
公安机关查获的犯罪团伙作案工具，通讯员供图

专项行动打掉“两卡”团伙42个
今年以来共抓获涉“两卡”人员1559名

宁波公安“断卡”行动成效显著

10月10日，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召开全国“断卡”行动部署会，在全国范围部署开展“断卡行动”。行动开展以来，宁波公安组织精干警力辗转多省循线追捕，成功打掉“两卡”团伙42个，采取强制措施485人，查获个人银行卡1541张、手机卡3398张，“断卡”行动成效显著。今年以来，全市公安机关共抓获涉“两卡”人员1559名，对375名买卖、转租、转借银行卡、电话卡人员开展惩戒。

行动开展初期，在市联席办的牵头下，通过抽调反诈、网安等警种精干力量，市公安局刑侦支队第一时间组建“断卡”行动研判打击专班，围绕涉案“两卡”线索做好梳理分析，经过集中研判转变成有效信息后，为各地组织开展落地打击提供精准的科技、信息支撑。同时，市联席办充分发挥协调沟通优势，会同市场监督管理局、人民银行宁波中心支行等职能部门，联合三大通信运营商等单位，以“地毯式”摸排行动为契机，联合推进打击整治工作，确保各项“断卡”措施落地到位。

“行动初期我们就梳理出全市1月–9月本地开户涉案银行卡1423个，关联对象624名，研判梳理出416名涉‘两卡’人员。”专班成员汤涛介绍说，“公安继续落地跟进调查，逐项研判、逐条见底、逐人锁定。运营商则对已开办的号码进行封停，并将相关身份同步给其他运营商，列入高危人员名单，各项工作同步开展。”

据了解，此次“断卡”行动期间，宁波公安按照“以打开路、以打促治、以打促防”的工作思路，对全部“两卡”线索一律做到逐项研判、逐条见底、逐人锁定，对一切相关的违法犯罪人员一号一档、一人一档，逐条做好核查研判，通过精准打击、溯源打击、集群打击，切实形成强大震慑力，让违法犯罪分子不敢开、不敢收、不敢贩。

截至目前，全市公安机关共打击涉“两卡”团伙42个，抓获涉“两卡”人员1559人，查获对公账户157个。

“下步，我们将继续组织高频度、多轮次、大规模的集中打击整治行动，不断掀起打击高潮，全力斩断‘两卡’开办贩卖产业链，彰显宁波公安机关坚决打击整治涉‘两卡’违法犯罪活动的态度和决心。”市公安局刑侦支队副支队长尚剑波说。

宁波公安提醒，此次“断卡”行动没有期限，全市公安机关将始终保持高压态势，依法严厉打击开办贩卖电话卡、银行卡违法犯罪。广大市民群众一定要妥善保管好自己的身份证件、银行卡、手机卡，一旦丢失要立即挂失。买卖、出借对公账户以及银行卡、电话卡等是违法行为，甚至还可能涉嫌犯罪。


抓捕现场。通讯员供图

●典型案例

案例一：2020年10月13日，受害人郑某微信收到好友请求，对方自称是镇海区区领导，以受疫情影响、家中亲戚公司急需资金周转为由向郑某借钱转账15万元。当时未有多想的郑某“慷慨解囊”，却不知掉进诈骗的“大坑”。

镇海公安分局在接到郑某报案后，迅速展开侦查，通过对嫌疑人微信号的分析抓住诈骗团伙的“尾巴”，后又顺藤摸瓜，赶赴湖北荆州，终于抓获以杨某为首的犯罪团伙。

该团伙通过非法获取手机号码，批量注册并贩卖微信号，为诈骗团伙提供作案微信账号，并有固定群成员替其辅助验证登入。理清团伙的上、下家信息后，专案组再次兵分多路，抓获犯罪嫌疑人王某等3人，成功打击此“黑灰产业链”。

案例二：2020年11月12日，犯罪嫌疑人高某被江北警方抓获。经审讯，高某交代其贩卖公司及对公账户并介绍他人贩卖从中获利的犯罪事实。通过高某的指认，警方发现其背后还有更大的“阴谋”。

原来，早在2018年，陈某伙同另外3人利用放贷广告吸引高某等借贷人，一步步骗取信任，然后让高某等人去各地注册公司获取营业执照等证件，陈某再将其证件贩卖“上家”谋取钱财。获得这一重大线索后，江北公安分局经侦大队利用大数据追踪技术，将以陈某为首的犯罪团伙连根拔起。

●阅读延伸：

“断卡”断的是什么“卡”？

手机卡：包括平时所用的三大运营商的手机卡、虚拟运营商的电话卡和物联网卡。

银行卡：包括个人银行卡、对公账户、结算卡、非银行支付机构账户（即我们平时所说的微信、支付宝等第三方支付）。

相关惩戒措施

宁波市公安机关对于涉嫌开办贩卖“两卡”者展开惩戒措施：记录到个人征信报告；不得为其新开立账户，其中包括银行开户及其他金融机构开户；对出租、出借或者出售电话卡的执行失信惩戒；5年内暂停在银行账户非柜面业务、支付账户所有的业务。

记者 张贻富
实习生 陈露颖 通讯员 王西泽

警惕！
冒充公检法 老套路有新花样

年关将近，又到了诈骗案件高发时段，冒充公检法的诈骗大有卷土重来之势。近期，市反诈中心连续接到多起冒充宁波市公安局进行诈骗的警情，案件损失金额较大，日常回访劝阻工作中也发现不少群众有接到过冒充宁波市公安局进行诈骗的电话。

11月30日，宁海的夏女士接到一个电话，对方自称是“宁波公安局民警”，以夏女士涉嫌一起非法集资案件为由，要求夏女士配合调查，并将电话转接到“长沙市公安局”。电话那头自称“长沙市公安局周警官”，与夏女士核对身份信息后，让夏女士配合加QQ好友。因对方能准确报出自己的基本信息，夏女士不疑有他，便添加了对方为QQ好友。

很快，“周警官”通过QQ发来自己的警官证照片，这让夏女士对其身份更加深信不疑。之后，对方称要审查夏女士有无参与非法集资，并要求夏女士共享QQ屏幕，以方便其协助指导操作。夏女士打开共享，并在对方的指导下获取支付宝网商贷贷款额度，再将支付宝余额及网商贷贷款额度共计1.5万余元，全部提现至支付宝绑定的银行卡。后夏女士收到银行验证码短信及扣款短信，再联系“周警官”时，发现QQ已被对方拉黑，这才意识到被骗了。

市反诈中心分析发现，最近几起冒充公检法诈骗案件中，QQ屏幕共享正在成为诈骗分子的常用手段，QQ屏幕共享可以将手机显示页面原封不动地共享给对方，而手机用户大都会设置自动弹出短信的功能，“短信验证码”自然也暴露给了诈骗分子。上述案件中，夏女士正是因为屏幕共享导致验证码泄露。

此外，部分诈骗分子还会要求受害人下载“安全防护”APP，这款APP自带拦截电话功能，目的与之前惯用的呼叫转移等手段一致，即让外界无法及时联系受害人。

市反诈中心提醒广大市民，无论诈骗分子手段如何更迭，只要记住公检法机关不会通过电话、网络通知涉案人核查资金，也不会通过QQ、微信等社交软件发送展示个人工作证、相关法律文书、制作笔录，更不存在所谓的安全账户。

记者 张贻富
通讯员 夏怡雯 周国亮