施。《反电信网络诈骗法》的颁布是深化反诈工作的迫切需要。针对反电信网络诈骗活动,要建立外部协助银行推行反诈活动机制,协助银行开展反诈活动的主体不仅包括电信业务经营者、互联网服务提供者,还包括公权力机关。针对当前电信网络诈骗活动猖獗的现象,实际反诈工作仍有很多实操性东西亟待解决,但《反电信网络诈骗法》的颁布为反电信网络诈骗活动提供了行动指南。

《反电信网络诈骗法》的出台,使我国反电信网络诈骗活动得到了推动。跟以往反电信网络诈骗网络活动对比,现在反电信网络诈骗活动开始注重综合治理,反诈职能由公安主

抓变为多元共治。强调源头治理,企业行业由协同配合变为主体参与。注重前端防范,理念方针由亡羊补牢变为未雨绸缪。明确惩处力度,法律根据由分散零碎变为系统完备。

参考文献:

- [1]王铭雪.电信网络诈骗特点及打防对策研究——以T市X区公安分局警情为例[J].法制与经济,2021,30(10):39-45.
- [2]李荣,吴汉迪,段继平.电信网络违法犯罪治理研究[J].网络信息法学研究,2021(02):166-178,296-297.
- [3]阴建峰,张印.电信网络诈骗帮助行为刑事责任体系之衔接——兼评《反电信网络诈骗法(草案)》第37条[J].山东警察学院学报,2021,33(06):39-50.
- [4]伍珂珂.商业银行防控电信网络诈骗风险的措施建议[J].中国信用卡,2021(11):70-74.
- [5]汤瑜.反诈立法为电信网络诈骗攻防战提供坚实法律保障[N].民主与法制时报,2021-11-04(003).
- [6]张宪双.防范电信网络诈骗 守护美好生活[N].四平日报,2021-09-28(003).
- [7]郭若蓓.防范电信诈骗视角下M银行账户风险管理研究[D].济南:山东师范大学,2021.
- [8]于琦.商业银行防范电信诈骗的风险管理对策研究[D].昆明:云南大学,2020.
- [9]刘惠智.电信诈骗案件中涉及银行的电子证据研究[D].广州:华南理工大学,2019.
- [10]田甲.论电信诈骗中银行的审慎义务[D].大连:大连海事大学,2018.
- [11]刘闽浙.金融机构防范电信诈骗现状、问题与对策[J].武汉金融,2018(07):78-80.
- [12]刘杰.基于社会责任的国有商业银行防范电信诈骗对策研究[D].保定:河北大学,2018.
- [13]沈文娟.基于银行电信诈骗事件探析金融机构风险防范策略[J].黑龙江金融,2017(10):74-76.

作者简介:

金霁(1978—),女,汉族,湖北黄冈人,本科,研究方向:民法金融业务。