



广州市电信网络诈骗犯罪审判 白皮书

(2016—2018年)

广州市中级人民法院

2019年5月16日

目 录

前 言	1
一、电信网络诈骗犯罪案件的概况及特点	2
(一) 诈骗手段多样, 手法频繁更新且新旧模式并存 ...	3
(二) 犯罪主体年轻化特征明显	10
(三) 广州法院案件审判质效较好	11
(四) 纠纷类型多样, 案件审理难度较大	12
二、电信网络诈骗犯罪案件产生的原因	12
(一) 大量个人信息遭泄露、甚至被买卖, 成为 犯罪分子筛选潜在行骗对象的重要手段	12
(二) 移动通信网络的防护存在安全隐患, 缺乏对 电信企业和银行的有效监管	13
(三) 犯罪分子依靠技术手段, 具有较强的反侦查 能力	13
(四) 被害人因自身贪念、心理承受能力差、识别 能力差等弱点, 易陷入犯罪分子精心设计好的 圈套	14

三、电信网络诈骗犯罪案件审判工作的主要做法	14
(一) 重视电信网络诈骗案件审判工作	14
(二) 扎实做好电信网络诈骗案件的审理工作， 提高审判质效	15
(三) 加强协调配合，建立多部门联动、跨区域 协作机制，形成打击合力	16
(四) 加大宣传力度，提高公众防范电信网络诈骗 的意识	17
四、防范电信网络诈骗犯罪的对策及建议	18
(一) 妥善保管个人信息	18
(二) 加强账户安全管理	19
(三) 提高金融安全意识	19
(四) 培养良好支付习惯	20
结 语	22
附件：广州法院电信网络诈骗犯罪审判十大典型案例	23

前 言

现代信息技术在高速向前发展，近年来，信息网络的普及，促进了经济社会平稳快速发展。据相关资料统计，截至 2018 年 12 月，我国网民规模为 8.29 亿，网民的人均周上网时长为 27.6 小时。网络信息量大，传播速度快，具有高度便捷性、互动性、透明性和开放性等特点。即时通讯、移动支付、网购、外卖、网约车等极大方便了人民群众的学习、工作和生活。但与此同时，利用信息网络实施的新型违法犯罪活动也日益增多，特别是电信网络诈骗犯罪呈日益高发趋势，严重侵害人民群众财产安全和合法权益，已成为当今影响社会治安的突出违法犯罪问题。习近平总书记强调，“在互联网这个战场上，我们能否顶得住、打得赢，直接关系我国意识形态安全和政权安全。”

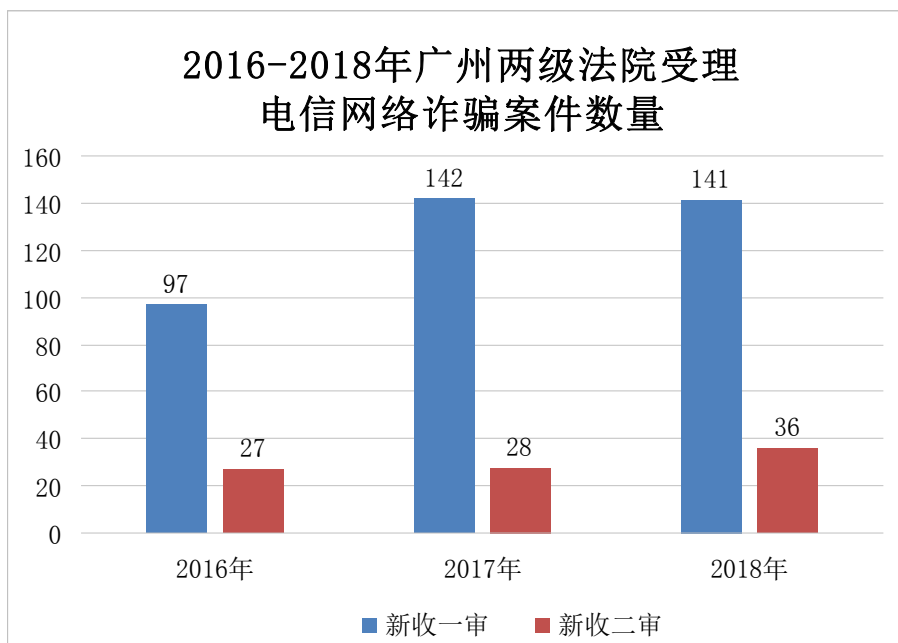
“过不了互联网这一关，就过不了长期执政这一关。”

广州市两级法院历来十分重视对人民群众合法权益的保护，认真贯彻中央及省、市重点整治电信网络诈骗犯罪的要求，紧紧围绕司法为民、公正司法的工作主线，

充分发挥刑事审判职能，完善工作措施，依法惩治电信网络诈骗犯罪，取得了良好的法律效果和社会效果，为促进经济发展和社会稳定提供了强有力的司法保障。

一、电信网络诈骗犯罪案件的概况及特点

2016-2018年三年间，广州市两级法院新收一审电信网络诈骗案件380件1473人。其中2016年新收一审97件372人，2017年142件556人，2018年141件545人。广州中院2016-2018年新收二审电信网络诈骗案件91件530人，其中2016年新收二审27件185人，2017年28件144人，2018年36件201人。整体而言，案件高发、频发，数量整体呈上升趋势。



2016 - 2018 年广州市两级法院审结一审电信网络诈骗犯罪 342 件，判处 1277 人，其中被判处五年以上重刑的共 193 人，处罚金人民币 38,921,000 元。广州中院 2016 - 2018 年审结二审电信网络诈骗案件 91 件 532 人，其中 2016 年审结二审 29 件 160 人，2017 年 30 件 184 人，2018 年 32 件 188 人。其中 2017 年审结的李某某等 25 人电信网络诈骗案，被害人数为 761 人，总计诈骗数额高达人民币 5000 多万元。

（一）诈骗手段多样，手法频繁更新且新旧模式并存

电信网络诈骗犯罪的形式层出不穷，常见的多达 30 余种，诈骗手段不断翻新，从最初的以“中奖”形式实施诈骗，到现在的诈骗领域涉及金融、电信、社保、物流、交通、电子竞技等各行各业。许多犯罪分子还会根据社会热点、潮流、政策等信息，针对不同职业和年龄段的人员，精心设计骗局，令人防不胜防。从我市审理的案件看，主要有以下类型：

一是通过网上虚拟平台，发布虚假信息引诱汇款诈骗。此类犯罪案件约占全市已审结案件的 23.98%。犯罪分子利用网络、打电话、信息群发等方式，发布融资贷款、

办理入户、招聘、租房、就学、推荐股票、考试保过、招嫖、为网络赌博提供保证金、中奖信息、网络刷单返利、合作生意、兑换外币、网上刷业绩返款、慈善捐款可以“以一返十”等虚假诈骗短信或信息，引诱被害人按照其预先设置好的程序进行转账汇款、交费等操作，骗取钱财。例如，有些案件是被告人在互联网上发布虚假私家侦探信息，以开展调查婚外情、开房记录、手机卫星定位等业务收取调查费、保证金为由实施诈骗活动。

二是网上购物诈骗。此类犯罪案件约占全市已审结案件的 14.62%。犯罪分子在网上发布低价销售 iPhone 手机、电脑、相机、电动车、摩托车、服装、游乐园套票、演唱会门票、球鞋、电子购物卡、玉器、“海马”“燕窝”等中药材的虚假信息，骗取被害人的订金或货款。近几年，随着网络游戏及微信抢红包等风靡，犯罪分子的诈骗手段日益翻新，利用网络或电话虚假出售游戏装备、充值 Q 币、游戏点券、游戏币等，谎称其能出售麻将作弊软件，以收取押金、授权码使用费、开通费、诚意金等借口结伙骗取或利用网络上已过期无法正常使用的微信抢红包软件，以高价售卖等方式骗取被害人财产。

三是冒充专家推销假药、“三无”伪劣产品等诈骗。此类案件约占 14.33%。以诈骗的方式向被害人推销减肥、丰胸类等保健品。通过角色扮演，以假装调查被害人购买减肥、丰胸类等保健品后服用感受，要求客户拍身体部位照片，捏造客户病情，冒充权威人士向被害人提供减肥、丰胸等知识咨询，夸大产品功效，诱骗被害人向其购买“三无”保健品。例如，已审结的以谢某某为首的特大诈骗犯罪团伙，首先利用网络平台投放广告发布虚假信息，推销声称具有壮阳功效的“英国卫裤”产品，在全国范围内吸引顾客购买。期间，被告人非法获取患有三高、糖尿病等慢性疾病的老年客户信息后导入电脑 K8 系统，并推送给网管，由网管分派给一线组员；组员假冒中国中医研究院调查科主任等身份拨打客户电话，按照虚假内容的话术单，以用药调查、分析病情等名义骗取客户信任，谎称治愈康复功效推销该司药品或将有购买意向的客户通过 K8 系统转给二线组员，二线组员假冒中国中医研究院专家、院长等身份继续拨打电话诱骗客户购买其公司药品。随后，被告人将网上购得的药品、保健品等委托快递公司送货并代收货款。

四是冒充银行、电信等客服人员诈骗。此类犯罪案件约占全市已审结案件的 9.65%。犯罪分子利用改号显号软件、伪基站等设备，冒充银行、电信、移动客服号码广泛发送信用卡消费、网银升级、电子密保过期、积分兑换、办理优惠套餐、假冒中国移动公司 10086 号码发送虚假话费充值信息等虚假诈骗信息，诱骗被害人按其方法操作或收取费用，达到诈骗目的。例如，增城法院审结的一起诈骗案，犯罪分子利用车上搭载的“伪基站”设备及手机发送虚假的中国建设银行诈骗短信，先后在广东省海丰县、惠阳市、广州市增城区等地人口密集区域，驾车移动发送诈骗短信共约 4 万多条。

五是以恋爱交友为名诈骗。此类案件约占 9.65%。犯罪分子使用虚假身份在婚恋交友网站注册虚假信息，以恋爱交友名义取得被害人信任，通过编造各种理由，例如购房、家人生病急需用钱等，骗取被害人财物或引诱被害人进行高额消费。

六是“猜猜我是谁”“我是你领导”“你到我办公室来”等冒充熟人诈骗。此类案件约占 9.06%。犯罪分子用电话或通过 QQ 等社交账户联系被害人，以“猜猜我

是谁”等语言骗取被害人信息，或通过已购买得知的被害人信息，冒充外地的朋友或亲戚、领导，在骗取被害人信任后，谎称自己正在出差办事，并以出车祸、嫖娼或赌博被抓、家人住院、急需借钱、在国外转账给航空公司不方便等理由，要求被害人通过银行汇款救急而达到骗取钱财的目的，或假装生意合作伙伴、冒充房东等，骗取对方汇款到自己账户。

七是冒充国家工作人员等方式骗取被害人财物，达到非法占有的目的。此类案件约占 4.97%。犯罪分子冒充国家安全局、公安机关、检察机关、邮电局、社保局等国家工作人员称被害人涉嫌洗黑钱及名下的银行存款有非法所得等，骗取被害人钱财，达到非法占有的目的。例如，很多案件中诈骗集团按照统一安排，犯罪分子分别充当一线、二线人员，冒充医保部门、公安局等国家工作人员身份，通过向不特定中国大陆公民群发诈骗语音包、拨打电话，利用改号软件及“钓鱼网站”链接、“木马”程序链接等电信技术手段，向被害人虚构其医保卡被盗刷、个人信息被盗用、涉嫌犯罪、资产需要清查等事实，诱骗被害人向该诈骗集团所控制的账户转账

或汇款，骗取其钱财，或者冒充最高人民检察院检察官，向被害人虚构个人信息泄露、涉嫌贩毒、洗钱等重大刑事犯罪，资产需要清查、保全等事实，诱骗被害人将资金转至“安全账户”。

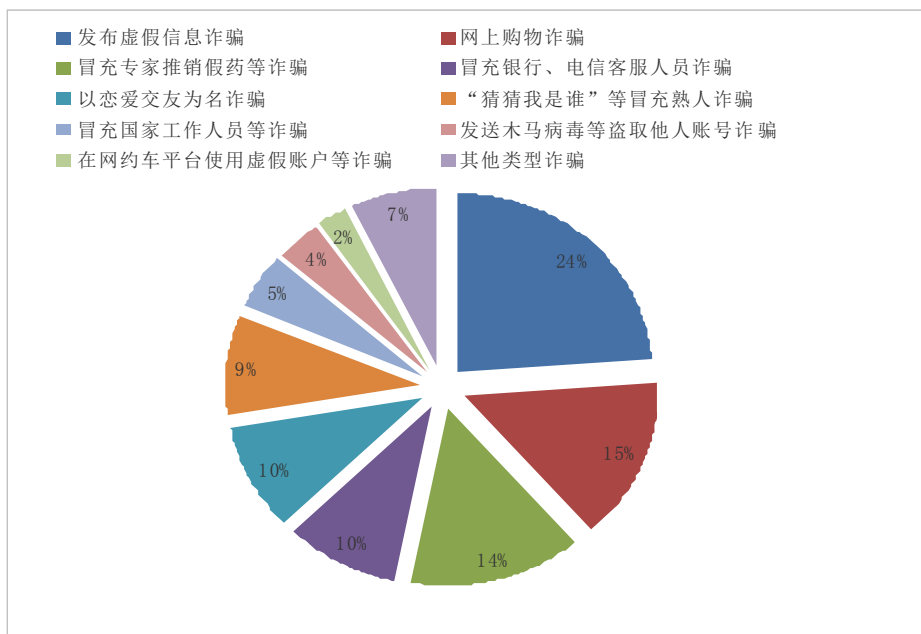
八是通过发送木马病毒、盗取他人微信账号密码、篡改他人邮件等获取被害人个人信息的方式，达到骗取财物的目的。此类案件约占 4.09%。犯罪分子通过互联网发送木马病毒，利用木马病毒程序盗取中木马病毒手机用户的姓名、身份证号码、银行卡号及银行绑定的手机号等信息，然后利用网上支付的方式盗刷用户的银行卡购物。例如，通过在互联网上发送带有木马病毒的信息链接盗取他人 QQ 账号及密码，后从被盗 QQ 号主人的好友中物色诈骗对象，并冒充 QQ 号主人向诈骗对象谎称有物品从国内托运到国外，同时让被害人通过电话与所谓的物流公司经理联系后得知因为没有支付货款而没有发货，再以 QQ 号主人在国外无法在国外转账到物流公司等托词，让被害人通过转账代为支付物流费的方式进行诈骗。

九是使用虚假账户以低价招揽代客叫车业务，在直

接收取乘客车资后，采取不付车资给网约车平台的方式诈骗。此类案件约占 2.34%。近几年，随着网约车的盛行，此类犯罪案件也越来越多。犯罪分子通过技术手段获取虚拟的手机号码、验证码等信息，冒用他人信息资料在网约车平台上注册大量隐瞒其真实身份的虚假账号，并使用这些虚假账户以低价招揽代客叫车业务，待需要用车的乘客向其提出用车需求后，即使用其恶意注册的滴滴账户等呼叫快车，提供给乘客搭乘，并收取乘客数十元不等的费用，但其在司机服务结束后却不支付任何费用。

十是其他类型。除上述的案件类型，还有少量其他类型的案件。近几年，随着微信抢红包和网络点餐的增多，还出现了新型电信网络诈骗案件，犯罪分子通过发布“微信红包外挂软件”“抢红包软件”广告，诈骗被害人财物，或使用其在互联网上非法购买的身份信息，在美团外卖平台上注册“骑手”ID，见到有用户下单美团跑腿代购服务，就抢下客户订单，电话联系客户要求加其微信，然后以自己钱不够为由，让客户先将购物款项通过微信转账至其微信账户，收到钱后即将客户拉黑。

此外还有少量 ATM 机虚假告示诈骗、虚拟交易等类型电信网络诈骗案件。

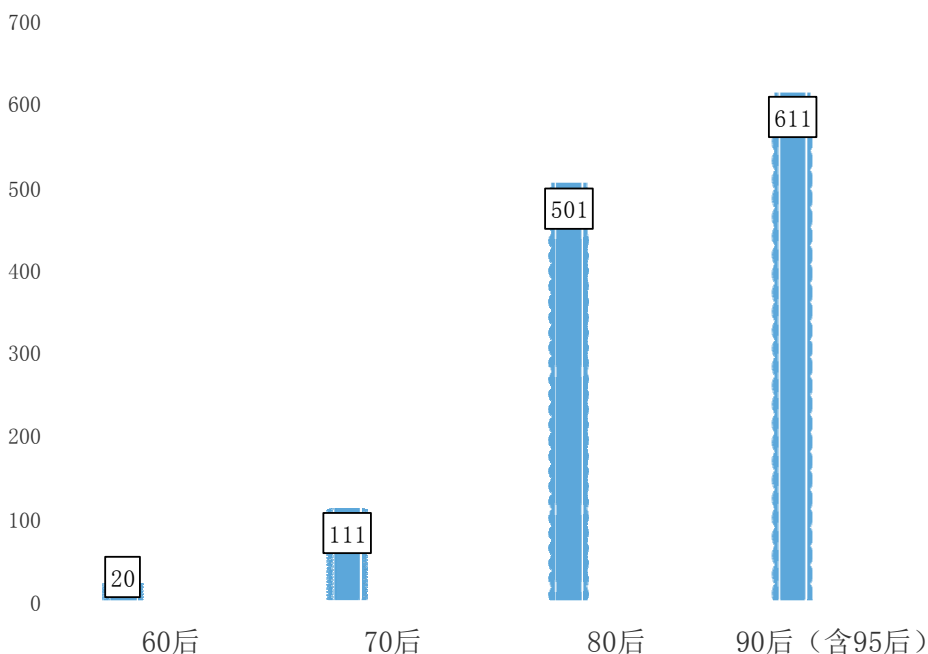


（二）犯罪主体年轻化特征明显

2016年-2018年审结的案件，已判决1277人，其中1980年以后出生的被告人有501人，90后的有611人，90后约占47.85%。其中95后的被告人有183人，在90后的被告人中占据了29.95%。犯罪主体日趋年轻化，被告人30岁以下的人数将近一半。究其原因，一方面年轻人接触网络多，较易掌握网络诈骗的技术，对新兴技术的接受力强，也更易利用新兴技术、社会热点进行诈骗；另

一方面，许多年轻人早早辍学，对诈骗集团的分辨能力较弱，很多时候在诈骗集团招工时他们并不清楚公司性质。目前电信诈骗、集资诈骗等犯罪集团往往披着合法的外衣以某某公司名义招工，因此也提醒年轻人外出打工时，尤其是到境外务工，对公司的基本情况应了解清楚。一旦不慎落入犯罪团伙，应择机报警或通知家人。

被告人年龄阶层分布图



（三）广州法院案件审判质效较好

2016 - 2018 年广州市基层法院审结一审电信网络

诈骗案件 334 件，其中上诉案件数为 91 件，上诉率约为 27.25%。上诉率较低，案件大多在基层法院解决。2016 - 2018 年，广州中院二审审结电信网络诈骗案件 91 件 532 人，维持 87 件，发改 4 件，发改率较低。

（四）纠纷类型多样，案件审理难度较大

电信网络诈骗案件情况复杂，目前随着科技的发展，案件类型更加多样化。电信网络诈骗高科技化日趋凸显。例如，犯罪分子利用改号显号软件、伪基站等设备，冒充银行、电信、移动客服号码广泛发送信用卡消费、网银升级、电子密保过期、积分兑换等虚假诈骗信息，诱骗被害人按其方法操作或收取费用，或通过外挂软件等诈骗被害人财物，达到诈骗目的。技术事实认定、数额认定、共同犯罪人员的地位和涉案金额认定等都是审判中常遇到的难题。因此，新型疑难复杂案件不断涌现、犯罪分子众多且诈骗手段日益高科技化，都给审判工作带来不少压力。

二、电信网络诈骗犯罪案件产生的原因

（一）大量个人信息遭泄露、甚至被买卖，成为犯罪分子筛选潜在行骗对象的重要手段

在日常生活、工作中，人们经常需要填写各种个人资料，由于缺乏相应的保护和保密措施，这些个人信息很容易被不法分子收集并利用。诈骗犯罪分子正是通过各种非法途径，轻易掌握大量潜在被害人的手机号码、家属资料，甚至身份证号码等重要个人信息用于行骗。

（二）移动通信网络的防护存在安全隐患，缺乏对电信企业和银行的有效监管

因移动或者联通的 GSM 网络设计存在漏洞，老式的 SIM 卡并没有验证呼叫方是否合法，也无法验证 SMS 短信发送方是否来自真实的手机。伪基站流动性强，成本低，几千元即可从网上购得伪基站需要的所有设备，且使用随意方便，例如背着在街上、汽车上或放在某个地方均可使用，这也是伪基站快速地被犯罪分子利用的原因。目前一些电信企业和银行对客户信息数据库保护不善，防数据盗窃机制不健全，从而为犯罪分子获得客户信息并实施诈骗提供可乘之机。

（三）犯罪分子依靠技术手段，具有较强的反侦查能力

犯罪分子一般采取远程、非接触式诈骗，利用网络

电话批量自动群拨电话、群发手机短信；一旦收到被害人转账的款项后就迅速将赃款分流，分不同组跨省区域、跨银行转账至另外数十个银行账户，难以查控；而且诈骗团伙分工明确，不同组之间不知道对方的情况，侦查机关难以将其一网打尽。

（四）被害人因自身贪念、心理承受能力差、识别能力差等弱点，易陷入犯罪分子精心设计好的圈套

电信网络诈骗伪装性高、形式层出不穷，在完全没有心理防范意识的情况下非常难以识别。随着诈骗技术不断升级换代，防诈骗提醒往往滞后，令人防不胜防，尤其是老年人，常常难以识破骗术，沦为诈骗团伙的目标人群。诈骗团伙往往会根据不同被害人群的不同弱点“量身定做”骗术，而被害人在遇事时往往缺乏冷静思考分析，在未及时寻求他人帮助之前就盲目听从犯罪分子的“安排”。

三、电信网络诈骗犯罪案件审判工作的主要做法

（一）重视电信网络诈骗案件审判工作

广州中院高度重视电信网络诈骗专项整治工作，始终将电信网络诈骗案件的审判作为刑事审判的一项重要

工作来抓。一是指派业务精湛、经验丰富的法官成立专门的合议庭审理电信网络诈骗案件。二是加强业务培训和指导。三年来，广州中院严格按照相关工作制度要求，指导基层法院顺利开庭审理多件电信网络诈骗案件，如花都法院审理的陈某某等 17 人诈骗案、林某某等 12 人诈骗案、黄埔法院审理的崔某某等 22 人诈骗案、海珠法院审理的曾某某等 36 人诈骗案等。三是作为市打击治理电信网络新型违法犯罪工作联席会议成员单位，广州中院认真履行职责，将刑二庭设为联络部门，保质高效完成联席会议的各项工作部署。

（二）扎实做好电信网络诈骗案件的审理工作，提高审判质效

一是严把“三关”，提高案件审判效率。全面落实刑法、刑事诉讼法的规定，严把证据关、程序关和法律适用关，确保电信网络诈骗案件审判工作依法进行。强调依法快审快判，强化高效办案意识，要求每一宗案件在查清案件事实、准确定罪量刑的前提下尽量缩短案件审理时间，提高审判效率。二是严格贯彻宽严相济的刑事政策。对电信网络诈骗犯罪团伙的首要分子、骨干、累

犯、惯犯、职业犯等加大刑罚惩处力度，依法从严从重惩处。对于犯罪情节较轻，归案后认罪态度好、主动协助追赃、积极协助抓捕的偶犯、从犯注意教育感化，依法从宽处理。三是加大财产刑的适用力度，突出经济制裁手段。依法加大罚金、没收、追缴违法所得、收缴犯罪工具等财产刑的适用力度，消灭电信网络诈骗犯罪分子“重操旧业”的物质条件，对社会上企图再犯或正在实施此类犯罪的人员起到有力的震慑作用，使其不敢犯、不再犯。

（三）加强协调配合，建立多部门联动、跨区域协作机制，形成打击合力

电信网络诈骗犯罪组织严密、分工明确、跨地区作案、赃款转移便利等特点，需要多个部门的协作。广州中院充分利用全市打击电信网络诈骗工作联席会议这一平台，切实加强公安、检察、金融、电信等职能部门协作配合，实现审判工作与侦查、公诉、执行等工作的有效衔接。一是通过审判职能延伸，与侦查机关、公诉机关交流办案经验，制定证据搜集、证据指引等工作流程，共同提升电信网络诈骗案件的侦查、起诉质量。二

是健全案件信息沟通机制，加强协调配合，及时补查证据、交换意见，确保准确认定事实、正确定罪量刑，将相关案件办成经得起考验的铁案。三是加大赃款赃物追缴力度，协助相关部门执行、处理案件中赃物及扣划赃款等工作，最大限度确保判决得到有效执行。推动建设跨区域司法协作机制，对跨地域、涉及被害人分布广的电信网络诈骗案件，加强与周边地区公、检、法等机关的沟通和协作，进一步健全案件协调机制，确保犯罪分子被及时惩处。四是协调配合，达成共识。为确保两高一部《关于办理电信网络诈骗等刑事案件适用法律若干问题的意见》的准确适用和加强对基层法院的指导，我市公、检、法机关就案件管辖问题、犯罪团伙认定等问题达成一致意见并形成工作座谈会纪要，达成共识。

（四）加大宣传力度，提高公众防范电信网络诈骗的意识

加强对电信网络诈骗犯罪的法治宣传工作，发挥法治宣传的互动性和实效性，通过法院公众媒体平台、庭审直播等方式适时向社会通报具有重大影响的典型案例，通过剖析电信网络诈骗犯罪的手法、特点，提出有

针对性、实用性的防范措施，提高广大群众对电信网络诈骗的防范意识和防范能力。定期组织全市两级法院对电信网络诈骗犯罪案件进行集中宣判，形成打击电信网络诈骗犯罪的高压态势，有效震慑犯罪分子，确保电信网络诈骗案件审判工作实现政治效果、法律效果和社会效果的统一，切实维护广大人民群众合法权益。

四、防范电信网络诈骗犯罪的对策及建议

（一）妥善保管个人信息

当前社会环境下，个人信息的泄露、贩卖等现象突出，已成为诈骗犯罪黑色产业链的重要组成部分。由于许多电信网络诈骗方式都以获取被害人隐私信息为先决条件和必经步骤，因此，广大人民群众把好个人信息保护的第一道关口，从源头杜绝隐私外泄对于避免财产损失至关重要。一方面，要保护好个人身份信息。在非必要情况下，不向陌生人提供身份证号码、工作单位、家庭住址、职务等重要信息。不将身份证照片或号码保存在手机中。另一方面，要保管好个人账户信息。在相关网站输入账号、手机号码、查询支付密码等重要信息前要谨慎核实域名真实性，不点击可疑链接，不连接来历

不明的无线网络，不扫描非正规渠道获取的二维码，谨防钓鱼陷阱。

（二）加强账户安全管理

一些电信网络诈骗案件反映出部分群众银行账户管理存在明显漏洞，因此，提高银行账户安全性，给自己的账户上好“锁”，是风险防范的关键一环。例如，为银行卡、网上银行、手机银行设置复杂性较高的密码；不在任何网站上设置与网上银行、手机银行等相同的用户名和密码；不向任何人透露或转发短信验证码及其他形式的动态密码。此外，为防范电信网络诈骗，人民银行、银监会等金融监管机构近期印发了一系列文件，要求同一个人在同一家银行只能开立一个Ⅰ类户，开立多个Ⅰ类户的，需进行清理；暂停涉案账户开户人名下所有账户的业务，经公安机关认定的用于开展电信网络新型违法犯罪的涉案账户，要中止业务往来等。上述规定从银行支付端设置防线，群众应积极配合银行执行相关规定，保障自身财产安全权益免受侵害。

（三）提高金融安全意识

被害人金融知识不足或风险意识薄弱是多数电信网

络诈骗最终得逞的直接原因，因此，提高对金融产品和服务的认知能力及自我保护能力，是群众防骗避损的核心应对之策。特别是近年来电信网络诈骗的受害人群更加广泛，逐渐从老年人、受教育程度较低群体向中青年、高学历、高收入人士蔓延，加强金融知识学习已成为每一位群众的必修课。例如，群众应密切关注媒体报道和网络曝光的诈骗案件，全面了解近期出现的作案手法，并提醒家人朋友提高警惕。对电信运营商通过短信推送的安全提示信息，以及公安机关通过网站、公众号不定期发布的风险防范要点，应认真研读并牢记。另外，银行利用各渠道开展的金融知识宣教活动系统性、针对性强，对资金安全保护大有裨益，群众应当予以关注。

（四）培养良好支付习惯

电信网络诈骗尽管无孔不入且真假难辨，但只要群众时刻保持警惕，养成良好支付习惯，把控住对外转账汇款的最后一道关口，仍可有效避免资金损失。例如，接到熟人通过短信、微信、微博、QQ、邮件、语音等形式发送的转账请求，或询问银行卡、网银密码等重要信息时，要通过电话核实确认；陌生人或长期失联的“熟

人”要求汇款时，须保持谨慎多方求证，遇到可疑情况及时向公安机关、银行、电信运营商等机构咨询；如确需向对方转账，应尽量选择次日到账方式并于事后再次核实，如有异常及时申请撤销；具有移动支付习惯的消费者应选择安全性较高的支付产品，并下载安装正版应用软件；避免在与移动支付软件绑定的银行卡中存放过多资金，以便分散和锁定风险。

结 语

预防和治理电信网络诈骗犯罪是一项系统工程，是全社会的共同责任。广州法院将始终全面贯彻党的十九大精神和习近平新时代中国特色社会主义思想，对照“四个走在全国前列”的目标要求，积极适应经济发展新常态，进一步健全审判工作机制，坚决有效遏制电信网络诈骗犯罪活动，为粤港澳大湾区建设提供优质司法服务、优化法治营商环境，为促进社会和谐稳定、维护人民群众财产安全和其他合法权益提供强有力的司法保障！

〔广州法院电信网络诈骗犯罪审判十大典型案例〕

案例一

崔某某等 22 人电信网络诈骗案

【基本案情】

2016 年 6 月中旬起，台湾地区男子“达哥”（另案处理）先后纠集被告人迟某某等组成电信诈骗犯罪集团，在亚美尼亚共和国（以下简称亚美尼亚）首都埃里温市设立诈骗窝点，对大陆居民实施电信诈骗活动。其中，2016 年 7 月 13 日，被告人崔某某、赖某某、陈某某、范某某、许某某前往亚美尼亚诈骗窝点。该犯罪集团组织严密、分工明确、公司化运作。在诈骗形式上，该犯罪集团首先由一线成员冒充被害人所在地中国移动公司客服人员或通讯监管局工作人员，拨打被害人电话（或是向被害人发送事先制作的语音包，待被害人回拨后，由一线人员接听），谎称被害人个人信息泄露、被他人利用从事洗钱或诈骗等违法犯罪活动，建议报警处理；二

线成员则假扮大陆公安人员接受被害人报警，制作电话报警笔录，并称被害人涉嫌洗钱或诈骗犯罪，若要洗脱嫌疑，需转由检察官处理（部分案件中二线人员取得被害人信任后，直接套取被害人的银行资金情况，要求对被害人进行资金清查以排除作案嫌疑，诱使被害人转账或汇款至所谓的“安全账户”）；三线成员则假扮处理案件的检察官等对被害人继续实施诈骗，要求被害人将资金转至“安全账户”进行资金清查。待被害人将资金转账或汇款至“安全账户”后，上述被告人则迅速通知相关人员取款或转账，将被害人资金占为己有。2016年7月至8月19日期间，该犯罪集团成功实施诈骗19宗，共骗得人民币1244416元。

【裁判结果】

一审以诈骗罪判处被告人崔某某有期徒刑十一年，并处罚金人民币十二万元；以诈骗罪判处其余被告人有期徒刑三年至十年六个月不等，并处罚金人民币一万元至十万元不等。一审宣判后，崔某某等人提出上诉。二审经审理后，驳回上诉，维持原判。

案例二

王某、林某某等 17 人电信网络诈骗案

【基本案情】

2013 年起，同案人瞿某某为了谋取非法利益，成立广州更美商贸科技公司，先后聘用被告人林某某、王某担任公司总经理，被告人瞿某某担任负责人事、行政、采购和监听等后勤部门的主管、同案人徐某担任财务部门主管、覃某某担任话务部门主管、被告人周某某及同案人伍某某担任回访部主管。利用广播电视、互联网等媒体投放广告，在全国范围内吸引客户，待取得被害人联系方式等资料后，通过话务部人员以电话营销的方式与之联系，向其推销声称具有丰胸、增高、壮阳等功效的产品并进行一次销售，在获取被害人身体状况等详细信息后又通过回访部人员进行二次销售，引诱被害人对自身的身体状况和产品功效陷入错误的认识，从而一步步购买没有相应宣传效果的产品。经统计共骗取 927 名被害人货款人民币 8493940 元，且上述损失均无法追回。

【裁判结果】

一审以诈骗罪判处被告人王某有期徒刑十一年六个月，并处罚金人民币十万元；以诈骗罪判处被告人林某某有期徒刑十二年六个月，并处罚金人民币十五万元；以诈骗罪判处其余被告人缓刑至有期徒刑六年不等，并处罚金人民币五千元至五万元不等。一审宣判后，王某等人提出上诉。二审经审理后，驳回上诉，维持原判。

案例三

梁某等人电信网络诈骗案

【基本案情】

2015年2月至2015年5月，被告人梁某、邵某某、林某某、江某某、蔡某某伙同同案人邵某彬、“光进”（另案处理）先后参与上家梁某某、“西狗”、“阿虎”（均另案处理）等同案人组织的“以猜猜我是谁”为主要诈骗方式的电信诈骗集团。由该集团内的同案人（均另案处理）在全国各地假冒被害人的亲戚、同学、同事、朋友、领导等骗取被害人的信任，再以嫖娼、醉酒被公安机关抓获需要保证金或急需用钱、送礼等名义，骗得被害人将财物存入指定银行账户，再通知上述被告人取款，上述被告人接到通知后组成若干提款小组负责持银行卡在海南省、广东省等地银行ATM机取款，并从提取款项中提成5%，在组内平分提成，余款交给上家。被告人梁某实施诈骗94宗，诈骗财物共计人民币2738800元；其他被告人诈骗财物共计人民币83000元至2703000元不等。

【裁判结果】

一审以诈骗罪判处被告人梁某有期徒刑十三年，并处罚金人民币三十万元。以诈骗罪判处其余被告人有期徒刑一年十个月至十二年不等，并处罚金人民币五千元至二十五万元不等。一审宣判后，梁某等被告人提出上诉。二审经审理后，驳回上诉，维持原判。

案例四

李某桂、李某景电信网络诈骗案

【基本案情】

2016年1月至2017年3月，被告人李某桂、李某（另案处理）组织被告人李某景及同案人王某某、叶某某、刘某某、陈某某、谭某、张某某、严某某、黄某某、李某厅（均另案处理）等人，通过网上发布中奖低价购买正版苹果手机的虚假广告，骗取被害人点击进入填写个人信息，再电话联系被害人下单订购，将从网上低价购得的假冒苹果手机通过顺丰速运发货，以货到付款方式骗取被害人支付货款。被告人先后共骗取60名被害人共计人民币111109元。

【裁判结果】

一审以诈骗罪判处被告人李某桂有期徒刑三年，并处罚金人民币一万元。以诈骗罪判处被告人李某景有期徒刑一年六个月，并处罚金人民币三千元。一审宣判后，被告人均未上诉，判决已生效。

案例五

刘某某电信网络诈骗案

【基本案情】

2016年1月至3月期间，被告人刘某某为牟取非法利益，指使下线同案人林某某、肖某某、李某某（均另案处理）携带伪基站设备，驾驶车辆去到广西壮族自治区、广东省，利用伪基站发送诈骗短信，通过诈骗短信骗取被害人信任后，再由其他同案人相互配合诱导被害人到银行柜员机转账到被告人上线指定的账户中。被告人刘某某伙同同案人林某某、肖某某、李某某共同发送诈骗短信约177万条，其中骗得27名被害人共计799558元。

【裁判结果】

一审以诈骗罪判处被告人刘某某有期徒刑十年三个月，并处罚金20000元。一审宣判后，刘某某提出上诉。二审经审理后，驳回上诉，维持原判。

案例六

邹某某电信网络诈骗案

【基本案情】

被告人邹某某自 2013 年起，在婚恋网站百合网上虚构姓名、家庭、婚姻、工作等身份信息，以婚恋为名与多名被害人交往，骗取被害人的信任，再利用借钱办事、话费充值等理由骗取被害人钱财。先后共骗得多名被害人人民币 28211.83 元。

【裁判结果】

一审以诈骗罪判处被告人邹某某有期徒刑一年二个月，并处罚金人民币八千元。一审宣判后，邹某某提出上诉后又撤回上诉，二审裁定准予撤诉，目前案件已生效。

案例七

王某某电信网络诈骗案

【基本案情】

2017年2月至5月，被告人王某某在微信等网络平台上以网络“刷单”购物返还货款并获取提成为幌子吸引被害人，先让被害人支付“入会费”“培训费”等费用，完成额度较小的“刷单”购物并及时返还全部货款和少量提成，取得被害人的信任，进而诱骗被害人进行更高额度的“刷单”购物，在被害人支付相应货款之后，即拉黑被害人的微信拒不返还货款。被告人王某某通过上述方法，共骗取多名被害人“入会费”“培训费”以及货款等共计人民币122839元。

【裁判结果】

一审以诈骗罪判处被告人王某某有期徒刑三年，并处罚金人民币五千元。一审宣判后，被告人未上诉，判决已生效。

案例八

李某某等 5 人电信网络诈骗案

【基本案情】

2016 年 8 月始，被告人李某某以其租住的广东省中山市沙溪大道 6 号时代倾城 xx 栋 xx 房为窝点，纠合被告人李某东、李某华、张某某、李某洋实施电信诈骗。被告人李某某等先从互联网上购买大量考生信息，然后在互联网上找人群发能出售“会计职称考试”“职业医师考试”“社会工作者资格考试”的试题答案、能修改考试分数等信息。当有被害人信以为真时，被告人使用 QQ 与被害人进行联系，便以收取保密费、保证金等名义逐步骗取被害人款项。2016 年 8 月至 2017 年 6 月期间，先后骗得 27 名被害人共 97160 元。

【裁判结果】

一审以诈骗罪判处被告人李某某有期徒刑三年三个月，并处罚金人民币二万元；以诈骗罪判处其余被告人

有期徒刑十个月至一年九个月不等，并处罚金人民币三千元至五千元不等。一审宣判后，被告人均未上诉，判决已生效。

案例九

黄某某等 7 人电信网络诈骗案

【基本案情】

2017 年 6 月间，被告人黄某某先后纠集被告人谢某某、廖某 1、覃某某、廖某祥、廖某华、廖某 2 等人，预谋进行电信网络诈骗活动，由被告人谢某某提供广东省东莞市石龙镇清华街 xx 号 x 楼住所，被告人黄某某提供笔记本电脑、手机等工具。各被告人通过互联网发送带有木马病毒的信息链接盗取他人 QQ 账号及密码后，再从被盗 QQ 号的好友中物色诈骗对象，随后冒充 QQ 号主人向诈骗对象谎称有物品从国内托运到国外，但无法在国外转账到物流公司等，让被害人通过转账代为支付物流费用。得手后由同案人提取或转入其他账户，总共诈骗被害人 25650 元人民币。

【裁判结果】

一审以诈骗罪判处被告人黄某某有期徒刑一年二个

月，并处罚金人民币一万元。以诈骗罪判处其他被告人有期徒刑九个月至一年不等，并处罚金人民币五千元至一万元不等。一审宣判后，被告人未上诉，判决已生效。

案例十

林某某电信网络诈骗案

【基本案情】

2017年1月至2018年1月，同案人邱某某伙同其女友被告人林某某与其哥哥邱某源、妹妹邱某琳（均另案处理）等人共同研究、互相协助作案，通过非法获取的虚拟的手机号码、验证码等信息，在滴滴出行平台上恶意注册大量账户，并在网络上以低价推广和招揽叫车业务，待需要用车的乘客向其提出用车需求后，即使用其恶意注册的滴滴账户呼叫快车，提供给乘客搭乘，并收取乘客数额二十元不等的费用，但在司机服务结束后却不支付任何费用，导致提供用车服务的被害单位滴滴出行科技有限公司无法收取车费。通过上述方式，被告人林某某帮助同案人邱某某先后通过554个订单骗取滴滴出行科技有限公司车费共计人民币71995.37元，另外其独立接单，通过同案人邱某某骗取滴滴出行科技有限公司广东分公司车费共计人民币869.66元。

【裁判结果】

一审以诈骗罪的从犯判处被告人林某某犯诈骗罪，判处有期徒刑十个月，并处罚金人民币二千元。一审宣判后，被告人未上诉，判决已生效。