【反诈拒赌 支付在行动】典型电信网络诈骗案例类型及防范提示

为深入学习贯彻习近平总书记关于打击治理电信网络诈骗犯罪的重要指示精神，落实党中央、国务院重大决策部署及人民银行有关工作要求，切实提高人民群众防范电信网络诈骗意识，助力建设更高水平的平安中国，中国支付清算协会坚持“为人民群众办实事”的宗旨，汇总国家反诈中心、会员单位、互联网络等发布的相关素材，梳理具有典型风险特征和启发意义的电信网络诈骗案例类型，向社会公众提供和宣教,，引导普通老百姓正确认知和防范欺诈风险，牢牢守护人民群众的钱袋子安全。

案例 1：新冠特效药诈骗

刘爷爷接到陌生电话，对方自称是当地防控中心的工作人员，声称刘爷爷的健康码和检测报告有异常，可能感染新冠肺炎，不过还在潜伏期，情况不算太严重。对方说现有一款特效药，5000 元三个疗程，每天坚持服用就会恢复健康。刘爷爷非常害怕，立马向对方提供的账号转账，然而迟迟没有收到接受治疗的通知，这时刘爷爷才反应过来自己被骗了。

风险提示：防疫工作人员不会直接推销产品、擅自收取费用，不要轻信陌生电话！

案例 2：领取“防疫补贴”诈骗

康爷爷居家隔离期间，收到短信称“接社保部门通知，

国家将发放补贴，请收到邮件的居民自助办理，认真填写以免补贴不能准时入账。”随短信附有一个二维码链接，提示扫码自助办理。康爷爷扫码进入网页，输入银行卡号、姓名以及收到的手机短信验证码。随后康爷爷收到银行扣款短信13万元。康爷爷连忙打电话给社区进行核实，被告知不存在这种补贴，这才意识到自己被骗了。

风险提示：收到类似“疫情补贴领取、办理”等消息时，应通过官方渠道进行核实确认。

案例3：冒充流调工作人员诈骗

李奶奶接到自称流调电话，询问是否去过某超市，时空重合人员需隔离。李奶奶表示没去过，于是对方称李奶奶的健康码可能被盗用，据“调查”李奶奶不仅去过，还参与超市内办银行卡领鸡蛋活动，目前该银行卡涉嫌诈骗，并发来包含李奶奶详细身份信息的执行文书，李奶奶慌了神。对方表示，李奶奶需缴纳保证金到指定“安全账户”，待调查完资金流水，再将钱返还。李奶奶按对方要求转账10万元，但再次联系时已经被对方拉黑，这才察觉被骗。

风险提示：流调工作人员和公安机关不会以任何理由让流调对象转账和进行所谓的“资金核查”，更不存在所谓的“安全账户”！

案例4：刷单返利诈骗

邹奶奶退休后想找个轻松的兼职赚外快，经过网络查询，找到刷单兼职招聘。起初，她尝试支付1.9元，马上得到4.9元返现。看到资金入账后，邹奶奶放松警惕，根据招聘方指

示下载指定App，先小额刷单返现，后来金额越来越大，返现却没有了。邹奶奶想退出，要求对方退款，结果又被对方以验证账户安全等各种理由骗取7万余元。醒悟后，邹奶奶报警。

风险提示：骗子以兼职刷单的名义，先以小额返利为诱饵，诱骗投入大量资金后，再拉黑。切记，千万不要被蝇头小利迷惑，千万不要为刷单交纳任何保证金和押金。

案例5：冒充“公检法”诈骗

薛爷爷接到一个自称民警的陌生电话，对方告知薛爷爷涉嫌某洗钱案，要求他添加QQ号。添加好友后，对方发来警官证和含薛爷爷身份信息的刑事拘捕令，并要求薛爷爷找个安静的地方接受远程调查，不能挂断通话。随后对方声称需要验证经济能力、信用能力证明其无罪，让其在网络平台及银行贷款后汇款到某账号上，称结案后会退回。薛爷爷向对方提供的账号转账62万元人民币，之后才发现被骗并报警。

风险提示：公检法机关会当面向涉案人出示证件或法律文书，不会提出远程转账汇款或验证经济能力等要求。

案例6：虚假投资理财诈骗

老张的社交账号收到陌生好友申请，添加后对方向其推荐股票交流群。老张入群后，看到群友“收益”颇丰，便心动了。在群内客服引导下，老张安装“理财软件”并充值6万元，一周内盈利7800元并提现。看到“赚钱”这般容易，老张将全部积蓄100万元投入充值。但很快，老张发现账户

已经无法登陆。此时，老张才意识到被骗了。

风险提示：投资理财，请选择银行、证券公司等正规途径！切勿盲目相信所谓的“炒股专家”和“投资导师”。

案例 7：充值折扣诈骗

小李的社交账号收到陌生好友申请，对方称提供手机充值服务，实付 80 元即可获得价值 100 元的充值卡。小李先试着支付 80 元，第二天充值金额就到账。见如此，小李便想赚笔大的，一次性转账 5 千元，可是第二天他查询手机卡余额发现并没有金额到账，对方账号也把他拉黑，这才意识到被骗了。

风险提示：陌生人添加社交账号好友，一定要确认好对方的真实身份。当对方谈到钱财时，要提高防范意识，莫贪小便宜。

案例 8：虚假票务诈骗

赶上寒暑假小张都会出去旅游，正因是临近旺季，这次小张未订到心仪的机票，最后通过搜索引擎找到一个小网站，上面的机票价格低廉但库存紧张。小张赶忙预订，但付款成功后，页面显示“出票失败”，并建议购买更高等级舱位。小张见其建议售价仍低于市场价，便再次付款。但依然显示“出票失败”。这时小张察觉到不对，想要退款，却发现没有退款通道，这才意识到自己被骗。

风险提示：请务必通过正规渠道购买车（机）票，不要轻易点击、扫描任何来历不明的网址链接、二维码，防止手机中毒，银行账户被盗！

案例 9：“杀猪盘”诈骗

小李在社交软件上认识一名自称在国外做军医的人，经过一段时间聊天接触，两人感情逐渐升温。某日，“国外军医”声称获得 100 万美元任务津贴，放在他那里不安全，要快递给小李，小李答应了。随后“国外军医”开始以运费、保险费、被海关扣留等各种理由向小李索要了超 28 万元。之后，“国外军医”突然失去了联系，此时小李才恍然大悟。

风险提示：素未谋面的网友、网恋对象推荐网上投资理财、炒数字货币（虚拟币）、网购彩票、博彩赚钱或通过各种借口直接索要钱财的要当心，谨防上当受骗！

案例 10：网络贷款诈骗

小徐近期开销大需要一定资金度过难关，想起微信上一个自称能帮忙办理贷款的好友。经联系，该好友称能帮小徐办理贷款，但需先交 30%手续费，后期手续费会连同贷款一起返还。小徐分两笔向对方提供的账号转账共 5000 元，而后对方告知审核未通过，需再缴纳“审核费”，小徐再次转账 6000 元。第二天，对方再次要求转账进行解冻资金，这时，小徐才意识到自己被骗并报警。

风险提示：办理贷款一定要到正规的金融机构。凡是在放款之前，以交纳“手续费、保证金、解冻费”等名义要求转账刷流水、验证还款能力的，都是诈骗。

案例 11：冒充客服诈骗

小蒋接到陌生电话，对方自称是售后客服，称小蒋在平台上购买的商品未达到国家检测标准，现以商品的三倍价格

退还金额到小蒋账户。对方准确说出购买物品及时间，小蒋信以为真。在对方的诱导下，将自己的银行卡号、短信验证码等信息告知对方，直到银行卡内的钱被转完后，小蒋才意识到自己被骗。

风险提示：电商平台退款通常是原路返还购物者的银行账户或支付账户，无需购物者在其他软件中进行操作，更不会要求购物者通过扫码、点击链接、提供银行卡密码、短信验证码等方式进行退款！

案例 12：快递理赔诈骗

经常网购的小王接到自称是快递公司工作人员的电话，被告知自己的快递新冠病毒检测呈阳性，需进行销毁，公司将对王女士进行赔偿。王女士按照指引扫描了对方提供的二维码，将自己的身份证号、银行卡号、短信验证码等一系列信息提供给了对方。随后王女士发现自己账户内的 4 万多元被转走了，这时候才意识到被骗了。

风险提示：网购商品有任何问题，要通过官方 App 或网站进行联系，切勿扫描未知二维码或下载来源不明的软件、APP 等，切勿随意透露个人隐私信息。