浙江省实施《中华人民共和国反电信网络诈骗法》办法

浙江省第十四届人民代表大会常务委员会

公告

第 35 号

《浙江省实施〈中华人民共和国反电信网络诈骗法〉办法》已于 2025 年 9 月 26 日经浙江省第十四届人民代表大会常务委员会第十九次会议通过，现予公布，自 2025 年 12 月 1 日起施行。

浙江省人民代表大会常务委员会

2025 年 9 月 26 日

浙江省实施《中华人民共和国反电信网络诈骗法》办法

（2025 年 9 月 26 日浙江省第十四届人民代表大会常务委员会第十九次会议通过）

目录

第一章　总则

第二章　宣传教育

第三章　电信治理

第四章　金融治理

第五章　互联网治理

第六章　综合措施

第七章　法律责任

第八章　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《中华人民共和国反电信网络诈骗法》和其他有关法律、行政法规，结合本省实际，制定本办法。

第二条 本办法适用于本省行政区域内的反电信网络诈骗工作。

第三条 县级以上人民政府应当加强对反电信网络诈骗工作的组织领导，建立健全反电信网络诈骗工作机制，明确反电信网络诈骗目标任务，协调解决反电信网络诈骗工作中的重大问题。反电信网络诈骗工作按照规定纳入平安建设、法治建设等相关考核评价体系。

乡镇人民政府、街道办事处按照规定开展反电信网络诈骗宣传教育，协助有关部门做好劝阻潜在被害人、劝返涉诈嫌疑人员等工作。反电信网络诈骗相关工作纳入基层网格化管理。

第四条 公安机关牵头负责反电信网络诈骗工作，会同有关部门和单位建立健全信息共享、工作联动、会商通报、联合执法、案件督办、信息公开等工作制度，承担相关组织协调、推进落实等日常工作。

金融、电信、网信、市场监督管理等部门按照职责履行监督管理主体责任，负责本行业领域反电信网络诈骗工作。

人民法院、人民检察院发挥审判、检察职能作用，依法防范、惩治电信网络诈骗活动。

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。

第五条 有关部门和单位应当加强反电信网络诈骗工作协作，实现跨部门、跨行业、跨区域协同配合、快速联动。

省公安机关应当推动反电信网络诈骗工作省际合作，加强案件办理、技术反制、涉诈资金冻结和处置等方面的信息共享与工作协同。

第六条 单位和个人应当加强个人信息保护，增强电信网络诈骗防范意识和能力，协助、配合有关部门和单位依法开展反电信网络诈骗工作。

履行反电信网络诈骗工作职责、义务的部门和单位，应当根据相关单位和个人的涉诈风险程度，确定精准、合适的预防方式和处置措施，避免影响其正常生产经营活动和生活便利。

第七条 “96110”为反电信网络诈骗专用号码，用于电信网络诈骗行为的举报和反电信网络诈骗的宣传防范、预警劝阻以及处置措施的申诉处理等工作。

公安机关应当会同有关部门建立和完善“96110”运行机制，加强工作人员业务培训和管理，规范工作流程，提高举报、申诉等事项的处理能力。

第二章　宣传教育

第八条 各级人民政府和有关部门应当建立健全覆盖全社会的反电信网络诈骗宣传教育体系，加强反电信网络诈骗宣传教育，普及防骗、识骗知识，提高公众电信网络诈骗防范意识和反电信网络诈骗的参与度。

公安、金融、电信、网信、教育、民政、交通运输、卫生健康、市场监督管理等部门和村（居）民委员会，应当创新宣传教育载体和形式，结合重点行业、区域、群体特点和案件态势，开展反电信网络诈骗宣传教育进学校、进企业、进医院、进社区、进农村、进家庭等活动，增强宣传教育的针对性、精准性。

第九条 工会、共产主义青年团、妇女联合会、残疾人联合会等组织应当结合各自工作对象的特点，开展反电信网络诈骗宣传教育工作。

鼓励志愿服务组织、志愿者依法有序参加反电信网络诈骗宣传教育等工作。

第十条 公安机关应当及时发布新发电信网络诈骗典型案例以及相关警示信息，增强宣传教育的时效性。

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及时向服务对象推送有关部门发布的本领域电信网络诈骗典型案例以及相关警示信息等资讯。

第十一条 公安、金融、电信、网信以及人民法院、人民检察院等部门和单位应当结合下列类型的电信网络诈骗典型案件，制作反电信网络诈骗宣传教育资料，增强宣传教育的警示效果:

（一）以高额投资回报或者宣称掌握内幕消息等形式，诱导被害人转账或者寄递黄金、现金的投资理财类诈骗;

（二）以购物刷单给予返利为诱饵，诱导被害人高额充值、转账的刷单返利类诈骗；

（三）以低价打折、低价海外代购等虚假优惠，诱导被害人缴纳税费、保证金等的虚假购物类诈骗；

（四）冒充银行业金融机构、网贷平台客服，以办理大额贷款为由诱导缴纳手续费、保证金等的虚假贷款类诈骗；

（五）冒充公检法干警，以被害人涉嫌洗钱等违法行为为由，恐吓并诱导被害人将资金转入“安全账户”的虚假涉案类诈骗；

（六）在婚恋、交友网站打造虚假身份形象，建立网络“恋爱”关系，编造理由诱导转账的网络婚恋、交友类诈骗；

（七）通过剪辑视频、模拟声音等方式，以家人、亲友、同事等身份诱骗被害人转账的仿冒熟人类诈骗；

（八）诱导被害人下载虚假贷款、转账应用程序或者登录虚假网站，骗取其银行账户及交易密码、验证码，再转移被害人账户内资金的窃密类诈骗；

（九）其他典型案件类型。

鼓励单位、个人创作反电信网络诈骗宣传教育作品，丰富作品形态。公安、金融、电信、网信等部门应当加强指导，推广典型宣传教育作品。

第十二条 各级各类学校、教育培训机构应当开展电信网络诈骗防范宣传教育，将反电信网络诈骗知识纳入安全、法治教育内容，定期开展针对性宣传教育活动。

国家机关、企业事业单位、其他组织应当加强对其工作人员的反电信网络诈骗宣传教育。

第十三条 广播、电视、报刊、网络等媒体以及公共场所管理者应当加大反电信网络诈骗公益宣传教育力度。

第三章 电信治理

第十四条 电信业务经营者应当依法全面落实用户真实身份信息登记认证制度和网络信息安全制度，依法履行公民个人信息保护责任。

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用户实名制的管理责任，强化代理商资质审核，禁止代理商再次委托代理。代理商应当使用基础电信企业和移动通信转售企业提供的电话实名制系统为用户办理入网手续，不得留存用户实名登记信息。

基础电信企业应当健全语音专线、中继线路类电信线路和短信端口管理制度，通过技术监测、协议约定等方式，严格执行接入审核标准，实施动态监测，优化处置流程，规范使用行为；发现异常使用情形的，应当重新核验使用者身份和使用场景，并根据核验结果采取相应处置措施。

第十五条 电信业务经营者对申请办理电话卡开卡业务的用户，应当核查其相关情况；经核查确认申请用户有下列异常办卡情形之一的，有权按照规定拒绝办理开卡业务:

（一）持有的电话卡总数已超出国家规定的限制数量;

（二）其名下存在涉诈异常电话卡且未通过重新核验;

（三）国家规定的其他情形。

第十六条 电信业务经营者办理新用户电话卡入网业务时，应当对开通境外短消息、电话接收接听服务进行反电信网络诈骗风险提示；对已开通但未实际发生业务的，应当引导其关闭相关服务。

电信业务经营者应当重点甄别境外电信网络诈骗活动严重地区主叫号码，对网内和网间虚假主叫、不规范主叫进行识别、拦截；对公安机关通报的涉诈号码实施拦截。

第十七条 电信业务经营者对监测识别的涉诈异常电话卡应当按照国家规定重新进行实名核验，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，可以限制、暂停有关电话卡功能。

第十八条 医院、宾馆、酒店、网吧等场所的管理者，应当加强对经营场所通信设施的安全管理，对非法安装、使用外联设备进行排查；发现非法安装、使用外联设备可疑情形的，应当及时报告公安机关。

电信业务经营者应当完善通信设施日常巡视检查制度，对非法安装、使用外联设备进行定期排查；发现非法安装、使用外联设备的，应当立即处置，并报告公安机关和电信主管部门。

第四章　金融治理

第十九条 银行业金融机构、非银行支付机构对申请办理银行账户、支付账户开户业务的客户，应当核查其相关情况；经核查确认申请客户有下列异常开户情形之一的，有权按照规定拒绝办理开户业务：

（一）存在异常的组织开户行为；

（二）开户业务与其实际需求明显不相符；

（三）有明显理由怀疑其办理开户业务有从事电信网络诈骗违法犯罪活动嫌疑；

（四）其名下的其他账户已被采取涉诈风险管理措施；

（五）国家规定的其他情形。

客户不配合进行身份识别的，银行业金融机构、非银行支付机构有权按照规定拒绝办理开户业务。

第二十条 银行业金融机构、非银行支付机构为客户开立银行账户、支付账户时，应当按照国家规定开展客户尽职调查，依法识别受益所有人，根据客户尽职调查情况确定风险等级，实施账户分类分级管理，合理设置账户功能、支付渠道和支付限额。

第二十一条 银行业金融机构、非银行支付机构为客户提供结算服务时以及与客户业务关系存续期间，有权根据客户银行账户、支付账户历史交易和风险状况变化等情况，按照规定动态调整客户风险等级，相应采取降低非柜面支付限额、暂停非柜面业务等风险管理措施。

第二十二条 银行业金融机构、非银行支付机构应当按照国家规定，建立健全转账风险提示制度，在客户转账环节设置诈骗防范提醒。

第二十三条 银行业金融机构、非银行支付机构应当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系统，加强异常账户和可疑交易监测。

对监测识别的异常账户和可疑交易，银行业金融机构、非银行支付机构应当重新核验客户身份、核实交易情况；经核查无法排除异常或者可疑情形的，应当根据风险情况，采取延迟支付结算、限制或者中止有关业务等必要的防范措施。

对监测识别的转账收款方为涉诈账户等紧急情况，银行业金融机构、非银行支付机构有权直接采取延迟支付结算、限制或者中止有关业务等必要的防范措施。

银行业金融机构、非银行支付机构应当将异常账户和可疑交易情况报告公安机关。公安机关应当立即研判，并将研判情况向银行业金融机构、非银行支付机构反馈，由其按照规定采取相应的风险处置措施。

第二十四条 公安机关对电信网络诈骗涉案资金适用冻结措施，应当遵守有关资金冻结的法律、行政法规和国家规定，不得超权限、超范围、超数额、超时限冻结资金。对不符合整体冻结情形的账户，应当在查明后及时变更为限额冻结。对账户内没有涉案资金流入，或者流入账户的涉案资金系提供商品、服务并完成交易后合法收取的市场合理对价的，应当在查明后及时解除冻结。

公安机关依法采取紧急止付或者冻结措施后，应当在国家规定的期限内完成核查工作，甄别资金性质，核实涉案数额，准确适用冻结措施。

第五章　互联网治理

第二十五条 公安、电信、网信等部门应当督促互联网服务提供者依法履行涉诈信息监测和处置等义务，指导电信业务经营者和互联网服务提供者开展电话卡与互联网账号关联安全风险防范工作。

互联网服务提供者应当依法全面落实用户真实身份信息登记认证制度和网络信息安全制度，并按照公安、电信、网信等部门要求，对涉案和涉诈异常互联网账号所关联注册的互联网账号重新进行核验，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。

第二十六条 电信业务经营者、互联网服务提供者应当履行互联网涉诈风险提示义务，引导用户通过备案网站、官方应用商店等可信渠道获取网络访问和应用程序下载服务。

第二十七条 电信业务经营者、互联网服务提供者应当加强对涉诈互联网账号、网站访问链接、应用程序以及其他涉诈信息的动态监测；对涉诈的互联网账号、网站访问链接和应用程序，依法采取清理涉诈信息、关闭账号、封堵下载链接、关闭网站或者应用程序、下架应用程序等处置措施，并将相关情况及时报告公安、电信、网信等部门。

第二十八条 对未按国家规定办理许可或者备案手续，经甄别存在涉诈异常情形的网站访问链接和应用程序，公安、电信、网信等部门应当通知电信业务经营者、互联网服务提供者采取封堵下载链接、关闭网站或者应用程序、下架应用程序等处置措施。

第六章　综合措施

第二十九条 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》《中华人民共和国反电信网络诈骗法》等法律、法规规定，根据合法、正当、必要和诚信的原则处理个人信息，采取必要措施保障所处理个人信息的安全，防范个人信息被非法公开、提供或者买卖。

公安机关办理电信网络诈骗案件，应当同时查证犯罪所利用的个人信息来源，依法追究相关人员和单位责任。

第三十条 快递经营企业应当按照规定登记寄件人身份和物品信息，对寄递物品进行验视；发现寄递批量电话卡、物联网卡、银行卡或者寄递黄金等高价值物品、现金的，应当按照规定及时向公安机关报告。

互联网货运、出租汽车等行业的从业人员在服务过程中发现运送黄金等高价值物品、现金的，应当按照规定及时向公安机关报告。

第三十一条 省公安、金融、电信等部门应当加强人工智能等新技术的应用，统筹完善本行业领域的大数据监测识别反制技术措施，加强涉诈用户信息交叉核验，建立有关涉诈异常信息、活动的监测识别、动态封堵和处置机制。

省公安机关负责统筹建立反电信网络诈骗电子数据共享平台，推进金融、电信、互联网、商业、医疗、教育、快递物流、交通运输、公共服务等行业领域涉诈样本信息数据共享，加强对其他行业领域大数据监测识别反制技术措施的统筹指导，协调推进监测识别标准的科学性和一致性。

第三十二条 省公安机关应当将涉案电话卡、物联网卡、银行账户、支付账户、互联网账号、网站访问链接和应用程序及时通报电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者；有关单位应当按照公安机关要求，即时采取限制、暂停服务等处置措施。

公安机关应当会同金融、电信、网信等部门，组织电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者等建立健全预警劝阻系统，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。

第三十三条 对具有涉诈异常情形的电话卡、物联网卡、银行账户、支付账户、互联网账号、网站访问链接和应用程序等采取处置措施后，除依法需要保密外，应当按照谁决定谁负责的原则，由作出决定的部门和单位即时向被处置对象告知处置原因、救济渠道以及需要提交的资料等事项。作出决定的部门和单位应当建立完善申诉渠道，及时受理申诉并核查；核查通过的，应当即时解除有关措施。

被处置对象可以通过“96110”向公安机关提出申诉，并说明事实和理由。公安机关应当对被处置对象申诉的事实和理由立即进行核查；核查通过的，应当即时解除或者通知相关单位即时解除处置措施，消除影响。

第三十四条 公安机关办理电信网络诈骗违法犯罪案件，应当通过统一的信息化系统开展电子化调查取证。具体办法由省公安机关会同省有关部门制定。

电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者等数据持有者在接到公安机关协查通知后，应当通过统一的信息化系统及时提供符合要求的电子数据。

第三十五条 公安机关应当加强对电信网络诈骗违法犯罪案件的追赃挽损，会同有关部门依照法律、行政法规和国家规定完善涉案资金处置制度，及时返还被害人的合法财产。

银行业金融机构、非银行支付机构应当依法协助公安机关查清被害人资金流向，将所涉资金返还至公安机关指定的被害人账户。

第三十六条 公安机关应当会同有关部门建立健全电信网络诈骗违法犯罪案件线索举报奖励制度。有关部门和单位发现电信网络诈骗违法犯罪案件线索的，应当及时移送公安机关。

电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者应当分别设立举报和反馈渠道，对被举报的涉诈电话卡、物联网卡、银行账户、支付账户、互联网账号、网站访问链接和应用程序等及时进行核查，并依法予以处理。

第三十七条 县级以上人民政府应当做好反电信网络诈骗工作的基础设施建设和人员、装备保障，并将“96110”运营、宣传教育、人员劝返等反电信网络诈骗工作所需的必要经费纳入本级财政预算。

县级以上人民政府应当加强反电信网络诈骗专业人才和志愿者队伍建设，建立特殊人才引进制度。

第三十八条 对电信网络诈骗违法犯罪案件，人民检察院作出不起诉决定或者人民法院作出免予刑事处罚判决，但需要给予行政处罚的，应当按照规定程序移送公安机关或者相关行政执法机关，由其依法及时作出行政处罚决定并反馈处理情况。

人民检察院、人民法院和公安机关发现有关部门和单位在个人信息保护和电信网络诈骗风险防范方面存在突出问题或者重大风险隐患的，应当依法提出检察建议、司法建议、公安提示，有关部门和单位应当及时研究处理并反馈处理情况。

人民检察院在履行反电信网络诈骗职责中，对于侵害国家利益和社会公共利益的行为，可以依法向人民法院提起公益诉讼。

第三十九条 县级以上人民政府应当完善通报和约谈工作机制，定期通报反电信网络诈骗监测处置、案件态势等情况，对反电信网络诈骗工作履职不力的有关部门和单位进行约谈。

电信业务经营者、银行业金融机构、非银行支付机构、互联网服务提供者以及其他履行反电信网络诈骗工作职责、义务的单位及其工作人员，因依法履行职责、义务被投诉，或者发生电信网络诈骗案件但有证据证明其已经尽职尽责的，不予追究责任。

第七章　法律责任

第四十条 违反本办法规定的行为，法律、行政法规已有法律责任规定的，从其规定。

第四十一条 违反本办法第十八条第一款规定，医院、宾馆、酒店、网吧等场所的管理者未对非法安装、使用外联设备进行排查，或者发现非法安装、使用外联设备可疑情形未及时报告，造成电话线路被盗用实施诈骗的，给予警告；情节严重的，由公安机关处一万元以上五万元以下罚款。

违反本办法第十八条第二款规定，电信业务经营者未按规定对非法安装、使用外联设备进行定期排查，或者对发现的非法安装、使用的外联设备未立即采取处置措施的，由电信主管部门责令改正，给予警告；拒不改正的，处五万元以上二十万元以下罚款。

第四十二条 违反本办法第二十五条第二款规定，互联网服务提供者未按规定对涉案和涉诈异常互联网账号所关联注册的互联网账号重新进行核验，或者未按规定采取相应处置措施的，由公安、电信、网信等部门按照职责责令改正，给予警告；拒不改正的，处五万元以上二十万元以下罚款；情节严重的，处二十万元以上五十万元以下罚款。

第八章　附则

第四十三条 本办法自 2025 年 12 月 1 日起施行。

来源：中国.浙江人大