

黑产大数据

信贷欺诈虚假流水研究报告



目录

前言	3
一、 虚假流水种类及作恶流程	5
1.1 纸质/PDF 流水	5
1.2 虚假银行 APP 流水	6
1.3 官方银行 APP 虚假流水	10
二、 虚假流水运用场景	13
2.1 房贷场景	13
2.2 车贷场景	13
2.3 企业贷场景	13
2.4 消费贷场景	13
三、 防御思路	16
四、 总结	17

前言

银行流水记录了企业、个人的资金往来明细，反映了主体现金流、经营绩效等重要信息。在我国，银行流水是主体资信的重要证明材料，广泛应用于公私融资、股权投资等业务中。真流水是指通过银行柜台打印出来的流水单。相反，假流水是指通过黑产、中介等渠道虚构出来的流水单。

在信贷场景中，一部分人因资质不符、缺乏条件等问题无法正常申请贷款，只能通过虚假需求、虚假流水等“假数据”来达到借贷融资目的。目前，银行方或贷款机构无法直接对接他行的个人、企业流水信息，需要贷款客户自主提供相关流水信息，完成相应的贷款审核。这就为黑产提供了可乘之机，通过提供定制虚假的个人、企业流水资料，为贷款客户通过贷款审批及获取更高的贷款额度。

以下为银川警方捣毁的车贷诈骗团伙事件，涉及诈骗团伙通过包装假工作、假收入流水给背债人申请车贷：

涉案1370余万元！银川警方捣毁车贷诈骗团伙

极目新闻 2024-09-03 13:28

近期，宁夏银川市贺兰县公安局打掉一个跨广西、甘肃、山东等12省区25市的购车贷款诈骗犯罪团伙，抓获犯罪嫌疑人6名，斩断了含招募、包装、骗贷、购车、销赃多个环节的犯罪全链条，涉案金额达1370余万元。



银川市贺兰县公安局接到银川市贺兰县某汽车销售公司报警称：公司24辆汽车的购车贷款逾期，回访发现购车人申请贷款资料中的家庭住址、工作单位、收入等信息都是虚构的，且购车人没有贷款资质及偿还能力，截至报案时，24辆汽车均已被过户出售，造成损失200余万元。



当下，黑产的造假手法不断更新、不断迭代，也更加真实，虚假流水可能被黑产使用于任何需要核验收入水平来评估还款能力但又未核验或无法核验第三方官方接口数据的贷款产品。

01

虚假流水种类及作恶流程

一、虚假流水种类及作恶流程

虚假流水主要涉及纸质版流水、PDF 流水、高低配手机 APP 流水、银行官方 APP 流水，其中展示方式涉及银行、第三方支付平台等 APP 版本；流水方向涉及打卡工资、收款码、对公账户等交易流水数据。以下为威胁猎人情报研究团队调研发现的一些黑产招募广告信息：

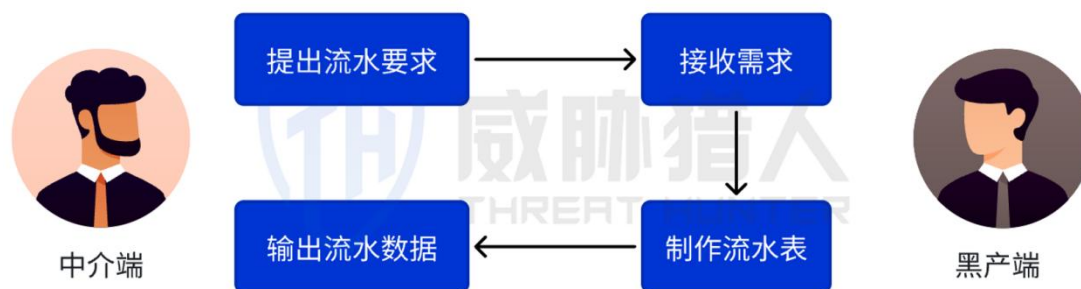
1 纸质流水、PDF流水 2 高低配手机APP流水、企业对公流水 3 微信、支付宝流水 新版个税 4 支付宝和微信公积金、征信包装、刻章 5 结婚证、房产证、驾驶证、营业执照等	主营业务: ●手机银行APP、微信App顶配[礼物] ●个人银行流水,打卡工资流水[庆祝] ●收款码类流水,个税/公积金App[玫瑰] ●房贷按揭流水,车贷按揭流水[發] ●对公账户流水,结清证明[發][烟花] ●微信账单明细、征信报告定制	全网最强辅助工具, 非高仿, 非1:1, 一手官网真实版App ① 转账 ② 导邮箱 ③ 充话费 ④ 充值到weixin, zfb, 粤省事查询, 面签神器, 懂的来。(欢迎 老板围观)
---	--	--

金融黑中介根据客户的资质情况及对应目标贷款产品需求，确定所需的流水种类，与伪造流水黑产专项定制纸质版或 PDF 版或虚假银行 APP 版或银行官方 APP 版流水。且不同的虚假流水种类有不同的价格及操作流程。

1.1 纸质/PDF 流水

纸质/PDF 虚假流水，指的是通过伪造手段制作的、以纸质或 PDF 电子文档形式呈现的银行流水记录。纸质版、PDF 版流水造假成本最低，使用层面也最窄，适用于仅需要客户提供纸质材料或 PDF 版本的贷款场景，或者有银行内部人员内外勾结的场景中，这种纸质/PDF 版流水制作成本较低，价格在 200-300 元左右。

金融中介根据客户情况提出流水制作结果需求，如流水周期长短、账户信息、月收入多少、余额等要求，黑产根据某银行官方流水格式、公章等信息在后台操作流水交易记录表，流水表制作完成后以 PDF 格式输给中介，中介再打印纸质版流水或直接提交 PDF 版流水申请贷款。



一般情况下，制造虚假流水的黑产只提供电子版或 PDF 版本，不提供数据源给中介或客户，类似于一些照相机构只提供照片，不交付底片的模式。金融机构可通过核验 APP 侧数据的方式校验流水的真实性，如：若客户提供打卡工资流水电子版，则可以通过现场核验客户手机银行 APP 的方式，验证数据的真实性。

以下是威胁猎人从黑产侧获取的一份 PDF 企业流水样本：

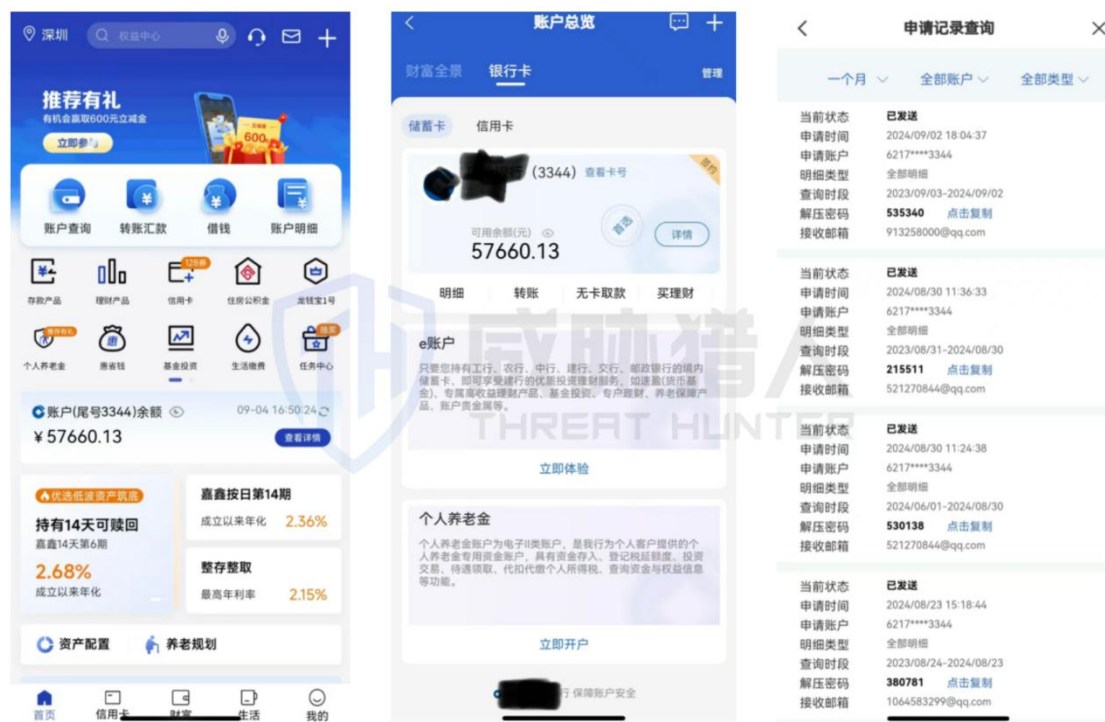
账户明细									
交易时间	收入金额	支出金额	账户余额	交易行名	对方省市	对方账号	对方户名	交易用途	会计日期
20230505 13:37:03	507860.00	0	532474.22	招商银行股份有限公司		57490101	天津滨海新区泰达科技有限公司	货款	20230505
20230505 14:56:21	531800.00	0	1064274.22	中国建设银行股份有限公司		31050000249	天津滨海新区泰达科技有限公司	货款	20230505
20230508 14:19:52	0	248212.86	816061.36	中国邮政储蓄银行股份有限公司		621386547	天津滨海新区泰达科技有限公司	货款	20230508
20230509 10:50:00	433200.00	0	1249261.36	招商银行股份有限公司		31050000249	天津滨海新区泰达科技有限公司	货款	20230509
20230509 11:27:56	0	229600.00	1019661.36	中国邮政储蓄银行股份有限公司		621386547	天津滨海新区泰达科技有限公司	货款	20230509
20230511 12:31:35	0	223700.00	795961.36	中国邮政储蓄银行股份有限公司		621386547	天津滨海新区泰达科技有限公司	货款	20230511
20230512 10:40:42	200034.36	0	995995.72	招商银行股份有限公司		31050000249	天津滨海新区泰达科技有限公司	货款	20230512
20230512 10:44:21	0	209700.00	786295.72	中国农业银行股份有限公司		622918476	天津滨海新区泰达科技有限公司	货款	20230512
20230515 13:34:45	0	265500.00	520795.72	中国农业银行股份有限公司		622918476	天津滨海新区泰达科技有限公司	货款	20230515
20230516 09:41:20	0	232900.00	287895.72	中国邮政储蓄银行股份有限公司		621386547	天津滨海新区泰达科技有限公司	货款	20230516
20230517 15:31:53	0	100000.00	187895.72	平安银行股份有限公司		623999051	天津滨海新区泰达科技有限公司	货款	20230517
20230518 14:26:45	0	53000.00	134895.72	中国农业银行股份有限公司		622918476	天津滨海新区泰达科技有限公司	货款	20230518
20230519 14:58:03	345000.00	0	479895.72	中国建设银行股份有限公司		31050000249	天津滨海新区泰达科技有限公司	货款	20230519

1.2 虚假银行 APP 流水

虚假 APP 流水指黑产按照银行官方 APP 的排版格式制作的山寨版 APP 软件。这类山寨版 APP 涉及手机银行、第三方支付平台等 APP，虽然不能真实交易，但仿真度极高，能操作

与账户、转账、交易等相关的点击查看、导出功能，一些非主要功能页面只能展示且无法点击进入下级页面。这类山寨版 APP 涉及手机银行、微信、支付宝等 APP。

以下为某虚假银行 APP 页面信息：



1.2.1 虚假银行 APP 特征

黑产伪造的银行 APP 根据各官方银行 APP 样式、模版及部分功能自主开发，为了节约伪造成本，很多 APP 内部功能缺失，在人工核验环节容易被发现。

威胁猎人实测某虚假银行 APP 发现，虚假银行 APP 存在以下特征：

(1) 涉及流水相关的页面功能可以正常展示且部分功能可以正常操作，但不能真实交易。

该虚假银行 APP 账户查询功能可以点击进入下级页面且查看卡号、查看明细、进入转账页面，转账汇款功能也可以点击进入下级页面且查看转账记录且可以进行进入转账流程、点击常用收款人个人账户可以进入转账页面，可操作转账流程且会显示转账成功且账户余额实时变动，甚至用假银行账户依然会显示转账成功。

以下为某虚假银行 APP 的转账记录情况：

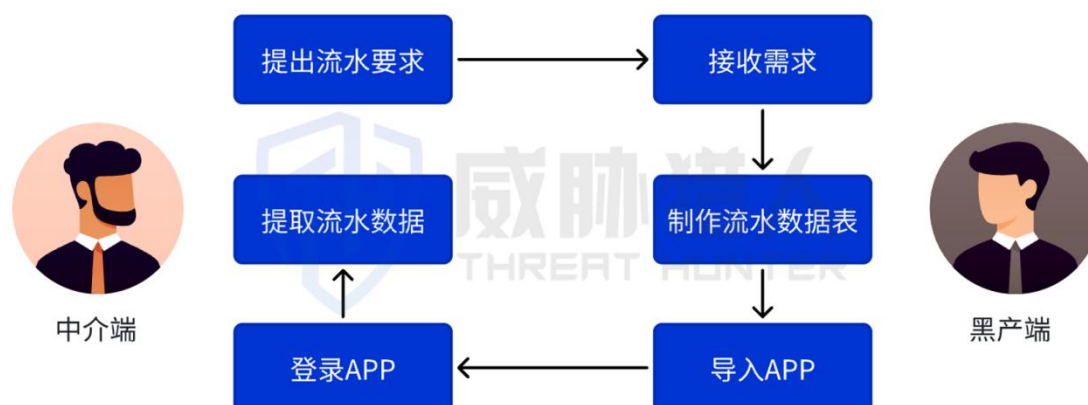


(2) 主页面不涉及流水相关的常规一级页面菜单可以正常点击进入下级页面，但二级菜单页面均无法打开，点击无效。该虚假银行 APP 首页页面生活缴费点击可以进入下级页面，但是二级页面所有信息均点击无效，无法打开下级页面。

(3) 非主页面及其他与流水不相关的页面仅有展示功能，均无法点击打开页面。该虚假银行 APP 首页养老等模块均无法点击打开，无法打开下级页面。

1.2.2 虚假银行 APP 欺诈流程

在实际欺诈场景中，黑产一般通过与金融中介渠道合作的方式攫取利益。首先，中介根据客户资质情况和贷款需求评估该名客户可能需要补充的流水数据，黑产则根据中介提供的相关要求，如客户虚假月收入、虚假月支出、虚假余额、流水制作周期、客户基本信息等数据制作详细的虚假流水数据表，并在已开发好的山寨版银行 APP 后台导入流水数据，生成客户账户信息。随后，中介端或客户端在对应山寨银行 APP 端登录客户账户，即可查看、展示、导出流水数据。



上述这类虚假流水数据的生成过程，黑产只需几小时即可完成，并从中获取几百元到几千元不等的非法利益。黑产提供制定各种金融类山寨 APP 版本的虚假流水服务，黑产按照中介提供的虚假信息在后台上传虚假流水数据，金融中介通过黑产提供的软件安装包下载并安装山寨 APP 即可使用假流水数据。

1.2.3 高低配 APP 版本

手机银行 APP 分为低配 APP 和高配 APP 两种版本，高低配 APP 上展示功能基本一致，均按照官方银行 APP 格式和版面制作，主要区别在于是否可导出邮箱，以及是否可“转账”。

(1) 手机银行低配 APP：只能查看 APP 内数据，APP 制造效果相对粗糙，展示个人账户信息、账户总览、收支明细、转账页面等信息，可以实现在面签环节把数据展示给工作人员核验或截屏留证，价格在 500-600 元不等。

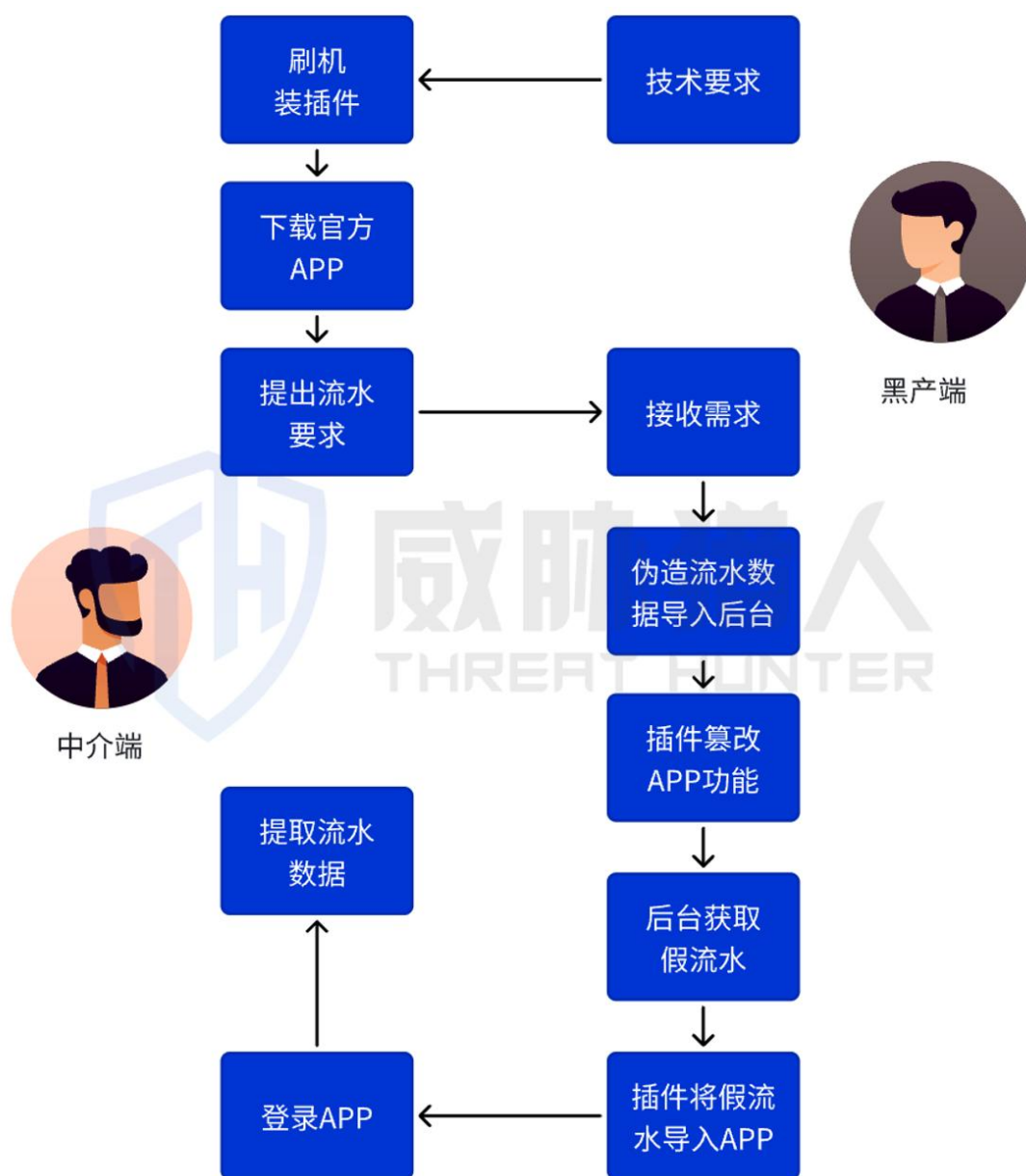
(2) 手机银行高配 APP：不但能查看 APP 内数据，APP 制造效果更真实，除展示个人账户信息、账户总览、收支明细、转账页面等信息，还有导出邮箱功能、还能“假转账”，能自由选择某个时间段内交易流水数据导出邮箱打印，客户可在贷款面签时当场导出数据并输出给面签人员，价格在 1200-2000 元不等。

高配版银行 APP 导出邮箱不需要输入手机验证码或验证码随意输入即可验证成功，且发件人邮箱地址故意设置的与真实官方邮箱地址相似度较高，需仔细查看区别。

另外，高低配 APP 均适用于安卓手机系统，IOS 系统暂未发现虚假银行 APP 流水案例。

1.3 官方银行 APP 虚假流水

官方银行 APP 虚假流水是黑中介通过特定的手机并刷机以逃避银行 APP 的反监测后, 安装黑产提供的指定插件软件, 再下载银行官方 APP, 黑产则利用远程控制该 APP 上传流水数据, 并在该手机 APP 内生成虚假流水。黑中介通过在官方 APP 伪造流水数据为客户申请贷款, 提升通过率和贷款额度, 为使用客户解决真实流水不足的问题。



手机设备刷机、安装作弊插件后，银行官方 APP 被修改，一般无法通过肉眼辨别修改特征，但可以通过技术分析发现官方 APP 某些功能可能被篡改。

威胁猎人通过分析得知，官方银行 APP 虚假流水作恶技术操作流程如下：

- ① 手机设备刷机。
- ② 安装 APatch 用于绕过 Root 检测。
- ③ 安装 Lsposed 作为 Hook 框架。
- ④ 安装 Lsposed 插件，该插件用于 Hook 银行 APP 流水展示相关函数，实现在 APP 中展示虚假流水。

技术逻辑：在设备获取 Root 后，可以在一定层面上绕过银行 APP 对设备环境的检测。

Lsposed 是一个功能丰富的 Hook 框架，黑灰产基于该框架开发插件，可以在不修改银行 APP 的情况下，对银行 APP 的部分代码进行劫持。在该场景中，黑灰产可能通过逆向定位到“获取流水”的代码，通过 Lsposed 框架，可以强制修改该代码的返回值，即虚假的流水数据，从而实现假流水展示。

以下为黑产劫持官方银行 APP 展示虚假流水的逻辑流程：



需要特别注意的是，这种刷机并安装插件后的手机，并不影响其他功能使用。黑产通过安装插件、远程控制手机端的银行官方 APP，这个 APP 完全真实，且所有的 APP 功能都可以正常使用。这个流程一旦跑通，后续只需更换客户银行账户、上传与客户对应的虚假流水数据表即可重复使用，但这些数据只能在该特定手机上显示。

02

虚假流水运用场景

二、虚假流水运用场景

虚假流水可能被黑产使用于任何需要核验个人收入水平来评估还款能力,但又未核验或无法核验第三方官方接口数据的贷款产品中,房贷、车贷等涉及面签环节为黑产重点攻击场景,其他如银行流水(个人、企业)未能连接银行端数据、个税数据未能连接官方税务中心数据、公积金流水未能连接官方侧数据等等仅依赖相关手机 APP 数据的贷款场景,均可能存在虚假流水攻击风险。

2.1 房贷场景

在购房按揭贷款、抵押贷款场景中,往往需要核验客户资产、社保公积金、收入流水等材料,需要客户提供纸质版收入流水、打卡工资流水,或者直接通过银行 APP 导出数据,这类场景可能存在虚假流水欺诈、骗贷风险。

2.2 车贷场景

在购车按揭贷款场景中,往往需要核验客户房产、社保公积金、收入水平等,需要客户提供纸质版收入流水、打卡工资流水,或者直接通过银行 APP 导出数据,也可能存在虚假流水欺诈、骗贷风险。

2.3 企业贷场景

在企业贷款场景如商户贷、流水贷、农户贷、经营贷等,一些金融机构要求企业提供企业流水或法人个人流水来证明企业的经营状况。如果涉及企业流水,黑产通过导出客户真实的企业、个人流水数据,并参照客户真实的上下线来往制作流水信息,使流水真中有假、假中有真,或者完全假。因此企业贷场景也可能存在虚假流水欺诈、骗贷风险。

2.4 消费贷场景

个人消费贷中，为确保申请客户工作的真实性，很多金融机构都连接第三方官方数据，如社保、公积金官方数据，因此避免了一部分欺诈，是虚假流水使用较少的场景。但仍然有一些金融机构需要核验客户收入流水，在此场景也可能存在虚假流水欺诈、骗贷风险。

03

防御思路

三、防御思路

黑产在虚假流水操作手法各异，且在不断迭代：从纸质版虚假流水，到虚假的银行 APP/第三方支付平台流水 APP 低配版、高配版，再到真实银行官方 APP 流水，操作成本越来越高，包装手段也更真实、更隐秘，对金融机构的攻击力度不断加强，金融机构面临的欺诈风险更为严峻。

为此，威胁猎人在反欺诈防御风险方向为金融机构提供以下建议：

- 1、建议加强对面签人员关于虚假银行 APP 流水特征风险培训，及时同步最新的虚假流水案例及欺诈手法特征，让面签人员时刻警惕贷款客户提供的银行 APP 流水的真实性。
- 2、建议加强对客户收入流水数据的审核力度，对大额或异常交易数据进行背景调查，核实交易的真实性和合理性。
- 3、建议在用户协议、贷款合同中要求用户承诺所提供的流水和交易记录真实有效、规定虚假流水的法律责任及警示伪造虚假流水的法律后果。

在贷款 APP 侧，威胁猎人为篡改银行官方 APP 风险从技术层面提供以下风控建议：

- 1、建议增加 xposed 对抗方案，如检测内存是否被修改。检测内存中的代码片段与原代码片段是否一致，若不一致，则当前内存被修改，可能被 hook。检测 self_map 中的 so 片段是否存在 xposed、libepic 等字符串，若存在则可能在不安全的环境下。
- 2、建议加强反调试保护。分别在 Native 层和 Java 层增加更多检测点，且分散到不同的动态链接库或类当中。通过增加多个对抗位置增加分析难度，延缓攻击者的分析进程。
- 3、若检测到设备处于异常环境，如 Root、Xposed 下，建议增加风险评分预警，并增加人工介入风险审核。

四、总结

虚假流水作为信贷欺诈的一种常见手段，不仅严重扰乱了金融市场的正常秩序，还极大地损害了金融机构的利益与消费者的信任。它通过伪造或篡改银行账户交易记录，绕过风控审批，使得原本不符合贷款条件的申请者获得资金，进而可能引发连锁的金融风险，包括不良率的上升、金融机构坏账增加以及对整个经济体系的稳定性构成威胁。因此，金融机构需要持续加强信贷审批过程中的数据验证与风险控制，提高技术手段识别虚假流水的能力，严惩信贷欺诈行为，维护金融安全与稳定、保护消费者权益。



关注“威胁猎人”

深圳永安在线科技有限公司（品牌名：威胁猎人）

☎ 官方服务热线：400-809-3699

✉ 官方合作邮箱：marketing@threathunter.cn

🌐 官网地址：www.threathunter.cn