CAICT 中国信通院

疫情防控期间电信网络诈骗防范治理优秀案例汇编

安全研究所

2020 年 4 月

版权声明

前　言

新型冠状肺炎疫情发生以来，信息通信行业深入贯彻习近平总书记在统筹推进新冠肺炎疫情防控和经济社会发展工作部署会议上的重要讲话精神，将涉疫情诈骗治理作为服务疫情防控大局的一条工作主线，全力做好电信网络诈骗防范治理工作。针对疫情期间诈骗治理新形势，工业和信息化部出台指导性文件，组织建立专项工作机制，从技术防范、创新管理、联防联控、宣传引导等方面进行工作部署。

为落实有关要求，进一步加强疫情期间电信网络诈骗防范治理，及时梳理总结行业优秀案例与有益做法，在工业和信息化部网络安全管理局指导下，中国信息通信研究院电信网络诈骗治理中心发起疫情期间电信网络诈骗防范治理优秀案例征集活动，经案例征集和专家评审等环节，最终遴选出51个针对性强、创新性好、治理成效显著的优秀案例。这些优秀案例在行业内具有较强的代表性、创新性和示范性，做好进一步的推广应用，对有效提升全行业电信网络诈骗防范治理能力具有积极意义。

目 录

一、案例征集基本情况及分析

（一）案例征集及入选情况

本次优秀案例征集评选活动共收到报送案例77个，入选优秀案例51个，入选率为66%，其中报送技术防范类案例35个，入选优秀案例24个；报送创新管理类案例12个，入选优秀案例12个；报送联防联控类案例12个，入选优秀案例7个；报送宣传引导类案例16个，入选优秀案例8个；报送其他类案例2个。

（二）优秀案例总体分析

本次案例报送主体多、内容丰富、实践效果好，入选案例具有一定的典型性和代表性，能够充分反映出疫情防控期间电信网络诈骗治理的优秀做法和有益经验。从报送主体看，优秀案例来自各地通信管理局、基础电信企业、重点互联网企业及安全领域专业技术厂商等行业相关单位。从具体内容看，优秀案例涉及技术管控、创新管理、联防联控和宣传引导等多方面内容，基本涵盖了疫情期间电信网络诈骗治理的主要方向。从实践效果看，优秀案例针对疫情期间行业治理重点难点问题，进行的积极探索和有益尝试，取得了较好的治理成效和社会效益。

（三）优秀案例分类分析

1、以技治网，利用新一代信息技术全面提升疫情期间技术防范

能力。疫情期间，信息通信行业充分利用大数据、人工智能等新一代信息技术，积极开展涉疫情诈骗态势监测、研判分析、预警提示、拦截处置等工作，有效阻断诈骗信息传播途径。**一是**加强诈骗电话、短信监测处置。基础电信企业充分发挥行业数据优势，及时升级更新诈骗电话大数据防范预警系统，根据涉疫情诈骗手法套路完善策略模型，密切监测涉疫情诈骗态势变化，不断强化涉疫情诈骗电话、短信的精确监测识别和实时拦截。**二是**深化涉疫情互联网诈骗治理。腾讯、360 等重点互联网企业运用人工智能对诈骗行为特征建模分析，精准识别涉疫情诈骗，加强对诈骗新手法的处置力度。任子行、无糖等安全企业利用云计算、深度学习等技术实时监测分析通过论坛、贴吧、微博等渠道传播的涉疫情诈骗信息，构建虚假售卖防疫物资非法网站识别打击系统，实现对涉疫情诈骗网站精准预警和溯源打击。**三是**积极探索网络黑灰产整治。基础电信企业及行业安全厂商针对智能群呼设备等网络黑灰产技术设备展开专门研究，研发基于多源数据的GoIP诈骗电话智能分析系统，建立黑灰产违法违规设备快速追溯体系，实现快速溯源、精准响应。

2、创新管理举措，全力保障疫情期间防范治理工作顺利推进。

疫情期间，信息通信行业结合疫情期间电信网络诈骗治理工作新情况，不断优化工作机制，创新工作举措，确保防范治理工作有序有效推进。**一是**完善号码线上复通机制。山东、浙江等地基础电信企业完善线上处理流程，针对误停机用户通过电话、短信、微信公众号等方式设立快速解封绿色通道，实行“不见面”办理，有效解决疫情期间

“实人”认证难题。**二是**强化号卡办理重点环节管控。北京、天津等地基础电信企业针对线上号卡办理加大管控力度，进一步完善异常批量购卡联动劝阻机制，多措并举拦截高危不良订单。**三是**优化治理工作流程。湖北移动及时调整优化疫情期间疑似涉诈号码的分析处置流程，将被动处置改为主动处置，极大减少误报误处置情况。有效提升用户满意度。海南、宁夏针对疫情期间诈骗新形式，优化反诈监测、摸排、核查、甄别、处置、追责工作流程，进一步完善对涉诈号码的闭环管控。

3、开展联防联控，积极构建疫情期间协同治理工作格局。疫情期间，信息通信行业加强行业内外联动，强化信息共享，积极输出涉诈线索，着力构建密切、协同、互通的共治格局。**一是**深化行业内协同联动机制。河南基础电信企业加强省内协同，针对异常漫入高危地区电话号码开展联合监测，及时发现涉诈团伙线索，有效阻断诈骗风险。**二是**加强与公安机关密切协作。上海、天津、重庆、山东、陕西、海南等多地基础电信企业在疫情期间加强与属地公安机关反诈中心合作，开展涉疫情诈骗信息联合研判、联合处置，利用自身系统、技术优势加强涉诈信息线索输出，协助公安机关破获多起涉疫情诈骗案件。

4、加强宣传引导，着力提升用户涉疫情诈骗风险防范意识。疫情期间，信息通信行业加强宣传渠道方式创新，提升宣传品质效果，不断扩大反诈宣传教育的覆盖面与影响力。**一是**充分发挥短信传播覆盖优势。基础电信企业结合自身优势，创新工作思路，精准分类不同

人群，梳理多种诈骗场景，发送针对性涉疫情诈骗防范公益短信，最大化宣传引导以降低用户上当受骗风险，疫情期间累计发送各类诈骗防范公益短信上亿条。**二是**创新拓展宣传新媒体渠道。电信和互联网企业积极跟踪涉疫情诈骗最新手法，制作宣传提醒内容，通过微信、微博、短视频、网络直播等宣传方式，组成行业反诈新媒体矩阵，展开全方位、立体式协同反诈宣传，及时向群众预警疫情期间高发诈骗类型。**三是**积极开展实时劝阻。阿里巴巴等重点互联网企业开发应用智能语音交互等前沿技术，针对虚假销售口罩、防控疫情虚假捐助等涉疫情诈骗，以发送强制提醒短信、闪信或一对一电话等方式向疑似被骗用户实时预警，全力防止用户资金损失。

（四）未来工作展望

在工业和信息化部的统一调度指挥和全行业的共同努力下，疫情期间信息通信行业电信网络诈骗防范治理工作已经取得了阶段性明显成效，涉疫情诈骗已经连续多周呈现明显下降趋势。但与此同时我们也清醒的看到：诈骗分子紧跟当前社会热点频繁更新变化诈骗手法套路，从单一平台诈骗转向多网络平台连环诈骗，迷惑性、隐蔽性明显加强，极大增加了防范治理工作的难度和复杂性。

面对当前电信网络诈骗的治理难点，信息通信行业应该在充分总结本次涉疫情诈骗治理成功经验的基础上，在技术防范、创新管理、联防联控、宣传引导等方面深入推进治理工作，进一步深化拓展治理成效。

一是在技术防范方面，充分利用新一代信息技术，在现有技术防范预警能力基础上，加强反诈基础设施建设和产品服务开发，全面提升电信网、互联网一体化管控能力。

二是在创新管理方面，在涉疫情诈骗治理专项工作机制基础上，引导行业责任主体针对互联网诈骗治理、电话卡及物联网卡管理等重点问题，创新工作机制举措，加强重点环节管控，进一步优化完善信息报送、态势研判、责任督导、成效评价等制度机制。

三是在联防联控方面，在强化行业内部协同的基础上，不断深化与公安机关、网信办、人民银行等部门的联动，建立完善诈骗风险预警、涉诈信息研判处置、电子取证回溯等联合工作机制，形成诈骗线索发现、事件预警处置的问题共治、风险联防能力。

四是在宣传引导方面，积极跟踪最新诈骗手法套路，及时制作宣传预警内容，针对重点人群进行针对性宣传提醒；积极开展多渠道新媒体宣传，扩展反诈宣传覆盖面，全力放大宣传成效。

二、案例报送情况梳理

疫情期间信息通信行业电信网络诈骗治理优秀案例入选情况列表

类别	序号	案例名称	报送单位
一、技术防范类	1	抗疫在前线 反诈在身边 山东管局通信网诈骗防范系统全面打击新型电信诈骗	山东管局
	2	精准施策，防范涉疫诈骗电话	山东省通信网络保障中心
	3	强化技术管控，从源头阻断疫情期间电信诈骗行径	广西移动
	4	基于电子围栏技术的态势分析及精准打击	广东联通
	5	中国电信疫情诈骗电话分析、识别和预测集成学习 AI 系统	中国电信
	6	基于 NLP 技术的涉疫诈骗电话检测及自动劝阻系统	珠海高凌
	7	抗击疫情，反诈不停，筑建抗疫反诈新防线	重庆移动 国瑞数码
	8	关于疫情期间涉及短信渠道的新型诈骗形式挖掘	山东省通信网络保障中心
	9	智能、高效、精准的疫情短信防诈骗技术创新项目	广东电信
	10	行业短信可信分发，助力 5G 新消息业务健康发展	山西移动
	11	科技战疫，腾讯在行动。	腾讯
	12	百度多举措打击虚假有害信息，为“战疫”护航	百度
	13	基于移动互联网大数据分析，助力疫情期间防范和打击网络诈骗	云南电信
	14	新冠疫情期间涉互联网诈骗监测分析	任子行
	15	虚假售卖防疫物资非法网站识别打击系统	成都无糖
	16	基于微博大数据识别的多维度反欺诈技术机制	新浪微博

	17	“大数据+人工智能”助力疫情期间电信网络诈骗治理	中国移动信安中心
	18	360 手机卫士—应龙综合反诈平台	360 公司
	19	基于大数据综合分析及呼叫行为关联等技术防范涉疫诈骗等违法行为实践	上海电信
	20	北京移动启动“智慧中台”对疫情诈骗联防联控	北京移动
	21	加强 IM 虚假信息监控，预防电信诈骗骚扰	贝壳找房
	22	重拳出击黑灰产，助力抗疫护安宁	广东移动
	23	“多卡宝”设备电信网络诈骗防治	云南移动 中国移动信安中心
	24	基于多源数据的 GoIP 诈骗电话分析系统	微智信业
二、创新管理	25	创新电信网络诈骗处置手段 协同联动提升案件处置效率	山西管局
	26	远程认证核实身份，无须到厅处理复通	广东电信
	27	优化完善疫情期间用户申诉处理复通机制	山东移动
	28	疫情期间实体渠道针对异常批量购卡联动劝阻机制	天津电信
	29	深化疫情期间警企合作模式，强力遏制号卡涉疫诈骗新形势	宁夏电信
	30	强化线上商城订单筛查治理	北京联通
	31	创新处置方式，提升用户满意度	湖北移动
	32	手机端防诈骗全流程一键关停	海南电信
	33	抓源头、强管控，上下联动防诈骗	青海电信
	34	互联网自助式“e”认证，破解疫情期间“实人”认证难题	浙江移动
	35	来电名片保障效率，连接信任守护安康	广东电信
	36	“实名实人”用户复机投诉线上认证流程优化	陕西移动 中国移动信安中心

三、联防联控	37	携手公安、友商联合打击电信网络诈骗团伙	河南电信
	38	强化政企联动机制、积极开展事中劝阻	山东移动
	39	利用大数据分析支撑公安精准打击本地活动 GOIP 设备	陕西移动 中国移动信安中心
	40	警企联动部署实施短信收端拦截疫情涉诈短信策略	上海电信
	41	利用信令数据构建诈骗用户识别预警模型,配合公安机关坚决打击违法犯罪行为	海南联通
	42	创新联防联控机制，精准打击境外电信网络诈骗	天津移动 中国移动信安中心
	43	精准抗“疫” 腾讯赋能疫情防控加速度！	腾讯
四、宣传引导	44	疫情期间建立差异化的反诈宣传机制	山东移动
	45	全民创意宣传反诈，护航抗疫稳定民心	广东移动
	46	钱盾反诈机器人抗疫期间反欺诈创新实践	阿里巴巴
	47	支付宝反欺诈防骗宣传引导创新实践	阿里巴巴
	48	“全民反诈首都无诈”北京电信疫情期间警企联防联控系列宣传活动	北京电信
	49	五个第一，打响疫情反诈骗宣传战	福建联通
	50	新媒体助力宣教工作显特色，多措并举开展防范电信诈骗宣传	广东联通
	51	抖音多渠道全方位做好疫情期间防范治理电信诈骗宣传	字节跳动

三、优秀案例汇编

（一）技术防范类

结合案例涉及领域、解决问题等实际情况，技术防范类又可进一步细分为诈骗电话处置、诈骗短信处置、涉疫情互联网诈骗治理、综合类、灰黑产整治等 5 类。

A.诈骗电话处置类

1、抗疫在前线，反诈在身边，山东管局通信网诈骗防范系统全面打击新型电信诈骗

实施单位：山东省通信管理局

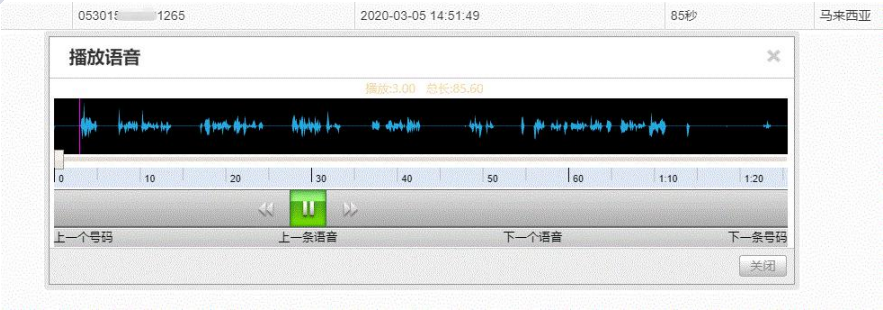
新冠疫情的爆发，衍生出了大量与疫情相关的电信诈骗。国瑞数码支撑山东省通信管理局建设的通信网诈骗防范系统保证正常运行，同时进行技术防范手段方式创新。一是及时优化通信网诈骗防范系统的诈骗分析监测策略，增加“口罩”、“N95”、“疾控中心”、“新冠疫情小组”、“机票代购”、“酒精”、“感染”等监测策略 140 余个。二是利用大数据分析技术，增加涉诈态势信息检测分析功能，及时获取电信诈骗新闻事件，预判新型诈骗风险趋势，为提升诈骗防控能力提供大数据支撑。同时将诈骗态势整合成反诈骗宣传信息通过运营商及互联网企业下发。通过以上技术创新，通信网诈骗防范系统

自 1 月 21 日至 4 月 9 日期间，累计监测新型诈骗事件 17687 起，处置诈骗号码等 3855 个，累计向运营商和企业下发新型诈骗态势信息数百次。

2、精准施策，防范涉疫诈骗电话

实施单位：山东省通信网络保障中心

自疫情以来，山东省通信网络保障中心坚持防疫与发展“两手抓”“两手硬”，做好防范治理涉疫诈骗和平台建设相关工作。一日一通自称为腾讯微信客服中心的境外来电引起保障中心人员警觉。该通电话称被叫有一个微信号出售口罩，收到货款后没有发货而被人举报，要求进行身份验证，核查信息。保障中心分析其目的是利用疫情特点进行信息套取及诈骗，于是立即采取针对措施。一是制定疫情防诈策略，进行精准施策、系统调优、综合研判并及时预警。二是延伸涉疫情电话诈骗套路，由腾信客服中心联想到仿冒公安机关、疾控中心、通信管理局，由“口罩未发货”联想到“非法买卖防疫物资”“非法入境”，对系统关键词进行优化配置。三是统筹抓好诈骗类型防范工作。对疫情电话诈骗进行监测、预警的同时，兼顾防范冒充客服、冒充快递等诈骗类型。对疑似诈骗电话进行综合研判，及时进行预警工作，避免群众财产损失。



3、强化技术管控，从源头阻断疫情期间电信诈骗行径

实施单位：广西移动

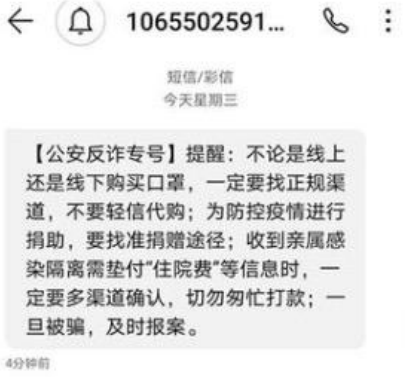
针对诈骗高发地区宾阳、东兴在疫情期间出现的电信诈骗，广西移动采用大数据分析技术进行建模，多次与公安机关沟通并根据疫情和行诈手段的变化完善分析模型，输出疑似高危号码，进行重点监测与处置，及时、有效地阻断诈骗风险。自该模型应用以来，累计对宾阳 20000 余个号码、东兴近 3000 个号码进行处置。同时经拓展核查，累计处置 3 万余个入网可疑号码。广西移动 2 月和 3 月涉案号码量较 1 月分别下降 41.8%和 33.5%，3 月在宾阳和东兴的广西移动涉案号码数量已降至个位数。

4、基于电子围栏技术的态势分析及精准打击

实施单位：广东联通

面对疫情期间诈骗形势的变化，广东联通利用电子围栏技术，实现对诈骗态势的分析以及诈骗窝点、诈骗号码的有效打击。一是加强态势分析，精准锁定诈骗高危地。结合公安警情数据，通过对诈骗样本的大数据分析，圈定全国诈骗高发地，形成电子围栏，并进行动态更新、重点监控，疫情爆发以来，已更新 39 个高危地区。尤其针对广东“茂阳湛”地区，制定四类专项模型，拦截诈骗号码，茂名地区涉案号码同比下降 99.13%。二是以智能探针为抓手，快速识别诈骗号码。以诈骗号码行为为探针，在电子围栏数据中进行系统适配检测，在号码进入电子围栏的第一时间输出研判结果，实现诈骗号码的精准识别和快速处置。在疫情期间通过电子围栏识别处置的诈骗号码共

6395 个，涉案号码较去年年底减少 36%。三是黑灰产业“号-证-端-点”全方面防范打击。在关停号码-证件加黑-拦截终端的基础上，利用电子围栏监测数据，对手机号码和 IMEI 号码进行聚类学习，经过多层深度挖掘，生成异常设备群组（如猫池、GOIP 设备等），最终定位诈骗窝点，同时与本地公安反诈中心保持联动，提供窝点信息，协助公安落地侦查。



5、中国电信疫情诈骗电话分析、识别和预测集成学习 AI 系统

实施单位：中国电信

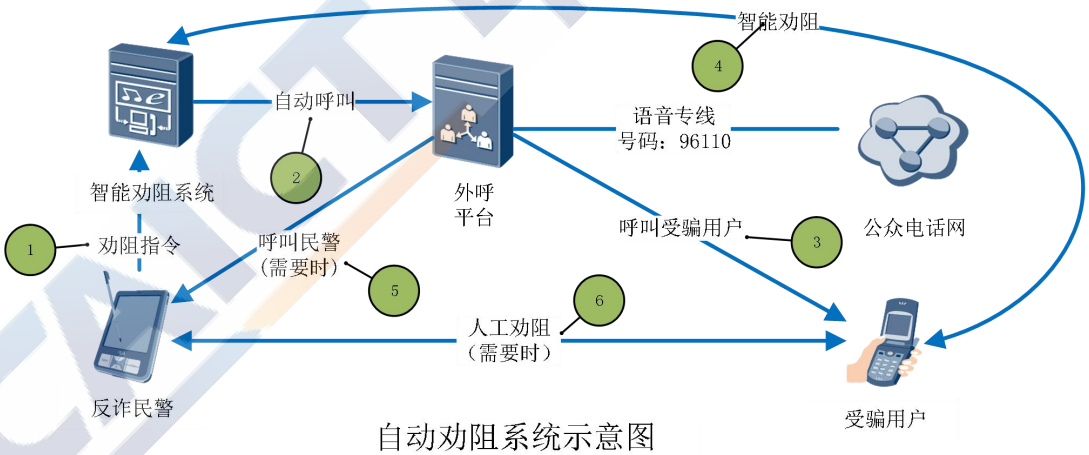
中国电信诈骗电话识别集成学习系统不断升级优化，切实做好涉及疫情电信网络诈骗防范保障工作。首先，学习 AI 系统基于中国电信集团公司数据中心，整合 12321 平台、侦办平台和全集团多维度数据资源，跨省份诈骗和一证多卡用户均能被识别，完整性强。其次，结合海量脱敏数据，学习 AI 系统增加用户的异常话务等行为信息，更加全面地刻画电话诈骗行为特征，准确率高。再次，学习 AI 系统建立欺诈团伙的识别模型，对用户举报投诉、异常信息等数据进行 AI 智能分析比对，筛查其中所包含的黑产、欺诈关联信息，再对模型结果清单进行多模型融合、结合互联网用户标记的标签体系，对模型结果进行核验，误杀率低。此外，学习 AI 系统对疫情期间“涉防疫医疗物资购买”、“航班行程退改签”、“冒充疫情工作人员”等最新涉疫情诈骗场景进行分析，根据数据表现优化模型，准确率高。学习系统 2、3 月份下发疑似清单中涉案号码逾千个，占该时间段中国电信涉案号码数量的 31.76%，在 3 月份欺诈案件数量激增的情况下经研判对下发清单中近半的号码进行了拦截、关停等处置。同时建立的欺诈骚扰黑、白名单数据库，有效减少误杀情况。

6、基于 NLP 技术的涉疫诈骗电话检测及自动劝阻系统

实施单位：珠海高凌信息科技股份有限公司

为提高防疫期间反电诈工作效率，高凌信息从技术防范措施入手，一是针对冒充公检法、虚假网络贷款、虚假退改签等传统类型的

诈骗电话衍生出含“疫情影响”、“口罩”、“防疫物资”的话术特征，采用 NLP 和机器学习技术不断训练和优化语义检测模型，提高涉疫诈骗电话检测效果。二是针对预警量比较大，反诈民警人工拨打劝阻电话效率较低的问题，设计自动化劝阻系统。通过与检测预警系统对接，自动获得潜在受骗用户电话号码，利用 96110 反诈专线自动拨打受骗用户电话，与被叫用户智能交互并记录反馈信息，极大提高劝阻效率，同时为模型优化积累了丰富数据。三是针对民警难以上门劝阻被诈骗分子深度洗脑的潜在受骗用户，提供被叫保护功能，在一定时间内拦截受骗用户的国际或省际长途电话，防止受骗用户进一步受骗，提高防诈效果。自应用涉疫诈骗电话检测及自动劝阻系统以来，某省平均每天检出涉诈电话总量超 7000 例，准确率超过 95%，其中涉疫诈骗电话超过 500 例，自动劝阻 5000 余次。



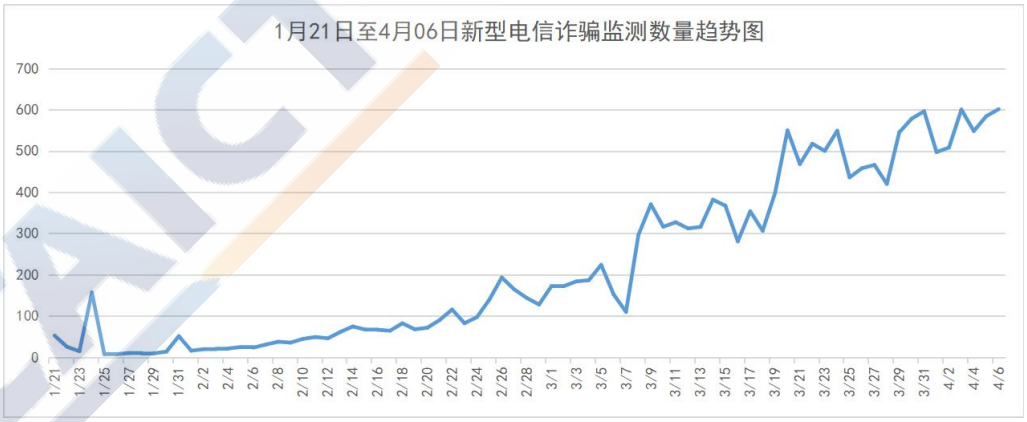
自动劝阻系统示意图

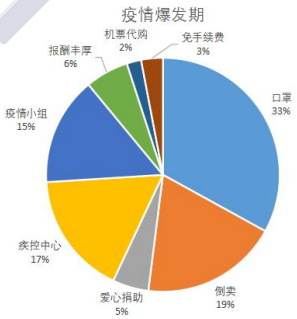
7、抗击疫情 反诈不停 筑建抗疫反诈新防线

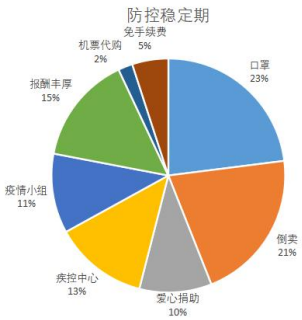
实施单位：重庆移动、天津市国瑞数码安全系统股份有限公司

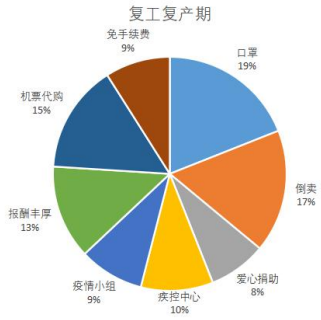
疫情期间，国瑞数码积极联动运营商、公安机关等多方力量，升级优化反诈预警联动系统，着力打击利用疫情实施的诈骗犯罪。一是

升级诈骗防范系统的诈骗分析监测策略，新增“口罩”、“N95”、“疾控中心”等30余个监测策略，并根据公安推送的诈骗线索，新增“特效药”、“病毒检测”等监测策略20余个。二是针对与以上信息相关联的诈骗热点事件，新增涉诈舆情信息的监测分析，为提前发现新型诈骗套路，预知诈骗风险提供数据支撑。三是升级公安反诈联动机制，加强对监测到疑似诈骗信息的人工研判及推送力度，每天向公安机关推送的诈骗预警信息数量为平时的1.5倍以上。四是支撑重庆移动有针对性地，向用户发送反诈宣传和反诈提醒信息，加强疫情期间的反诈骗宣传工作。五是支撑重庆移动调整诈骗监测和处置的模型，设置“抗疫白名单”，保障疫情期间抗疫工作相关号码的通信畅通。截止至4月6日，累计监测新型诈骗事件1.6万余起，协助破获新型诈骗案件160余起，添加白名单号码2.3万余个，重庆移动自1月22日起累计发送公益信息74批，共13.85亿条。









B.诈骗短信处置类

1、关于疫情期间涉及短信渠道的新型诈骗形式挖掘

实施单位：山东省通信网络保障中心

随着疫情防控形势的日益严峻，短信组作为山东省反诈防范平台的重要组成部分，在保障日常短信研判的工作的同时，积极从多种渠道获取新型诈骗渠道，多渠道设防，多方位研判，加大短信预防投入力度。

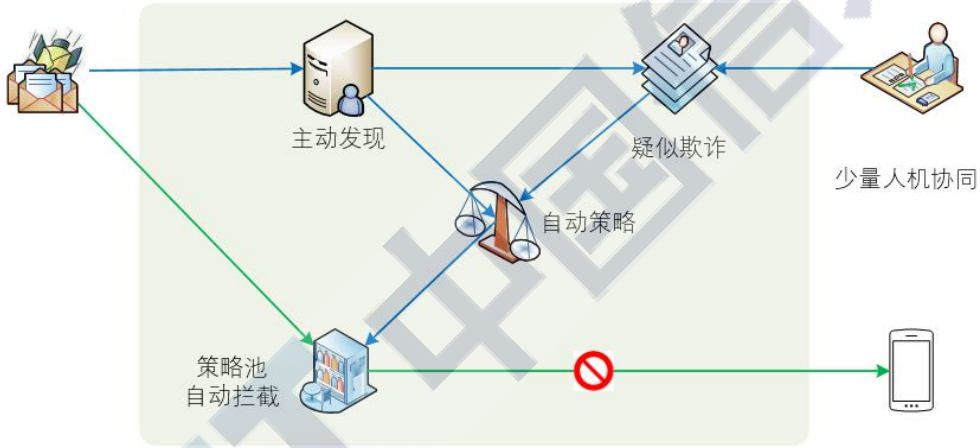
首先，短信组搜集分析大量疑似诈骗案例，分出出售防疫医疗用品、新冠肺炎治疗及预防、疫情期间虚假退改签等三类诈骗内容，获取短信关键词信息，制定部署短信拦截策略，关联出疑似涉诈的QQ、WX、URL及主送和被送手机号码。其次，针对大量新型诈骗突发态势，为提高对抗能力，工作人员坚持在岗，通过获取到的各类诈骗剧本和行为分析，加大对短信拦截的关键词和语义的分析研判力度，扩充有害短信模板库。同时加强与三大运营商企业的协同合作，始终坚守反诈抗疫一线，有效保障人民群众财产安全。

2、智能、高效、精准的疫情短信防诈骗技术创新项目

实施单位：广东电信

面对疫情期间的新型涉疫情诈骗短信，从技术层面上，广东电信利用自建的系统，建立航空诈骗、信用卡诈骗、新冠特效药等诈骗信息模型，人工智能增强实现专题垃圾信息治理，通过关键词、样本库与自研大数据实时分析技术，实时发现诈骗型垃圾短信发送行为特征、内容特征及发送趋势，实时拦截诈骗信息号码并自动更新受限号

码池及内容治理等策略，实现涉疫情诈骗短信的智能治理。此外，利用手机终端溯源的技术，对问题号码进行终端溯源，并通过终端反查其它问题号码，从源头对诈骗信息实施治理。从管理层面上，建立垃圾信息自助举报渠道，通过 10000 号进行推广，并安排值班人员 24 小时关注涉疫情诈骗的举报信息，并及时调整拦截策略，实施自动拦截。疫情期间，系统累计拦截与疫情相关的诈骗短信约 651 万条，治理效果显著。



3、行业短信可信分发，助力 5G 新消息业务健康发展

实施单位：山西移动

疫情防控期间，针对多渠道行业端口短信并发量较大的端口，内容安全管控技术措施滞后、对应管控能力不足等问题凸显，不利于定位潜在违规行为并实时阻断诈骗案件发生。山西移动创新采用了可信分发行业消息安全接入门户，一是充分利用端口行为分析模型、投诉举报数据分析模型、合作渠道投诉数据、端口备案类型库、反欺诈资源库等多数据融合分析，对违规发送行为进行实时阻断，降低被用户

投诉举报风险。二是基于端口基础信息数据库，比对拦截或举报的行为数据，及时审查违规端口，降低通道资源被关停的风险。三是充分利用历史话单、短信签名、内容跨域、举报数据开展基于历史短信记录进行多维度融合分析，对近期易被举报、业务违规的短信端口进行提前预警。四是综合分析端口短信投诉内容及用户退订数据，构建用户意愿画像分析模型，精细划分内容敏感标签意向；同时与通道方企业的端口备案信息进行核实匹配，对命中不愿接收意向的短信发送行为及时进行筛选和阻断操作。五是预充分利用短信预留内容合规性检测中心能力，实现对 URL 的长期监控和回扫，对发送后短信、短链变化的快速响应。疫情防控期间，累计监测处置垃圾短信 579 万条，其中违法诈骗类短信 25.9 万条；新增、更新垃圾短信策略 5915 条，其中与疫情相关 70 条。

C.涉疫情互联网诈骗治理类

1、科技战疫，腾讯在行动

实施单位：腾讯

疫情爆发后，腾讯公司在日常工作中发现有不法分子利用腾讯平台发布虚假售卖疫情紧缺物资信息、虚假爱心捐款信息、骗取学费等违法犯罪行为。反诈团队积极联合公司内部各安全团队，利用安全大数据、人工智能及机器学习等技术手段，运用宾果反诈骗防控系统、鹰眼反电话诈骗系统、麒麟伪基站定位系统等对各类诈骗开展防范治理、预警阻断、落地打击等工作。

腾讯守护者计划整合腾讯20多年黑灰产对抗经验、黑灰产大数据及AI能力，推出守护者智能反诈中枢，致力于帮助用户有效识诈、防诈，对电信网络诈骗犯罪开展全链条打击治理，打造全方位反诈体系。守护者智能反诈中枢通过对腾讯自有平台、工信部门、公安机关及合作伙伴所提供的用户投诉、举报、异常信息等数据进行AI智能分析比对，筛查其中所包含的黑产、欺诈信息，再经由反诈骗专家进行最终的研判。分析确定线索后，智能反诈中枢通过腾讯六大自研反诈系统联动公安机关，对诈骗团伙、链条进行打击治理。

已先后向国务院打击治理电信网络新型违法犯罪工作部际联席会议办公室推送50多批次，6000多条“疫情诈骗”线索，涉及全国31个省、市、自治区，并对多地警方线下打击提供支持。

2、百度多举措打击虚假有害信息，为“战疫”护航

实施单位：百度

疫情期间，网友对各种资讯的需求度持续上升，但海量信息往往真伪难辨，给了不法分子可乘之机。为保护网民信息安全及财产安全，百度积极配合有关部门，利用平台优势，成立专项小组，对相关电信诈骗信息进行清理整治。

百度搜索通过人工巡检发现问题信息集中在论坛等第三方平台，占总体有害信息的90%以上，其中境内活链占总体有效信息的88%以上，主要是售卖口罩、防护服等防疫用品行为。根据该线索，百度立即采取链接屏蔽治理措施，将问题链接添加屏蔽，切断传播来源。同时，百度积极向有关部门反馈相关线索，集中清理第三方平台售卖口

罩信息，积极上报有效的信息线索，联合打击网络电信诈骗。此外，百度也在加强贴吧内部管控，采取四大措施及时捕获诈骗信息并上报处置：一是通过关键词拦截查删并进行人工审核，及时清理有害信息；二是识别拦截有害图片、音视频等样本并落实入库；三是调用公司先进策略模型算法，降低有害信息传播与渗透的发生概率；四是通过用户大数据画像能力，挖掘并关闭账号，处罚恶劣违规用户。

截至目前，百度搜索累计屏蔽相关链接 2799 条；百度贴吧在疫情期间共向公安机关报送有价值的疫情线索 712 条，其中疑似诈骗的线索 85 条，已清理疑似诈骗有害内容 5.3 万余条，封禁账号 159 个，整治不法信息成效显著。

3、基于移动互联网大数据分析，助力疫情期间防范和打击网络诈骗

实施单位：云南电信

为进一步降低疫情期间边境地区诈骗对企业和个人造成的危害，云南电信从多角度、多方位运用移动互联网业务大数据分析手段，获取异常行为用户等信息，研究主流诈骗辅助工具原理，并与有关职能部门深度合作，通过多种打击和管控方法，主动切断诈骗分子与易受骗群体的联系方式，切实有效的降低云南边境地区的整体涉案。目前云南电信从无到有，建立了以下移动互联网分析处置能力。一是反诈方面引入互联网反诈功能，在语音、短信和互联网等反诈领域做到全覆盖的能力。二是在具备普通用户终端管制能力基础上，研究、验证和实现了对主流大容量电诈涉案工具的管控。三是在客服受理被处置

用户投诉时，反诈系统通过接口弹窗功能向客服系统推送差异化的解释口径及处置方法，提升客户满意度。在2020年第一季度，云南电信完成了工信部12321移动号码举报率低于百万分之四的月考核指标，体现出在移动互联网领域反诈工作的成效。

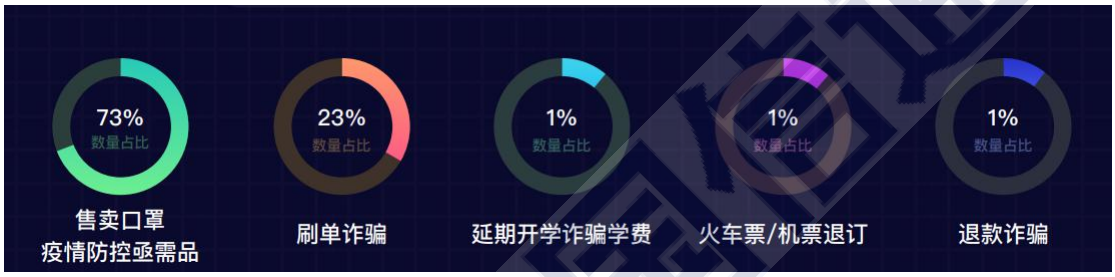
4、新冠疫情期间涉互联网诈骗监测分析

实施单位：任子行网络技术股份有限公司

疫情期间，任子行发挥公司对互联网诈骗事件的监测和研判分析能力，助力抗疫反诈工作落实部署。具体举措包括：一是组织技术力量，利用云计算平台，加强对互联网信息公开传播渠道各类公共信息的采集，通过多种信息智能采集技术每日实时采集信息；二是基于海量数据，采用有监督的机器学习方法，快速迭代，形成智能分析算法，对涉疫诈骗及传统诈骗持续监测和分析，对疫情期间的诈骗态势变化不断分析和总结，每周形成分析报告供管理部门参考；三是发现不法分子利用疫情场景，对传统的投资理财和贷款诈骗进行受害者引流等多种诈骗新手法；分析此类手法的引流网站、涉诈APP和诈骗网站的运行机制并汇报管理部门参考。截止3月底，任子行共研判识别疫情诈骗信息两千多条，向管理部门提供了多份分析报告。

疫情期间，任子行发挥公司对互联网诈骗事件的监测和研判分析能力，助力抗疫反诈工作落实部署。具体举措包括：一是组织技术力量，利用云计算平台，加强对互联网信息公开传播渠道各类公共信息的采集，每日实时采集重点论坛、重点贴吧和微博等信息；二是基于海量数据，采用有监督的机器学习方法，快速迭代，形成智能分析算

法，对涉疫诈骗及传统诈骗持续监测和分析，对疫情期间的诈骗态势变化不断分析和总结，每周形成分析报告供管理部门参考；三是发现不法分子利用疫情场景，对传统的投资理财和贷款诈骗进行受害者引流等多种诈骗新手法；分析此类手法的引流网站、涉诈 APP 和诈骗网站的运行机制并汇报管理部门参考。截止 3 月底，任子行共研判识别涉疫情诈骗信息 2171 条，向管理部门提供 8 份分析周报，配合管局进行了涉案信息分析，形成分析报告两份。



5、虚假售卖防疫物资非法网站识别打击系统

实施单位：成都无糖信息技术有限公司

建立虚假售卖防疫物资非法网站识别打击系统，基于自动发现模块、自动识别模块和自动反制模块，精确识别虚假售卖防疫物资非法网站，洞悉掌握虚假售卖防疫物资非法网站的程序类型、程序版本、组件类型、组件版本等程序特征，获取涉案平台数据和信息，并对非法网站其进行持续侦控，同步涉案信息，实现精准预警和科学研判。虚假售卖防疫物资非法网站识别打击系统还针对非法网站犯罪活动涉案信息查询、关联分析需求，为公安部门在侦查破案、预警防范等方面提供多方位、深层次的情报信息业务支撑服务。

6、基于微博大数据识别的多维度反欺诈技术机制

实施单位：北京微梦创科网络技术有限公司

微博作为大家日常获取信息和社交的主要渠道之一，做好平台的诈骗信息防范，责任和意义重大。微博技术团队以实时分析、识别欺诈内容及用户、第一时间预警提示为首要目标，重点在内容行为及用户实时识别、账号源头、行业联动、安全加固（短链跳转服务）等方面做好技术防范。首先，自主研发应用大数据、机器学习等领域新技术，如实时流处理技术、NLP 内容识别技术、社交图谱聚类挖掘技术，更快、更全、更准地识别欺诈内容和用户。通过持续反诈关键技术的投入，不断提升网络诈骗防范能力。其次，在账号源头上，加强对黑灰产盗号和养号的监控和处置。最大程度减少和避免重点账号被盗、黑灰产批量操作账号带来的疫情事件诈骗。再次，通过与阿里、百度等知名互联网公司合作，充分发挥利用对应公司安全数据历史积累与集群数据处理能力，引入多家互联网公司恶意网址链接检测服务。对微博平台上产生的短链对应的 URL，7*24 小时进行检查过滤，第一时间发现涉诈骗等恶意非法网页并进行拦截。然后，对容易被黑

灰产利用的长链转短的接口服务实行白名单机制管理，建立 t.cn 的弹性切阿里云机制，并开启高防服务。当前累计识别欺诈用户 30 万左右、欺诈内容 180 万条左右，覆盖欺诈场景 14 类。

D.综合类（电话、短信、互联网）

1、“大数据+人工智能”助力疫情期间电信网络诈骗治理

实施单位：中国移动信安中心

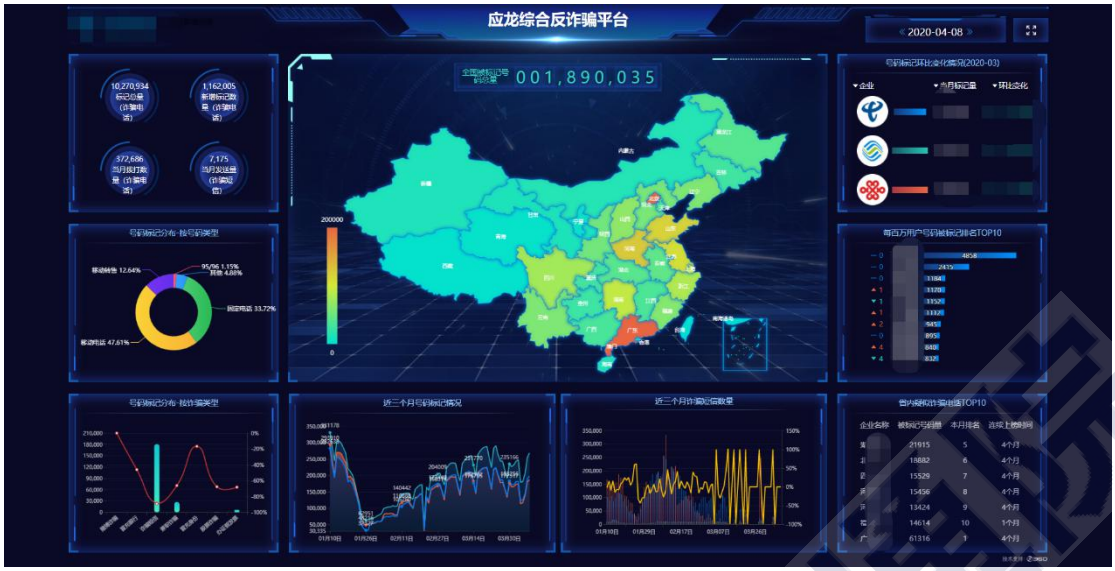
疫情期间，中国移动将大数据、人工智能技术应用到诈骗治理工作中的多个环节，有效提升事前监测、事中拦截、事后防范等能力。一是智能监测分析及研判预警，实现事前防范“盯得紧”。通过分布式 AI 爬虫技术，广泛收集诈骗相关互联网信息，建立多种 AI 分析模型，自动化分析诈骗趋势、情感倾向、热点话题等，实现智能化监控、分析与预警。二是灵活编排分析算法，实现事中处置“拦得准”。引入“微服务”架构，将文本、图片、音视频等各类内容安全分析能力充分解耦，封装为 61 项原子级的算法插件，并可进行灵活编排，针对疫情期间不断出现的新型诈骗场景，可汇聚各类数据、快速搭建精准识别模型，确保及时拦截处置。三是数据智能挖掘，实现事后共享“防得住”。利用大数据分析、人工智能、机器学习等技术，从海量原始数据中提炼出核心数据价值，建成“不良信用库”“客户风险预警案例库”等“威胁情报数据资产标签库”，疫情期间面向全网各单位提供诈骗治理共享服务。四是“云”端高效协同，实现突发事件快速联动处置。打破地域、企业组织壁垒，充分借助移动互联网资源，

建立立体化、多渠道的信息安全“云”沟通平台，助力内外联动，确保高效协同应对突发事件。疫情期间，中国移动累计拦截诈骗等类型短彩信约6.64亿条、骚扰诈骗电话41.15亿次、阻断不良网站访问6814.71亿次。同时，面向客户开展风险预警。通过公司官方微博、微信公众号、10086等渠道向客户发布30个新型诈骗风险预警案例，提升客户防范能力。此外，积极配合公安机关诈骗案件侦查工作，提供1万余条诈骗线索。

2、360手机卫士—应龙综合反诈平台

实施单位：360

360集团手机卫士团队在疫情初期，及时发现了大量与疫情相关的新型诈骗案例，进而对全国疫情反诈态势进行预警，对疫情相关诈骗短信进行拦截。同时，梳理了有潜在风险的疫情相关的诈骗关键词共14个，并基于此识别多种变体组合；持续关注疫情诈骗相关的电话、短信、URL等数据，为工信部反诈系统提供高精准的高危疑似样本累计200余条；结合最新疫情诈骗相关案例，通过公众号发布文章169篇。



3、基于大数据综合分析及呼叫行为关联等技术防范涉疫诈骗等违法行为实践

实施单位：上海电信、珠海高凌信息科技股份有限公司

疫情防控期间，上海电信综合利用反诈系统积累的海量话单、语音和短信等数据，进行呼叫行为关联分析等技术，以实现冒充公职人员、虚假贷款、虚假退改签等涉疫情诈骗电话和短信的精确监测识别和实时拦截；通过 10000999 举报平台实现与友商数据共享和联动处置，根据反诈系统大数据分析结果为潜在受骗客户推送预警及劝阻信息；针对长期占线及深度洗脑的受骗用户，采取话中阻断和被叫保护功能，有效压降涉疫诈骗等违法犯罪，提升防范效果。

4、北京移动启动“智慧中台”对疫情诈骗联防联控

实施单位：北京移动

疫情期间，部分“公检法”电信诈骗犯罪手段升级，不法分子综合利用短信、电话沟通、钓鱼网站等多种手法完成一次诈骗行为，如果只从单一手段入手，难免信息孤立、判断滞后。北京移动充分利用

现有系统和在建系统，整合形成具备联合治理能力的内容治理智慧中台，结合骚扰诈骗电话监控、垃圾短信监控、垃圾短信策略运营分析、行业端口垃圾短信科学管控、网上不良信息监测等多个安全管理系统，开展涉及疫情诈骗信息态势监测，实现系统间数据共享和关联分析，提升反诈综合实力。在具体实施过程中，采用统一数据收集、标准化模型环境、工作流引擎自动反制流程实现数据联动及响应处置，取得良好成效。截至目前，北京移动联合北京公安反诈中心累计关停诈骗电话 7 万余个，拦截违法诈骗类短信 50 万余条，处置钓鱼网站 4117 例，切实保障人民群众生命财产安全。

5、加强 IM 虚假信息监控，预防电信诈骗骚扰

实施单位：贝壳找房(北京)科技有限公司

疫情期间，犯罪团伙通过 IM 软件给贝壳找房经纪人发送虚假消息，开展电信诈骗。贝壳找房安全和风险中心立即成立了专项小组，加强 IM 虚假信息监控，预防电信诈骗骚扰。首先，添加与诈骗有关的敏感词、关键字等内容至 IM 敏感词识别项目的敏感词库中。其次，

对贝壳+、IM、房源平台、商业地产、信息公示、租赁用户等10余个平台开展诈骗敏感词过滤，一旦发现经纪人或用户发布的消息内包含银行账号、出售账户等敏感词或关键字，就会立即对其进行统计、汇集整理和分析。最后，判别是否为诈骗消息，确定为诈骗消息后系统会对其进行拦截或屏蔽，实现诈骗消息的过滤，降低经纪人和用户受骗的可能性，有效预防电信诈骗。同时，考虑到敏感词库的扩容和IM流量的增加，会导致服务器压力加大，提前安排工程师快速上架了硬件设施进行服务器的扩容，保障了专项顺利实施。目前，IM虚假信息监控专项措施已覆盖贝壳找房平台36万经纪人和每日67万用户的信息发布和言论过滤，有效的做到了虚假信息监控，预防电信诈骗骚扰。

E.黑灰产整治类

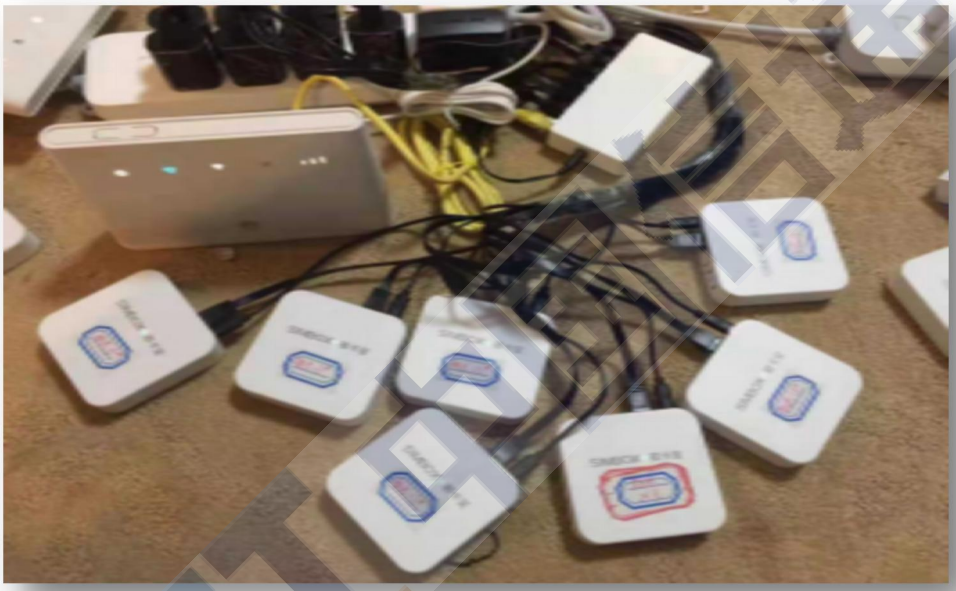
1、重拳出击黑灰产，助力抗疫护安宁

实施单位：广东移动

疫情期间，涉及防护用品、机票退改签、捐款、“冒熟”等类型的电信网络诈骗高发。不法分子大量使用GOIP、多卡宝等黑灰产工具实施诈骗，监测处置难度极大。针对该情况，广东移动基于网络信令和话单的大数据能力，从网络位置更新数据、话单数据中提取符合终端特征的号码及位置信息，与涉案号码特征和公安机关缴获的涉案设备信息进行匹配，自主研发了一系列针对GOIP、多卡宝等黑灰产工具专用监测模型，及时监测使用GOIP、多卡宝等黑灰产工具的主

叫号码和被叫号码，并与公安机关建立快速联动工作机制，及时向公安机关提供涉案信息线索。

疫情期间，广东移动累计向公安机关提供各类线索超5000条，为用户挽回经济损失超千万元，配合公安机关定位侦办了多起涉黑灰产设备的案件，实现了对黑灰产的有力震慑，为抗击疫情、保障民生做出了贡献。



2、“多卡宝”设备电信网络诈骗防治

实施单位：云南移动、中国移动信安中心

面对2020年以来云南边境地区电信网络诈骗依然高发的严峻形势，云南移动积极研究、主动沟通，参与中国移动集团公司专项研究项目，充分利用企业大数据精准定位及多元化分析能力的优势，在疫情期间紧急开展“多卡宝”设备诈骗治理工作。

“多卡宝”设备具备互联网远程操控能力，其操纵者隐蔽性较强。云南移动综合信令行为、上网行为、设备标签等多维度进行关联分析，

总结“多卡宝”设备特征，基于“设备串号”及“URL 访问”两个技术关键点，开展端到端测试和分析，并输出治理手段。一是对“多卡宝”设备进行封堵，即通过探索设备“设备串号”特征，建成拦截大数据模型，关停在云南边境地区使用的“多卡宝”关联通讯号码，并要求客户进行实名制复核。二是对“多卡宝”使用者进行拦截，即通过“URL 访问”特征，建成 URL 拦截模型，关停在云南边境地区“多卡宝”操纵者使用的通讯号码，并要求客户进行实名制复核。截至目前，该机制共识别处置边境区域疑似号码 3405 个，核准率达 99%以上。云南移动在疫情期间为新型设备诈骗治理提供了有利的技术支撑，也为全国其他重点区域提供可推广的“多卡宝”类设备治理思路和防控手段。

3、基于多源数据的 GoIP 诈骗电话分析系统

实施单位：北京微智信业科技有限公司

该系统以通话数据的协议类型、话单内容、IP 地址聚类等为数据源，建立 GoIP 网关设备快速追溯体系，实现快速溯源、精准响应；采用大数据分析算法（如深度学习、决策树等）分析找出诈骗通话行为，定义和输出诈骗 GoIP 通话类型，并具备输出新出现的诈骗通话行为的定义和模型的能力；建设 GoIP 诈骗电话黑样本库；可实时展示 GOIP 诈骗电话检测情况，并对诈骗电话话单信息及时预警。系统可实现日均发现疑似深度受害用户约 300 个，日均发现浅度受害用户约 100000 人，日均发现 GoIP 网关 10 个。

（二）创新管理类

1、创新电信网络诈骗处置手段 协同联动提升案件处置效率

实施单位：山西管局

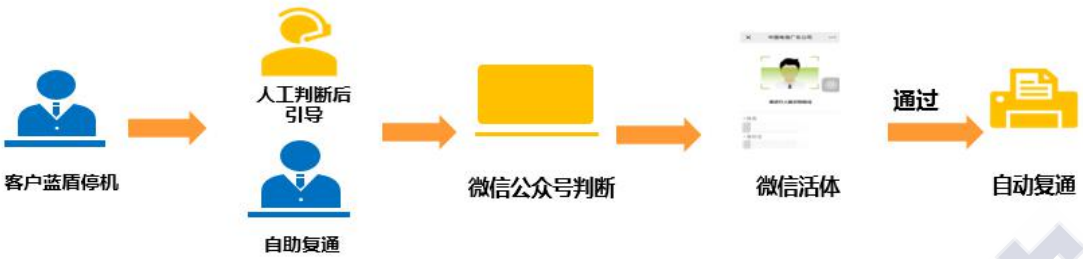
针对发现多起不法分子诱导用户集中办卡并非法收售实名制电话卡用于拨打诈骗电话的事件，山西管局印发了《关于依法严肃处置买卖电话卡的通知》，组织省内三家基础电信企业对涉诈电话号码开展协同处置工作。截止 3 月 31 日，共处置买卖电话人员 325 人，关停电话号码 501 个电话卡，其中，省移动关停电话号码 259 个，省联通关停电话号码 134 个，省电信关停电话号码 108 个。同时，山西管局与太原市公安局建立电信网络诈骗研判机制，实现对涉诈域名、涉诈电话、涉诈短信息的协同研判，为协调处置相关工作提供有力支撑。截止 3 月 31 日，共向太原市公安局推送涉诈短信息 46 件，经太原市公安局研判后推送的涉诈域名共计 698 个。

2、远程认证核实身份，无须到厅处理复通

实施单位：广东电信

针对疫情防控期间因防疫工作者号码被误举报、误关停的情况，广东电信对涉疫情被误关停的个人客户提供在线远程活体复通方式，客户通过关注微信公众号“中国电信广东公司”，输入“异常”，或进入“服务大厅”的“号码异常处理”界面，按指引操作完成后，即能快速复通号码。对涉疫情被误关停的政企客户，提供在线核验身份信息复通方式，客户拨打 10000 号，10000 号在线核验客户在 CRM 系统上留存的身份信息无误后，即可快速复通号码，无须出门到营业厅

进行复通。



3、优化完善疫情期间用户申诉处理复通机制

实施单位：山东移动

为做好疫情防控期间用户申诉的受理与处置，避免用户去营业厅复开增加风险，山东移动进一步完善了线上和电话复开的工作机制。一是建立绿色通道。针对公安机关电话无法打通的情况，建立了绿色通道，在核实用户的身份信息后，做好记录，没有问题的先行复开，然后将相关信息向公安机关报备，避免出现正常用户号码无法复通的问题。二是完善线上处理流程。将原有建议到店处理的流程全部临时改为线上引导并处理，建立了电话、短信、微信公众号等快速解封通道。通过对各类场景的客户号码关停前通过短信告知客户的服务处理环节，被误关停的用户只需按照短信提醒内容登录微信公众号进行在线视频认证，确认是本人在使用对应号卡后即可实现复开机功能，全流程 5 分钟左右，不受时间地域限制，可随时随地办理，方便正常用户快速恢复，提升了用户感知。

4、疫情期间实体渠道针对异常批量购卡联动劝阻机制

实施单位：天津电信

3 月以来，随着全国疫情好转和诈骗黑产复工，异常购卡情况明显增加。针对该问题，天津电信防诈专班协同渠道部及时启动研究并推行如下举措：一是第一时间分析可疑购卡者身份信息规律和开卡规律，精准缩小范围劝阻拦截。二是制定实体渠道防诈注意事项“一看、二问、三确定”，精准指导营业员分辨可疑人员。三是针对地处天津与河北省边界区各区营业厅制定更严苛劝阻举措，对过境批量异常购卡者与河北电信快速联动确认特征，联手阻止。四是灵活解读运用《中华人民共和国网络安全法》，委婉劝阻执意批量异常购卡可疑人员，从法律依据角度有力回绝可疑购卡者，并通过委婉措辞避免相关滋事闹事行为。五是对通信行业一证五卡规则灵活进行二次分流限制，结合本地具体情况适度延长一证购满五卡的周期，在确保合法用户正常享有一证五卡权益的同时，一定程度加大了涉诈人员的批量购卡难度。

5、深化疫情期间警企合作模式，强力遏制号卡涉疫诈骗新形势

实施单位：宁夏电信

疫情防控期间，宁夏电信针对疫情期间诈骗新形式，联动自治区反诈中心，针对性的强化了防诈监测、摸排、核查、甄别、处置、追责工作流程，确定自治区反诈中心为关停执法主体。扩展监测范围，深入摸排高危号码，异常号码实施关停,进一步落实责任，明确代理商及各责任单位追责处罚机制，对每个涉诈号码施行闭环管控。一是开展多点监测。将原有监测范围从漫出涉诈重点区域，扩展到话务异常号卡、友商涉案号码开户人在电信所开号卡。二是深入摸排。由自治区反诈中心主动联系高危号码，掌握用卡基本情况，对于不配合、关机等异常号码实施关停。三是扩展核查、细心甄别。对被举报号码、通报关停号码、高危关停号码的资费、入网时间、受理渠道进行分析。提取重点受理渠道受理清单，通过号码漫游信息、呼叫行为以及套餐等进行仔细甄别，预防性关停异常号码。四是强化处置。对各类举报、通报的涉诈号卡坚决实施关停，同时预防性关联关停名下其他号码。五是强化责任追究。要求责任单位对本区域内关停号卡占比达到 30%的代理商予以现场提醒谈话，占本单位总量 50%及以上代理商，暂停

受理发展权限，暂时停发佣金及各类奖励。

6、强化线上商城订单筛查治理

实施单位：北京联通

疫情防控期间，北京联通紧盯源头治理关键环节，重点针对线上渠道商城售卡加大核查治理力度，从前端入网，订单筛查入手，进一步做好被举报号码订单特征核查，订单处理严把审单、派单环节，做好恶意订单拦截，同时加强被举报号码拓展分析并对疑似号码及时关停处置，完善客户维系感知。在具体工作中，一方面针对高危黑名单客户同步进行订单拦截，2020 年 3 月已将线下的治理高危黑名单客户信息约 16 万个全量导入线上商城系统进行订单拦截；另一方面，针对 2020 年 1-3 月入网订单全面排查，通过对诈骗被举报号码高危客户做拓展核查处置，共计关停及退单号码 3582 个，同时将诈骗电话派送典型特征作为高危信息库，对每日订单进行动态监控拦截。

7、创新处置方式，提升用户满意度

实施单位：湖北移动

疫情期间，湖北移动适时对疫情期间诈骗疑似号码的分析处置流程进行调整，将常规的被动处置（对相应投诉先予以关停，用户停机后被动上门核验）改为主动处置（主动分析、主动沟通客户），极大的降低了误报误处置情况。同时，优化完善疫情期间用户申诉处理复通机制，制定灵活的实名信息核验方式，提升了用户满意度。

8、手机端防诈骗全流程一键关停

实施单位：海南电信

通过大数据平台进行数据建模，模型通过常规话务指标，结合用户的上网行为数据、位置信令数据、手机终端数据、个人基础信息等数据进行分析，经过算法不断迭代优化，最终形成5大防诈骗模型，模型分别是：漫出高危模型、本地高危模型，猫池诈骗模型、黑终端诈骗模型、漫入首次开机模型。模型输出的数据直接发送到指定审核人员的手上，通过手机端进行快速审批、一键关停。

9、抓源头、强管控，上下联动防诈骗

实施单位：青海电信

疫情期间，青海公司成立专项工作团队，对照近年来全国发生的诈骗案例，分析研判青海诈骗形式，全面梳理存量业务，针对酒店完美联盟、400、语音专线等重点业务进行全面排查，严禁业务源头违规办理。专项工作团队通过研判对于存在较大涉诈风险的存量低价值

沉默卡 33577 张进行了全面分析。为了形成上下联动机制，全员参与防诈骗，在专项工作团队分析的基础上，各市州分公司举一反三，指定专人对于前期发展的低价值单产品沉默用户开展核查，核查主要集中于我省办理低价值沉默卡是否流向外地，是否被不法人员收购及问题工号办理的其它业务的合规性核查。通过青海公司全体人员的不懈努力，最终通过大量数据分析，将 635 张高疑号码进行了关停。关停后青海公司防诈专班实时关注用户投诉情况，自关停至今，未接到用户投诉。

10、互联网自助式“e”认证，破解疫情期间“实人”认证难题

实施单位：浙江移动

浙江移动充分利用互联网的便捷性，推出“实人”认证“e”服务，破解疫情期间“实人”认证的难题，确保疫情期间防控管理流程的良性运行。一是明确“e”认证适用对象。“e”认证仅适用于浙江移动基于大数据技术自主分析的高危疑似号码，对于公安通报，12321 涉诈投诉，以及多次识别高危涉诈等相关号码的处置，仍按照原有流程要求执行。二是开放“e”认证通道。为便于用户及时通过“e”认证完成“实人”认证，对于符合“e”认证条件的疑似号码，在处置前触发带有“e”认证路径的短信通知，引导用户使用互联网开展实人认证。三是通过“刷脸”实现“实人”认证。用户可以根据系统提示，完成刷脸，以及《客户承诺书》、《客户服务协议》的确认签署。通过后台人像比对确认后，实现了用户自助式互联网实人认证，解决疫情期间“实人”认证难题。

11、来电名片保障效率，连接信任守护安康

实施单位：广东电信

疫情防控期间，针对在 12321 平台上检测到的多起政府、公安号码因涉及疫情被群众误举报为诈骗电话的情况，广东电信及时安排工作人员核查申诉此类号码，同时派遣客户经理跟进被举报号码单位，向政府、公安等疫情防控单位免费开通“来电名片”服务。通过办理该项服务，政府、公安等疫情防控单位致电居民时，居民手机屏幕上显示单位的“防疫名片”，从而避免误举报、误关停的事件发生，提升了居民对诈骗分子和真实防疫工作者的辨识能力，协助推动防疫工作的有效开展。截止到 4 月 6 日，已为政府、公安等疫情防控单位累计开通 11 万线，发送“防疫名片”140 万次；闪防疫热线电话接听率最高可提升 30PP，有效提升电话接听率，提高防疫工作效率。

12、 “实名实人”用户复机投诉线上认证流程优化

实施单位：陕西移动、中国移动信安中心

疫情期间，为尽可能避免投诉用户到厅店重录实名制，陕西移动特别开通线上认证流程，提升工作效率与客户满意度。首先，客户拨打 10086 投诉时，在告知复机办法时，引导至当地分公司信息安全投诉处理专员，或当地营业厅值班人员。其次，处理人员与用户电话沟通，告知需提供本人持身份证、SIM 卡（可看清串号）的照片，以及信息安全承诺书签字拍照，发送至指定邮箱或处理专员微信。审核通过后，为用户执行开机。再次，3 月下旬，陕西移动微信公众号线上自助实名制认证上线后，增加线上实名制自助认证环节。即：资料审核通过后，由直接开机改为准许用户进入自助认证渠道重录实名制开机。新流程启用后，以一月和三月对比，一月日均电话咨询量 70 余份，到店办理复机约 40 人次，符合条件成功复机的约 25 份；三月日均电话咨询量 80-110 份，到店办理复机 0 人次，符合条件成功复机的约 15 份。结果表明，审核流程比之前更严格，但全部由现场办理改为了线上办理，成效显著。

（三）联防联控类

1、携手公安、友商联合打击电信网络诈骗团伙

实施单位：河南电信

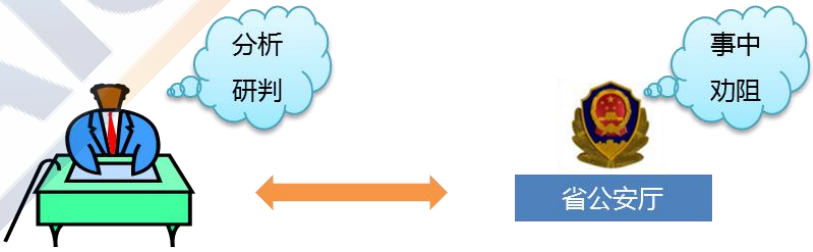
3 月 20 日郑州电信某营业厅发展的 18 张 49 元嗨卡同时漫游至云南高危基站被防诈骗系统拦截。经公司核查，当日 6 个人先后进厅办理手机卡，用户完成了机读身份证、活体检测、人证比对、签字等流程，完全符合国家实名制要求。号码从办理到漫游短短不过 5 天，转移非常迅速。为防止该团伙继续办理号码进行诈骗，郑州电信及时反馈线索至市公安局反诈中心，反诈中心迅速组织三家运营商展开联合协查。经友商郑州联通核查，发现该团伙当日同时间段在友商办理了 21 张手机卡，且全部有漫游云南异常行为。反诈中心迅速将该批身份证信息列入不良信用电话用户清单，有效阻止了该团伙继续办理号码进行诈骗的违规行为。目前郑州电信已安排专人专岗，每小时研判防诈骗系统输出异常漫游号码，协同反诈中心、联合友商协查处置违规用户，主动、批量拦截异常号码。

2、强化政企联动机制、积极开展事中劝阻

实施单位：山东移动

针对疫情期间人民群众迫切的购买物资心理极易被诈骗分子利用，导致虚假购物类诈骗高发的情况，山东移动在已有大数据监控模型的基础上，积极协同管局、公安开展联防联动，建立起诈骗电话关停—受害人劝阻两层机制。一是基于诈骗电话监控模型精准关停。通过大数据实时处理技术，对系统监控到的高度疑似诈骗号码进行预警监控，研判人员分析研判之后对诈骗号码进行关停。二是实施受害人事前劝阻。在关停诈骗号码的同时，通过政企联动系统同步将与诈骗号码产生通信的受害人号码推送给省公安厅反诈中心，并为反诈中心免费开通行业短信端口，用于给疑似受害人发送劝阻短信，对受害人进行合理劝阻。

山东移动与公安、省通信管理局建立联动机制，有效利用运营商的网络、渠道资源和公安部门的执法权和公信力，通过由运营商免费提供短信端口，由公安提供短信内容，对电信诈骗疑似受害人开展事中劝阻等干预工作。目前通过公安厅短信端口，累计下发劝阻短信 10 万余条，有效预警疑似有害用户 3000 余人。



3、利用大数据分析支撑公安精准打击本地活动 GOIP 设备

实施单位：陕西移动、中国移动信安中心

疫情之下诈骗团伙活动猖獗，行动隐蔽且频繁更换活动地点和时间，公安机关需要相应的技术手段与能力对其进行监测及定位。陕西

移动为支撑公安打击犯罪，针对该非重点治理范围，及时调整治理方向，组织各领域专家组成技术小组，购买并租借 GOIP 设备，基于 GOIP 特征展开多维度技术分析。根据省公安厅通报的团伙号码线索，研究制定“基站高频活动突增监测”等多项大数据分析模型监察侦测团伙活动，辅助线索搜集。同时组织团队临时调整基站技术参数，为公安机关提供定位服务。公安机关根据提供的线索数据，一周内连续破获 7 起案件，捣毁若干本地活动的特大型诈骗团伙。为此，陕西省公安厅联合省通信管理局力荐移动公司良好经验，并向全省其他地市大范围推广。

4、警企联动部署实施短信收端拦截疫情涉诈短信策略

实施单位：上海电信

疫情期间，针对上海地区频繁报告“短信+电话”组合方式诈骗案件和受害人数增幅明显的情况，上海电信与公安反诈中心及友商基

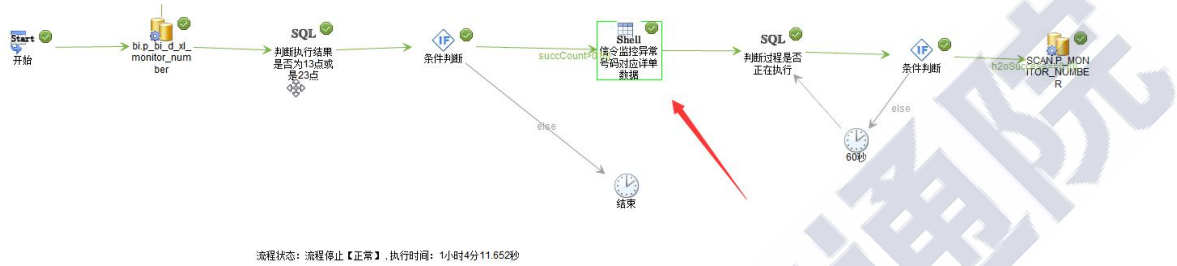
于大数据关联分析协同联动、及时处置，打击通讯违法犯罪行为。一是根据公安机关提供的涉诈短信样本及关键词，上海电信综合分析设定上百条符合实际防范情况的拦截策略，在短信接收端网元部署实施。二是收端部署可拦截不同运行商发送至本网的短信。本网发送的可即时对短信平台或手机号实施封堵，友商发送的会将相关数据通过10000999 诈骗举报平台转至友商处理，形成协同防范处置的效果。自疫情发生以来，共计拦截疑似涉疫诈骗短信 4300 条次；根据上海市反诈中心反馈，上海电信短信诈骗受害者数量大幅下降，成效明显。短信接收端成功实施拦截策略也获得上海市通信管理局及上海市公安局反诈中心认可。

5、利用信令数据构建诈骗用户识别预警模型，配合公安机关坚决打击违法犯罪行为

实施单位：海南联通

海南省儋州市是全国 13 个电信网络诈骗重点地区之一。新冠肺炎疫情发生以来，为进一步防范打击不法分子利用通信网络实施诈骗违法犯罪活动，海南联通积极与儋州市反诈中心加强合作，上线外省漫入儋州高危地号码模型，在诈骗行为实施前尽可能短的时间内就主动关停，协助儋州公安对漫入诈骗案件的办理。一是借助大数据平台能力，增加对外省号码漫入海南儋州特定区域内的号码进行分析，辅助儋州公安对漫入海南儋州的号码进行有效预警判断。二是对用户信令数据进行解析入库，实时分析用户语音通话特征，大幅压缩异常号码检出时延，每日推送疑似诈骗号码至儋州反诈中心进行研判。疫情

期间累计推送号码 2938 个，经公安机关研判准确率最高达到 70%以上。积极配合公安部门开展打击电信诈骗犯罪“3·25”集中收网行动，抓获一批电信诈骗犯罪嫌疑人，重点地区电信诈骗高发态势得到有效控制。

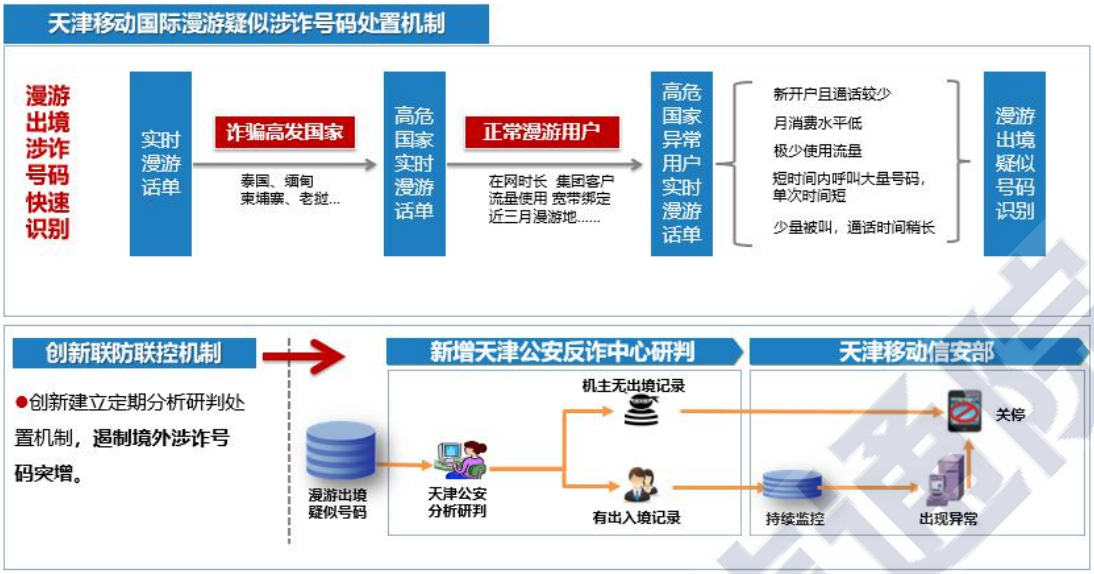


6、创新联防联控机制，精准打击境外电信网络诈骗

实施单位：天津移动、中国移动信安中心

疫情防控期间为落实电信网络诈骗防范治理工作要求，天津移动在集团公司信安中心、公司网络安全领导小组的指导下，重点加强对漫游到东南亚地区新增号码的监测力度，在移动集团内率先与属地公安反诈中心建立漫游出境号码对应身份信息出入境甄别机制，根据公安机关甄别结果进行处置，逐步实现境外诈骗电话的快速精准拦截。一是从入网时间、入网渠道、近期通话特征等多维度开展疑似诈骗电话的识别。二是与天津市公安反诈中心初步建立联合研判机制，将疑似号码报表等信息提交至市公安反诈中心研判及核查。三是根据公安机关研判结果，针对疑似号码对应的异常情况客户采取关停处置。2至 3 月，天津移动向市公安反诈中心提交国际漫游疑似涉诈号码 219 个，经全量研判，累计处置疑似涉诈号码 176 个，处置准确率 100%。据统计，疫情期间天津移动漫游至东南亚国家涉诈号码量较 2019 年 11 月下降 70%，有效遏制了疫情期间漫游出境号码涉诈上升势头，为

疫情防控工作提供坚实网信安全保障。



7、精准抗“疫” 腾讯赋能疫情防控加速度！

实施单位：腾讯

疫情防控期间，腾讯迅速成立疫情类诈骗专项治理团队，上线疫情专项举报入口，从线上对抗、线下打击、用户教育等维度层层发力，深入开展平台治理。一是持续线上对抗，有效遏制疫情诈骗。腾讯客服团队快速部署远程坐席，全体成员主动放弃春节假期，紧急启动远程办公机制，于 1 月 28 日紧急上线疫情专项举报入口，截至 3 月 30 日，腾讯 110 累计受理约 30 万起疫情专项举报，处理涉疫情相关违规帐号 80389 例。二是积极输送数据，推动刑事打击。腾讯客服及相关安全团队紧急成立疫情诈骗专项的黑产研究团队，每日对海量用户举报信息进行聚类分析，筛查其中所包含的黑产、欺诈信息，分析确定线索后，每日向国务院反诈联席办推送疫情类诈骗线索。截至 3 月 30 日，累计移交线索并协助警方侦破疫情相关案件 14663 件，抓获嫌疑人 6513 名。三是深化用户教育，体现平台社会责任。每日发布

疫情期间高发的诈骗手法解析文章，并通过权威媒体、腾讯 110 小程序、公众号、微博、短视频等多渠道传播，及时告知大众疫情诈骗态势和手法，以多种形式对用户进行宣传教育。

（四）宣传引导类

1、疫情期间建立差异化的反诈宣传机制

实施单位：山东移动

疫情期间，针对人民群众高度依赖网络途径，各类生活工作场景由线下向线上转移的新特点，山东移动有效利用企业自身技术和数据优势，根据大数据分析结果和公安机关提供的相关数据，对用户进行精准分类，对每类用户可能涉及的诈骗案件进行分析，并制定不同的宣传提醒口径进行警示。

山东移动面向学生家长、待业人群、未开学大学生和财务人员等不同的用户群体，通过利用“和彩印”功能、行业短信等方式，差异化地对以上类型用户进行诈骗宣传提醒，有效狙击诈骗分子不同的诈骗场景，提升宣传工作针对性，降低诈骗事件发生率。目前，山东移动针对全省易受骗高危用户的不同用户群体，利用“和彩印”、行业短信等宣传途径，累计宣传覆盖 2.3 亿人次，有效降低山东移动诈骗电话举报率。

2、全民创意宣传反诈，护航抗疫稳定民心

实施单位：广东移动

针对各类涉疫情电信网络诈骗层出不穷的情况，广东移动紧密跟

踪电信网络诈骗新手法、新花样、新工具，一方面发动全省员工开展反诈创意作品征集活动，共评选出《鼠兄诈骗小讲堂》、《贪念先生要机警》等6项反诈创意短视频，以及《正义之锤》、《“防骗”成语新解》等5项反诈创意宣传品；另一方面结合互联网领域和新兴领域诈骗案件，制作了利用区块链、杀猪盘、博彩网站、套路贷等手段的诈骗方式揭秘内容，通过微信、微博、短信、抖音、海报等方式进行宣传，并提供给公安机关进行全社会宣传。广东移动为贴近用户，创新探索如剪纸、漫画、短视频、短彩信等广大群众喜闻乐见的宣传形式，采用新旧媒体相结合、线上线下相结合的宣传渠道，累计向全省用户发送防诈骗提醒短信2.72亿条，发布防范疫情类诈骗宣传内容19篇，向公安机关提供反诈宣传素材11项，取得了良好反诈宣传效果。

3、钱盾反诈机器人抗疫期间反欺诈创新实践

实施单位：淘宝（中国）软件有限公司

疫情防控期间，不法分子诈骗手段“花样翻新”，为避免公众上当受骗，各地反诈中心与阿里巴巴联合推出钱盾机器人，通过“公安

反诈专号”发出反诈短信、闪信等强制提醒，开展技术升级和话术升级，推送疫情反诈预警信息1300万条，向潜在受害人拨打劝阻电话14万余次，预警销售口罩、防控疫情捐助等相关骗局。

首先，“钱盾反诈机器人”运用高科技手段开展预警劝阻，可同时通过电话、短信、闪信三种渠道，快速向被骗群众发布预警。其次，普通民众接到电信网络诈骗电话，公安部刑侦局钱盾反诈预警系统收到预警，钱盾反诈机器人立即自动拨打潜在受害人的电话或通过闪信强制弹窗提醒，来电信息显示为“公安反诈专号”。若潜在受害人在5分钟内既不接电话，也未处理闪信，钱盾反诈机器人会再次拨打电话、发送闪信，反复直至潜在受害人处理提醒信息。再次，“公安反诈专号”有专项技术保护措施，以确保来电显示字段不会被盗用、篡改。同时民警可根据不同类型电信网络诈骗的话术，通过AI语音交互技术获取相应的劝阻提醒内容，引导潜在受害人走出诈骗圈套。截止目前，钱盾反诈机器人已覆盖全国31省、市、自治区，共挽回群众损失超过2亿元，累计精准劝阻预警43万人次，劝阻成功率达97.7%。

4、支付宝反欺诈防骗宣传引导创新实践

实施单位：支付宝（中国）网络技术有限公司

针对疫情期间口罩诈骗、企业贷款诈骗、网课诈骗、复工求职欺诈等案件高发的情况，支付宝联合警方、抗疫防骗《警花说》、支大宝反诈等共同合作，以短视频、文章等内容警示宣传防骗技巧，提升用户防骗安全意识。一是在抗疫防骗《警花说》发布近期网课诈骗的

安全提醒，结合当下网课热点，通过支付宝安全弹窗，提醒上网课用户增强防骗意识和确认安全交易，得到公安部刑侦局等 13 家公检法蓝 V 转发。二是推出防骗功能---叫醒热线，当风控系统识别到欺诈风险时，以一对一电话方式及时唤醒被骗用户、防止资金损失。支付宝以日常点滴故事结合节点性重磅事件使宣传面广泛且有效，抗疫防骗《警花说》累计完成全网曝光量 3324 万；针对疫情期间保健品欺诈，推出的话题#90 岁妈妈教 70 岁女儿做人#，还原高龄化母亲对话女儿的生活化防骗场景，曝光 1.1 个亿；安全团队联合策划话题#45 个人群里 44 个是骗子#，通过真实案例还原，提醒广大受众提防新型诈骗，全网话题阅读量 1 亿，全网互动量 9.4 万，视频播放量达 1336 万。

5、“全民反诈首都无诈”疫情期间警企联防联控系列宣传活动

实施单位：北京电信

为加大电信网络诈骗犯罪防范宣传力度，北京电信积极开展“全民反诈、首都无诈”警企联防联控、线上线下协同宣传系列活动。一是制作警企联防联控个性化创意反诈宣传品。针对公安部最新发布的 19 类电信网络诈骗犯罪，重点围绕五类高发突出犯罪，制作使用北京电信及北京市公安局刑侦总队反诈原型人物的海报、折页等宣传品；在各营业厅和公安局所，张贴、滚动播放宣传品；电子版同步投放到电信网厅和掌厅。二是在“北京电信”及“北京反诈”官方公众号、微博、今日头条、直播间等媒体发布宣传软文或视频；并积极转载工信部的宣传软文。三是对全网用户发送疫情反诈宣传短信。四是

充分利用防疫民警驻守社区，对重点社区张贴宣传海报，发放宣传折页。目前，北京电信联合北京反诈、北京刑侦持续开展微信、微博、今日头条、抖音、直播间等新媒体平台的宣传，组成首都反诈新媒体矩阵，向群众及时宣传疫情期间高发诈骗类型并引导防范，形成了深入民心的全民反诈强大声势，为配合打击治理电信网络诈骗犯罪营造了良好的社会氛围。

6、五个第一，打响疫情反诈骗宣传战

实施单位：福建联通

疫情初期为保护用户信息与财产安全，福建联通第一时间响应电信网络反诈需要，启动反诈公益宣传工作，制定宣传计划安排与应急机制，快速进入“战斗准备”状态。首先，联通多个部门指定专人组建反诈宣传第一梯队，保障全天候响应反诈宣传任务，第一时间将工

信部、政府部门发布的防诈骗信息宣传到全省用户。其次，为确保宣传效果一流，福建联通根据涉疫情诈骗手段及特点，针对各种场景及时预警宣传；先后采取“防疫情电诈”公益短信系列、福建联通微信、微博公众号、营业厅 LED 屏滚动播放等方式扩大宣传面，累计发送短信 5776 余万条，原创宣传文稿 20 余份；同时将反诈骗宣传与普法宣传相结合，通过“小沃普法”宣传案例及小贴士系列，普及大众关于电信网络诈骗犯罪的法律知识，营造全民反诈骗的良好社会氛围。再次，福建联通对外与当地公安机关、省政府各相关厅局展开公益宣传联动，按日向省通信管理局报送日报；对内将所有反诈宣传通过全省职工之家公众号 100%覆盖到全省员工，同时倡导员工积极利用微信朋友圈扩大社会宣传，用实际行动践行国企干部员工的社会责任。

7、新媒体助力宣教工作显特色，多措并举开展防范电信诈骗宣传

实施单位：广东联通

不法分子诈骗手段“花样翻新”，让老百姓认识并懂得防范电信诈骗，是治理电信诈骗工作的重中之重。广东联通积极打造宣传载体，丰富宣传形式，精选宣传内容，充分发挥新媒体优势，扩大反诈宣传的传播面和影响力。一是通过警企联动走进社区加大入户宣传力度。以贴标语、挂横幅、派发宣传单等形式，提醒群众提高安全防范意识。截至目前，开展集中宣传 6 场次，发放宣传资料 2000 余份，接受群众咨询 20 余人次。二是采编真实案件案例依托新媒体渠道深入宣传。结合广东省疫情期间发生的真实案件，汇总盘点高发电信网络诈骗种

类与特点、作案手法与方式以及识别、防范方法，通过 “广东联通”官网官微、抖音、朋友圈、民警民生群等新媒体平台发布软文、视频，提醒广大员工和市民切勿中招，累计发送软文 15 篇，视频 3 个。三是设计“盟二哥”使反诈形象深入人心。以“关二哥”为灵感，反诈吉祥物——“盟二哥”的设计代表正气、守护、正义。历史传统人物特色与反诈创新相结合，不仅便于广泛记忆，同时还制作宣传警示视频、防诈手机壳、防诈飞行棋、抱枕等衍生作品，让广东联通反诈吉祥物融入到人们生活的方方面面，扩大反诈宣传的传播面和影响力。

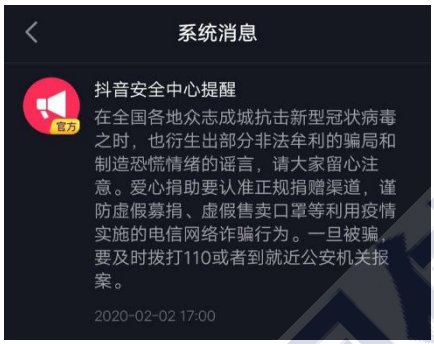


8、抖音多渠道全方位做好疫情期间防范治理电信诈骗宣传

实施单位：北京微播视界科技有限公司

疫情期间电信网络诈骗高发，抖音公司加大反诈宣传力度，对用户实施多渠道、全方位宣传引导，提升电信网络诈骗行为防范意识。一是针对高发诈骗类型，抖音通过抖音短视频、抖音站内信、抖音专设宣传版块、今日头条号、微信公众号、微博等多个渠道，向用户及时发出防诈辟谣等提示提醒，将宣传引导信息广泛触达用户。二是发布的宣传引导内容涉及科普教育、鉴真辟谣、防诈知识、打击公告等全方位信息。抖音将虚假募集、虚假售卖防疫物资等多种涉诈风险，

科学、有效地传至用户，以真实正向信息的宣传，对抗虚假诈骗信息的散播，以典型涉诈案例为反面教材，引导广大用户提高警惕，避免上当受骗。截至 4 月 1 号，抖音发布的防诈站内信触达全量过亿用户，抖音官方安全帐号发布的防诈安全教育视频总观看量超 100 万次。涉及抖音的涉疫情类诈骗发案量、反馈量整体处于较低水平。



中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62303731

传真：010-62300264

网址：www.caict.ac.cn