中华人民共和国反电信网络诈骗法（草案）

（二次审议稿）

目　　录

第一章　总　　则

第二章　电信治理

第三章　金融治理

第四章　互联网治理

第五章　综合治理措施

第六章　法律责任

第七章　附　　则

第一章　总　　则

第一条　为了预防、遏制和惩治电信网络诈骗活动，加强反电信网络诈骗工作，保护公民和组织的合法权益，维护社会稳定和国家安全，根据宪法，制定本法。

第二条　本法所称电信网络诈骗，是指以非法占有为目的，利用电信网络技术手段，通过远程、非接触方式，诈骗公私财物的行为。

第三条　打击治理中华人民共和国境内的电信网络诈骗活动或者中华人民共和国公民在境外实施的电信网络诈骗活动，适用本法。

境外的组织、个人针对中华人民共和国境内实施电信网络诈骗活动的，或者为他人实施针对境内的电信网络诈骗活动提供产品、服务等帮助的，依照本法有关规定处理和追究责任。

第四条　反电信网络诈骗工作坚持以人民为中心，统筹发展和安全；坚持系统观念、法治思维，注重源头治理、综合治理；坚持齐抓共管、群防群治，全面落实打防管控各项措施，加强社会宣传教育防范；坚持精准防治，保障正常生产经营活动和群众生活便利。

第五条　反电信网络诈骗工作应当依法进行，维护公民和组织的合法权益。

有关部门和单位、个人应当对在反电信网络诈骗工作过程中知悉的国家秘密、商业秘密和个人隐私予以保密。

第六条 国务院建立反电信网络诈骗工作机制，统筹协调打击治理工作。

地方各级人民政府负责本行政区域内反电信网络诈骗工作，确定反电信网络诈骗目标任务和工作机制，组织开展综合治理。

公安机关组织协调反电信网络诈骗工作，金融、电信、网信、市场监管等有关主管部门承担监管主体责任，依照职责负责本行业领域反电信网络诈骗工作。

电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者承担风险防控责任，建立反电信网络诈骗内部控制机制和安全责任制度，加强新业务涉诈风险安全评估。

第七条 有关部门、单位在反电信网络诈骗工作中应当密切协作，实现跨行业、跨地域协同配合、快速联动，加强专业队伍建设，有效打击治理电信网络诈骗活动。

第八条 地方各级人民政府和有关部门应当加强反电信网络诈骗宣传，普及法律知识，提高公众对各类新型电信网络诈骗方式的识骗能力和防骗意识。

教育行政、市场监管、民政等有关部门和村民委员会、居民委员会，应当结合电信网络诈骗受害群体的分布等特征，有针对性地开展反电信网络诈骗宣传教育防范进学校、进企业、进社区、进农村、进家庭等活动。

单位、个人应当加强电信网络诈骗防范意识，履行基本审慎义务，协助、配合有关部门依照本法规定开展反电信网络诈骗工作。

第二章　电信治理

第九条　电信业务经营者应当依法落实电话用户真实身份信息登记制度。

基础电信企业和移动通信转售企业应当承担对代理商落实电话实名制管理责任，在协议中明确代理商实名制登记的责任和有关违约处置措施。

第十条　办理电话卡不得超出国家有关规定限制的数量。

对经识别存在异常办卡情形的，电信业务经营者有权加强核查或者拒绝办卡。

国务院电信主管部门组织建立电话用户开卡数量核验机制和风险信息共享机制，并为用户查询名下电话卡信息提供便捷渠道。

第十一条　电信业务经营者对监测识别的涉诈异常电话卡用户应当重新进行实名核验，根据风险等级采取有区别的、相应的核验措施。对未按规定核验或者核验未通过的，电信业务经营者可以限制、暂停有关电话卡功能。

第十二条　电信业务经营者建立物联网卡用户风险评估制度，评估未通过的，不得向其销售物联网卡；严格登记物联网卡用户身份信息；采取有效技术措施限定物联网卡开通功能、使用场景和适用设备。

单位用户从电信业务经营者购买物联网卡再将载有物联网卡

的设备销售给其他用户的，应当核验和登记用户身份信息，并将销量、存量及用户实名信息传送给号码归属的电信业务经营者。

电信业务经营者对物联网卡的使用建立监测预警机制。对存在异常使用情形的，应当采取暂停服务、重新核验身份和使用场景或者其他合同约定的处置措施。

第十三条 电信业务经营者应当规范真实主叫号码传送和电信线路出租，对改号电话进行封堵拦截和溯源核查。

电信业务经营者应当严格规范国际通信业务出入口局主叫号码传送，真实、准确向用户提示来电号码所属国家或者地区，对网内和网间虚假主叫、不规范主叫进行识别、拦截。

第十四条 任何单位和个人不得非法制造、销售、提供或者使用下列设备、软件：

（一）电话卡批量插入设备；

（二）具有改变主叫号码、虚拟拨号、互联网电话违规接入公用电信网络等功能的设备、软件；

（三）批量账号、网络地址自动切换系统，批量接收提供短信验证、语音验证的平台；

（四）其他专门或者主要用于实施电信网络诈骗等违法犯罪的设备、软件。

电信业务经营者、互联网服务提供者应当采取技术措施，及时识别、阻断前款规定的非法设备、软件接入网络，并向公安机关和相关行业主管部门报告。

第三章　金融治理

第十五条　银行业金融机构、非银行支付机构为客户开立银行账户、支付账户等支付工具及提供支付服务，和与客户业务关系存续期间，应当建立客户尽职调查制度，依法识别受益所有人，采取相应风险管理措施，防范银行账户、支付账户等被用于电信网络诈骗活动。

第十六条　开立银行账户、支付账户不得超出国家有关规定限制的数量。

对经识别存在异常开户情形的，银行业金融机构、非银行支付机构有权加强核查或者拒绝开户。

中国人民银行、国务院银行业监督管理机构组织有关清算机构建立跨机构开户数量核验机制和风险信息共享机制，并为客户提供查询名下银行账户、支付账户的便捷渠道。银行业金融机构、非银行支付机构应当按照国家有关规定提供开户情况和有关风险信息。相关信息不得用于风险防控以外的其他用途。

第十七条　银行业金融机构、非银行支付机构应当建立开立企业账户异常情形的风险防控机制。金融、电信、市场监管、税务等有关主管部门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。

市场监管部门应当对企业实名登记履行身份信息核验职责；依照规定对登记事项进行监督检查，对可能存在虚假登记、涉诈

异常的企业重点监督检查，依法撤销登记的，依照前款的规定及时共享信息；为银行业金融机构、非银行支付机构进行客户尽职调查和依法识别受益所有人提供便利。

第十八条 银行业金融机构、非银行支付机构应当对银行账户、支付账户等支付工具及支付服务加强监测，建立完善涉电信网络诈骗特征的异常账户监测模型；中国人民银行统筹建立跨银行业金融机构、非银行支付机构的反洗钱统一监测系统，会同国务院公安部门完善与电信网络诈骗犯罪资金流转特点相适应的反洗钱可疑交易报告制度。

对监测识别的异常账户、可疑交易，银行业金融机构、非银行支付机构应当根据风险情况，采取核实交易情况、延迟支付结算、重新核验身份、限制或者终止有关业务等必要的防范措施。

银行业金融机构、非银行支付机构依照第一款规定开展异常账户和可疑交易监测时，可以依法收集异常客户互联网协议地址、网卡地址、支付受理终端信息等必要的交易信息、设备位置信息。上述信息未经客户授权，不得用于风险防控以外的其他用途。

第十九条 银行业金融机构、非银行支付机构应当按照国家有关规定，完整、准确传输直接提供商品或者服务的商户名称、收付款客户名称及账号等交易信息，保证交易信息的真实、完整和支付全流程中的一致性。

第二十条 国务院公安部门会同有关部门建立完善电信网络诈骗涉案资金即时查询、紧急止付、快速冻结、及时解冻和资金

返还制度，明确有关条件、程序和救济措施。紧急止付、快速冻结、资金返还由公安机关决定，银行业金融机构、非银行支付机构应当予以配合。

第四章　互联网治理

第二十一条　电信业务经营者、互联网服务提供者在与用户签订协议或者确认提供服务时，应当依法要求用户提供真实身份信息，用户不提供真实身份信息的，不得提供下列服务：

（一）提供互联网接入服务；

（二）提供虚拟专用网络、网络代理等网络地址转换服务；

（三）提供互联网域名注册、服务器托管、空间租用、云服务、内容分发服务；

（四）提供信息、应用和软件发布服务，或者提供即时通讯、网络交易、网络游戏、网络直播发布、广告推广服务。

第二十二条　互联网服务提供者对监测识别的涉诈异常账号应当采取重新核验、限制功能、暂停服务等处置措施。

互联网服务提供者应当根据公安机关、电信主管部门要求，对涉案电话卡、涉诈异常电话卡所关联注册的有关互联网账号进行核验，根据风险情况，采取限期改正、限制功能、暂停使用、关闭账号、禁止重新注册等处置措施。

第二十三条　设立移动互联网应用程序应当按照国家有关规定向电信主管部门办理许可或者备案手续。

为应用程序提供封装、分发服务的，应当登记并核验应用程序开发运营者的真实身份信息，核验应用程序的功能、用途。

电信、网信、公安等部门和电信业务经营者、互联网服务提供者应当加强对分发平台以外途径下载传播的涉诈应用程序重点监测、及时处置。

第二十四条 提供域名解析、域名跳转、网址链接转换服务的，应当按照国家有关规定，核验域名注册、解析信息和互联网协议地址的真实性、准确性，限制域名跳转次数，记录并留存所提供相应服务的日志信息，支持实现对跳转、解析、转换记录的溯源。

第二十五条 任何单位和个人不得为他人实施电信网络诈骗提供下列支持或者帮助：

（一）出售、提供个人信息；

（二）提供互联网接入、服务器托管、网络存储、通讯传输、线路出租、域名解析等网络资源服务；

（三）提供信息发布或者搜索、广告推广、引流推广等网络推广服务；

（四）提供应用程序、网站等网络技术、产品的制作、维护服务；

（五）提供支付结算服务，或者帮助他人通过虚拟货币交易等方式洗钱；

（六）其他为电信网络诈骗提供各类支持或者帮助的行为。

互联网服务提供者应当建立监测防范制度，对前款规定的涉诈支持、帮助活动进行监测、拦截和处置。

第二十六条 公安机关办理电信网络诈骗案件依法调取证据的，互联网服务提供者应当及时提供技术支持和协助。

互联网服务提供者在依照本法规定对互联网账号异常使用监测、涉诈支持、帮助活动监测和其他涉诈信息、活动监测中发现的可疑犯罪线索、风险信息等，应当依照规定，根据涉诈风险程度情况移送公安、网信、电信等部门。

第五章 综合治理措施

第二十七条 个人信息处理者应当依照《中华人民共和国个人信息保护法》等法律规定，规范个人信息处理，加强个人信息保护，建立个人信息被用于电信网络诈骗的防范机制。

履行个人信息保护职责的部门、单位对可能被电信网络诈骗利用的物流信息、交易信息、贷款信息、医疗信息、婚介信息等实施重点监管和保护。公安机关办理利用个人信息实施电信网络诈骗案件，应当同时查证个人信息来源，依法追究相关人员和单位责任。

第二十八条 电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者应当对从业人员和用户开展反电信网络诈骗宣传，在有关业务活动中对防范电信网络诈骗作出提示，对非法买卖、出租、出借本人有关产品、服务被用于电信网络诈

骗的法律责任作出警示。

新闻、广播、电视、文化、互联网信息服务等单位，应当有针对性地面向社会开展反电信网络诈骗宣传教育防范。

第二十九条 任何单位和个人不得非法买卖、出租、出借电话卡、物联网卡、银行账户、支付账户、互联网账号等；不得为非法买卖、出租、出借的上述卡、账户、账号等提供实名核验帮助。

对经设区的市级以上公安机关认定的实施前款行为的单位、个人和相关组织者，以及因从事电信网络诈骗活动受到刑事处罚的人员，可以采取限制其有关卡、账户、账号等功能和停止非柜面业务、暂停新业务、限制入网等措施。对上述认定和措施有异议的，可以提出申诉。具体办法由国务院有关主管部门会同国务院公安部门规定。

第三十条 国家支持电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者研究开发有关电信网络诈骗技术反制措施，用于监测识别、动态封堵和处置涉诈信息、活动。

国家网信、电信、金融管理和公安部门等应当统筹负责本行业领域技术反制措施建设，推进涉电信网络诈骗样本信息数据共享，建立有关涉诈信息、活动的监测识别、动态封堵和处置机制。

依据本法第十一条、第十二条、第十八条、第二十二条和前款规定，对异常情形采取限制、暂停服务等处置措施的，有关单位、个人可以向作出决定或者采取措施的有关部门、单位提出申

诉。有关部门、单位应当建立完善申诉渠道，对提出的申诉及时核查，核查通过的，应当即时解除有关措施。

第三十一条 国家推进网络身份认证公共服务建设，支持个人、企业自愿使用，电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者对存在涉诈异常的电话卡、银行账户、支付账户、互联网账号，可以通过国家网络身份认证公共服务对用户身份重新进行核验。

第三十二条 公安机关应当会同网信、电信和金融管理部门，以及电信业务经营者、互联网服务提供者、银行业金融机构、非银行支付机构等组织建立预警劝阻系统，对预警发现的潜在被害人，根据情况及时采取相应劝阻措施。

对电信网络诈骗案件应当加强追赃挽损，及时返还被害人的合法财产。对财产不能追回，因电信网络诈骗遭受重大生活困难的被害人，符合国家有关救助条件的，有关方面依照规定给予救助。

第三十三条 经国务院反电信网络诈骗工作机制决定或者批准，电信、金融、公安等部门对电信网络诈骗活动严重的特定地区，可以采取相应的风险防范措施。

第三十四条 对来自电信网络诈骗活动严重的特定地区人员或者前往电信网络诈骗活动严重的特定地区人员，不具有合法、真实出境事由，出境活动存在重大涉诈嫌疑的，移民管理机构可以决定不准其出境。

因从事电信网络诈骗活动受到刑事处罚的人员，移民管理机

构可以决定自处罚完毕之日起六个月至三年不准其出境。

第一款规定的特定地区由国务院反电信网络诈骗工作机制认定。

第三十五条 国务院公安部门等会同外交部门积极稳妥推进国际执法司法合作，与有关国家和地区建立有效合作机制，共同推进跨境电信网络诈骗犯罪打击治理。

第六章 法律责任

第三十六条 电信业务经营者违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

（一）未建立健全反电信网络诈骗内部控制机制或者未有效落实机制，经有关主管部门提出整改要求，拒不整改的；

（二）未履行电话卡、物联网卡实名制登记职责的；

（三）未履行对电话卡、物联网卡的监测识别、监测预警和相关处置职责的；

（四）未对物联网卡用户进行风险评估，或者未限定物联网卡的开通功能、使用场景和适用设备的；

（五）未采取措施对改号电话、虚假主叫或者具有相应功能

的非法设备进行监测处置的。

第三十七条 银行业金融机构、非银行支付机构违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令停止新增业务、缩减业务类型或者业务范围、暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

（一）未建立健全反电信网络诈骗内部控制机制或者未有效落实机制，经有关主管部门提出整改要求，拒不整改的；

（二）未履行尽职调查义务和有关风险管理措施的；

（三）未履行对异常账户、可疑交易的风险监测和相关处置义务的；

（四）未按照规定完整、准确传输有关交易信息的。

第三十八条 电信业务经营者、互联网服务提供者违反本法规定，有下列情形之一的，由有关主管部门责令改正，情节较轻的，给予警告、通报批评，或者处五万元以上五十万元以下罚款；情节严重的，处五十万元以上五百万元以下罚款，并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照，对其直接负责的主管人员和其他直接责任人员，处一万元以上二十万元以下罚款：

（一）未建立健全反电信网络诈骗内部控制机制或者未有效落实机制，经有关主管部门提出整改要求，拒不整改的；

（二）未履行网络服务实名制职责的；

（三）未按照规定核验域名注册、解析信息和互联网协议地址的真实性、准确性，未限制域名跳转次数，或者未记录并留存所提供相应服务的日志信息的；

（四）未登记核验移动互联网应用程序开发运营者的真实身份信息或者未核验应用程序的功能、用途，为其提供应用程序封装、分发服务的；

（五）未建立互联网账号、应用程序、涉诈支持、帮助活动，或者其他电信网络诈骗信息、活动的监测识别和处置机制的；

（六）拒不依法为查处电信网络诈骗犯罪提供技术支持和协助，或者未按规定移送有关犯罪线索、风险信息的。

第三十九条 违反本法第十四条、第二十五条规定，非法制造、销售、提供或者使用专门或者主要用于电信网络诈骗的设备、软件的，或者从事相关涉诈支持、帮助活动的，没收违法所得，由公安机关或者有关主管部门处违法所得一倍以上十倍以下罚款，没有违法所得的，处五十万元以下罚款；情节严重的，由公安机关并处十五日以下拘留。

第四十条 违反本法第二十九条第一款规定的，没收违法所得，由公安机关处违法所得一倍以上十倍以下罚款，没有违法所得的，处二十万元以下罚款；情节严重的，并处十日以下拘留。

第四十一条 反电信网络诈骗工作有关部门、单位的工作人员滥用职权、玩忽职守、徇私舞弊，或者有违反规定泄露国家秘密、商业秘密和个人隐私行为的，依法追究法律责任。

第四十二条 电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者违反本法规定，造成他人电信网络诈骗损失，构成民事侵权的，依法承担民事责任。

第四十三条 违反本法规定，构成犯罪的，依法追究刑事责任。

任何单位、个人组织、策划、实施电信网络诈骗活动的，或者为电信网络诈骗活动提供帮助的，依法追究刑事责任；尚不构成犯罪的，依法给予治安管理处罚。

第四十四条 有关单位和个人对依照本法作出的行政处罚和行政强制措施决定不服的，可以依法申请行政复议或者提起行政诉讼。

第七章 附 则

第四十五条 反电信网络诈骗工作涉及的有关管理和责任制度，本法没有规定的，适用《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国反洗钱法》等相关法律规定。

第四十六条 本法自 年 月 日起施行。