



★ 案件背景

随着电信网络诈骗手段的持续迭代翻新，不法分子已将黑手精准伸向保险客户群体。相较于传统的盗刷银行卡诈骗，新型诈骗手段更具迷惑性与隐蔽性。诈骗分子利用消费者对保险业务的信息差，通过“刷单返利”诱饵叠加“屏幕共享”技术，诱导消费者自行操作金融账户，从而窃取保单资金。很多消费者误以为“只要不转账、不泄露银行卡密码就不会被骗”，然而在当下的骗局中，仅凭短信验证码、人脸识别信息，不法分子就能轻易盗用保单现金价值，让消费者在不知不觉中背负重额债务。

1 案件简介

杨女士闲暇时喜欢刷短视频，2025年11月，她被一条“刷播抢单、轻松兼职赚外快”的广告吸引。点击链接后，对方要求杨女士扫描二维码进行“实名认证”。在“做任务赚钱”的诱惑下，杨女士按照界面提示，不仅填写了个人详细资料，还输入了短信验证码、拍摄了人脸影像并上传了身份证照片。完成操作后，杨女士并未收到所谓的“佣金”，反而在第二天接到了反诈中心的预警电话，提示其有境外交易信息。起初杨女士不以为意，甚至误以为是骚扰电话。直到家人察觉异常陪同其前往派出所核实才发现，不法分子利用杨女士泄露的信息，远程操控申请了其名下的线上保单借款。大额资金到账后经过多次中转，最终流入境外账户，追回难度极大，杨女士不仅损失了保障，还需自行承担这笔保单贷款的债务。

2 案例分析

本案是一起典型的“兼职刷单诱导”与“保单贷款盗转”相结合的复合型诈骗，其套路具有极强的针对性：

（一）诈骗套路解析

- 1.广泛撒网，精准钓鱼：**诈骗分子在短视频平台投放“低门槛、高回报”的兼职广告，利用受害人想赚取外快的心理，诱导其上钩。
- 2.窃取生物信息，突破风控防线：**诈骗核心在于诱导受害人进行“实名认证”。杨女士提供的人脸影像、身份证照片、短信验证码，实际上是正在诈骗分子的设备上远程注册登录金融机构的客户服务APP，完成身份核验后，诈骗分子即可操作相关金融业务。
- 3.利用保单价值，移花接木：**诈骗分子通过非法手段现场获取杨女士的保单信息，以其名义申请保单质押贷款。贷款资金到账后，迅速通过多层转账转移至境外，大大增加了警方冻结和追赃的难度。

（二）受害人心理盲区

- 1.贪图小利，缺乏警惕：**轻信“轻松赚钱”的虚假承诺，导致在利益诱惑下主动交出核心隐私信息。
- 2.认知盲区，忽视保单金融属性：**很多消费者不清楚长期保单具有现金价值，且可以通过人脸识别和验证码在线办理贷款，误以为保单只是保障凭证，不会被盗用。
- 3.轻信非官方渠道，忽略预警：**对96110反诈预警电话置若罔闻，甚至误判为诈骗电话，延误了黄金止付时机。

3 风险提示

为切实守护您的财产安全与保单权益，特此提示广大消费者牢记以下“三不、三必”原则：

三不原则：筑牢防线，守住底线

1.不轻信——刷单返利皆骗局

凡是遇到“刷单返利、刷流水、抢单赚佣金”等名义的兼职，均为诈骗。不存在正规、保本、高收益的刷单项目，切勿因小失大，不轻信陌生电话、短信和网络链接中的任何利诱信息。

2.不透露——核心信息严保密

人脸识别、短信验证码、支付密码是个人资金安全的核心防线。无论什么情况下，都不向对方透露自己及家人的身份信息、银行卡、密码、验证码等敏感信息。正规保险公司不会通过非官方渠道索要这些信息，凡是要求“刷脸”、“报验证码”的，一律拒绝。

3.不转账——陌生账户不汇款

决不向陌生人汇款、转账，尤其是涉及到大额资金时，更要谨慎核实对方身份和账户信息。凡是要求将资金转入个人账户，或声称“内部渠道”、“稳赚不赔”的，均为诈骗，坚决不转账。

三必原则：主动防范，及时止损

1.必核实——可疑情况官方确认

如遇自称客服要求关闭服务、自称公检法要求转账、网络交友推荐投资等可疑情形，务必通过金融机构官方客服热线或线下网点核实真伪，或拨打110求助咨询，切勿盲目听从陌生人的话术指引。

2.必警惕——屏幕共享绝不开启

警惕以“协助办理保单贷款”、“修复保单信息”为由，诱导您下载会议软件开启“屏幕共享”或“远程协助”的行为。一旦开启，您的所有操作和手机隐私将直接暴露给诈骗分子，必须保持高度警惕，坚决不开通。

3.必止损——察觉异常立即行动

若察觉手机被异常控制、资金出现不明变动，应立即强制关机或开启飞行模式切断网络，第一时间联系银行冻结账户，并拨打110报警。同时，务必接听96110反诈专线，避免因疏忽导致损失扩大。

4 结语

金融安全无小事，防范诈骗需牢记。面对花样翻新的骗局，广大消费者应时刻绷紧防骗这根弦，切勿轻信“天上掉馅饼”的好事。保护好个人信息，就是守护好您的“钱袋子”和家庭的保险保障。让我们共同筑牢反诈防火墙，让不法分子无机可乘。