威胁猎人
THREAT HUNTER

以 情 报 构 筑 数 字 化 安 全 基 石

黑产涉诈资金链

银行账户风险分布存在差异，涉诈资金混入商户流水



关于威胁猎人

威胁猎人 Threat Hunter（深圳永安在线科技有限公司）成立于 2017 年，以黑灰产情报能力和反欺诈技术为核心，专注于及时、精准、有效的业务欺诈风险的发现和响应。

公司围绕不同行业在数字化发展过程中面临的业务欺诈、数据泄露、钓鱼仿冒、API 攻击等风险场景，提供成熟多样的产品与服务，并多次入选 Gartner 技术成熟度曲线报告、IDC 威胁情报领域代表厂商。

公司总部在深圳，在北京、上海、重庆、新加坡等地设有分公司，并在深圳和重庆两地建立数字风险应急响应中心（DRRC），为客户提供 7*24 小时全天候数字风险应急响应和及时、优质的服务支持。截至目前，公司已为金融、政务、物流、互联网、科技、零售等行业的 300 多家客户提供安全服务，覆盖 85%头部互联网企业，每年帮助客户减少数十亿资金损失。

目 录

关于威胁猎人 2

一、黑产涉诈资金如何流转 5

1.1 上游：涉诈资金通过常规支付渠道流转 5

涉诈交易金额与交易笔数的月度峰值并不同步 5

手机银行渠道约占涉诈转账笔数的七成 6

1.2 中游：个人银行卡与企业对公账户呈现不同特征 7

风险对公账户：城市商业银行占比最高 7

个人风险银行卡：近七成集中于六大国有银行 8

1.3 下游：涉诈资金混入商户经营流水 8

风险商户关联多类收单机构，银行收单机构占比超四成 9

风险商户覆盖 80 余个行业，零售与批发合计约占近七成，餐饮行业排名第三 9

二、涉诈资金链识别不能局限于单一账户、渠道或场景 10

三、金融反诈资金链画像帮助金融机构补充外部风险识别能力 12

结语 14

一笔转账，在银行交易系统里往往只是一次普通资金往来。但在黑产涉诈资金链中，收款账户可能只是受害人资金流转的第一站。资金进入账户后，还可能经过归集、分散和多次中转，最终混入商户经营流水。个人银行卡、企业对公账户以及商户收单渠道，都可能成为涉诈资金流转的环节。

威胁猎人持续监测黑产涉诈资金活动。根据 2026 年 1—10 月监测数据，累计识别涉诈转账超 6.4 万笔，涉及金额约 6.6 亿元；其中，手机银行渠道交易笔数约占 67.37%。同时，监测发现风险商户覆盖 80 余个经营行业，从收单机构类型分布来看，银行收单机构占比约 41.12%。



本报告基于上述监测样本，从资金流转的上游、中游、下游三个环节，分析渠道分布、账户主体结构及商户收单场景的风险特征，涉诈资金活动呈现出几个值得关注的特征：

发现一：资金转移集中于常规支付渠道。

发现二：个人与对公账户的银行类型分布呈结构性差异。

发现三：下游资金经商户收单渠道进入经营流水。

一、黑产涉诈资金如何流转

从监测到的涉诈资金活动来看，资金流转涉及多个账户主体与支付渠道：上游通过常规支付渠道承接受害人资金，中游利用个人银行卡和企业对公账户进行归集、分散与中转，下游部分资金通过商户收单渠道混入经营流水。

图 1 黑产涉诈资金流转的三个环节与关键数据



数据来源：威胁猎人监测样本，2026年1—10月

1.1 上游：涉诈资金通过常规支付渠道流转

在涉诈资金链上游，黑产主要利用银行卡、第三方支付账户等承接和转移受害人资金。这些资金并非通过特殊的交易渠道流转，而是大量使用日常金融交易中的常规支付工具。

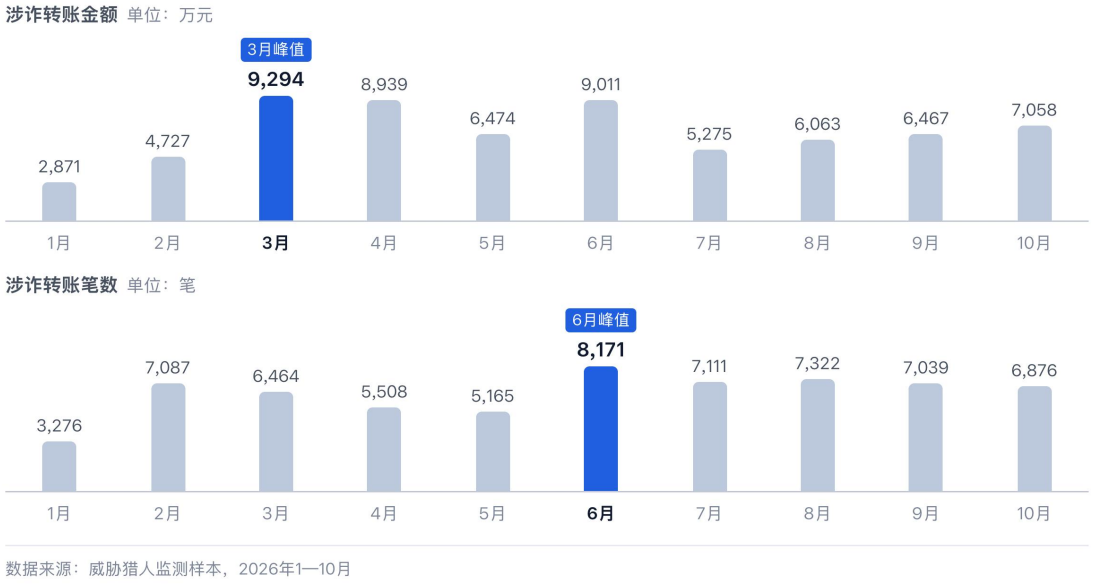
涉诈交易金额与交易笔数的月度峰值并不同步

2026 年 1—10 月，威胁猎人累计监测涉诈转账超 6.4 万笔，涉及金额约 6.6 亿元，平均每笔交易金额约 1 万元。

从月度变化来看，**涉诈交易金额在 3 月达到峰值，交易笔数则在 6 月达到峰值**，两者并不同步。这表明涉诈资金活动的交易规模与交易频次并不完全呈现一致的变化趋势。

对于金融机构而言，识别涉诈资金活动不能只关注单笔交易金额，还需要结合交易频次、交易对手及账户关联关系等信息进行综合判断。

图 2 涉诈转账金额与笔数的月度变化



数据来源：威胁猎人监测样本，2026年1—10月

手机银行渠道约占涉诈转账笔数的七成

从涉诈资金转账渠道来看，手机银行渠道完成的涉诈转账笔数约占 67.37%，第三方支付渠道约占 31.12%。手机银行是本次监测样本中涉诈资金转移的主要渠道。

这一分布说明，涉诈资金活动大量发生在常规金融服务渠道中。对于银行而言，识别风险的关键不仅在于交易通过何种渠道发起，还在于判断本行账户在交易中承担的角色：是作为风险收款方接收涉诈资金，还是作为受害人付款方发生资金转出。



1.2 中游：个人银行卡与企业对公账户呈现不同特征

在涉诈资金链中游，黑产利用个人银行卡、企业对公账户等进行资金归集、分散和中转。相关交易对手可能分布于不同银行，使资金流转涉及多个金融机构。

从监测样本来看，涉诈的个人风险银行卡与风险对公账户在银行类型分布上呈现出明显差异。

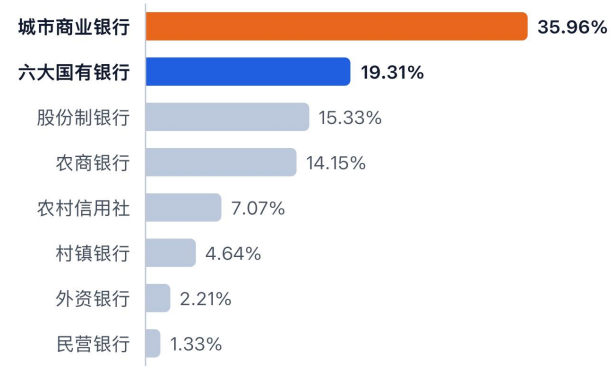
风险对公账户：城市商业银行占比最高

监测数据显示，在涉诈风险的对公账户中，城市商业银行约占 35.96%，六大国有银行约占 19.31%，股份制银行约占 15.33%。

从本次监测识别的账户分布来看，城市商业银行在风险对公账户样本中的占比最高。这提示金融机构在开展对公交易风险排查时，不应仅关注大型银行的交易对手，还需要结合跨行交易关系，对不同银行类型的对公风险账户进行关联核验。

图 4 风险对公账户的银行类型分布

图 4、图 5 横轴比例一致；蓝色为六大国有银行，橙色为城市商业银行



数据来源：威胁猎人监测样本，2026年1—10月

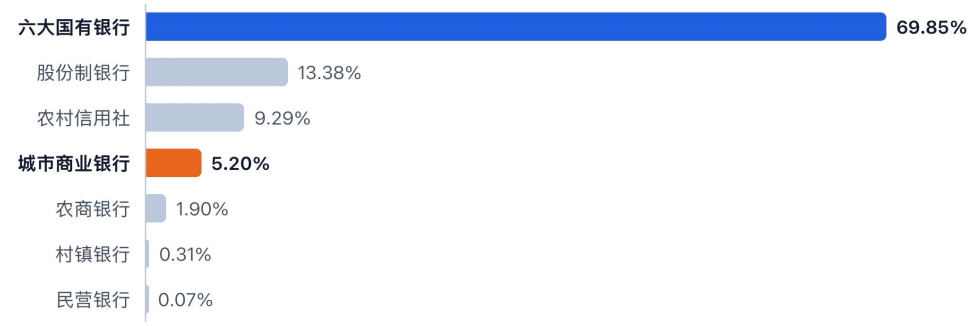
个人风险银行卡：近七成集中于六大国有银行

与风险对公账户的分布不同，监测识别的个人风险银行卡更多集中于六大国有银行，占比接近七成。

这一分布反映出个人风险银行卡与风险对公账户在银行类型上的差异。对于国有大型银行而言，除了关注外部风险交易对手，还需要加强对行内存量个人账户及其关联交易的风险排查。

图 5 个人风险银行卡的银行类型分布

图 4、图 5 横轴比例一致；蓝色为六大国有银行，橙色为城市商业银行



数据来源：威胁猎人监测样本，2026年1—10月

需要注意的是，上述数据反映的是本次监测样本中的风险账户分布，并不直接代表不同类型银行的整体涉诈风险水平。

1.3 下游：涉诈资金混入商户经营流水

商户收单环节为涉诈资金链中需要重点关注的风险场景之一。在涉诈资金链下游，部分资金通过商户收单及结算渠道进行流转，相关交易在形式上可能表现为正常消费，使涉诈资金混入商户经营流水。

风险商户关联多类收单机构，银行收单机构占比超四成

监测数据显示，在风险商户关联的收单机构中，第三方收单机构约占 58.88%，银行收单机构约占 41.12%。

这说明，涉诈风险商户并非只存在于第三方支付收单体系中，银行收单业务同样涉及相关风险。

对于金融机构而言，风险商户排查需要覆盖不同收单机构关联的商户，并结合商户真实经营情况、交易行为及外部涉诈风险线索进行综合核验，避免仅凭单一异常特征对正常商户作出风险判断。

图 6 风险商户关联的收单机构分布



数据来源：威胁猎人监测样本，2026年1—10月

风险商户覆盖 80 余个行业，零售与批发合计约占近七成，餐饮行业排名第三

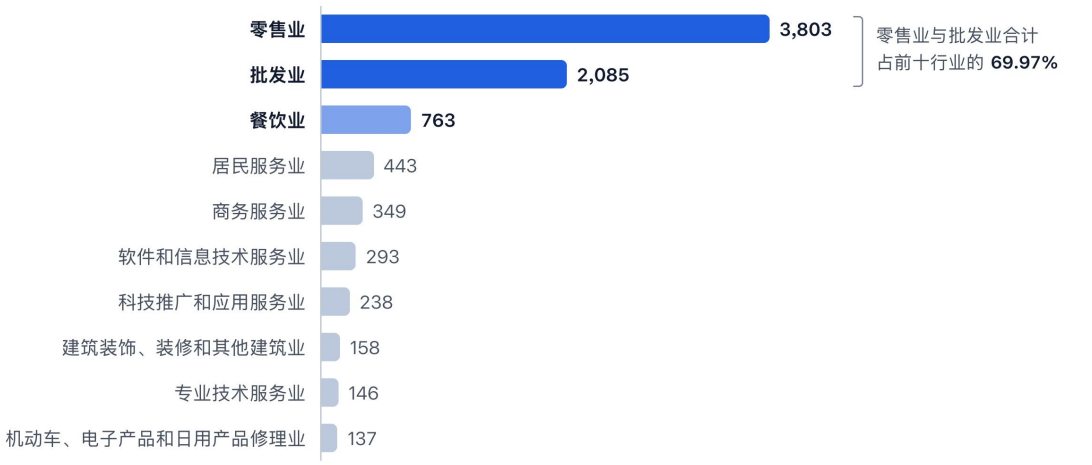
从经营行业来看，本次监测识别的风险商户覆盖 80 余个行业，呈现出较为分散的行业分布特征。

在风险商户数量排名前十的行业中，零售与批发合计约占近七成，餐饮行业排名第三；这一分布表明，风险商户涉及多个日常经营场景。

对于银行及收单机构而言，可以优先关注风险商户数量较多的行业，但行业类别本身不应成为判定涉诈风险的唯一依据。实际排查仍需结合商户经营特征、交易情况及外部风险信息进行核验。

图 7 风险商户数量排名前十的行业

单位：户



数据来源：威胁猎人监测样本，2026年1—10月

二、涉诈资金链识别不能局限于单一账户、渠道或场景

从上游资金承接、中游账户归集与中转，到下游商户收单，涉诈资金活动涉及不同账户主体、支付渠道及经营场景。

如果金融机构仅从某一种账户类型、某一支付渠道或某个经营行业开展风险识别，可能难以完整掌握涉诈资金活动涉及的关联主体与交易关系。

结合本次监测情况，可以从以下三个维度理解涉诈资金链识别中的风险盲区。

表 1　涉诈资金链识别的三个风险盲区

维度	常见看法	监测里更常见的资金链走法	风控排查容易漏什么
账户类型	重点关注个人银行卡，或认为企业对公账户相对安全	个人银行卡多用于分散收款与中转，对公账户多用于资金归集与集中转移	仅排查单一账户类型，可能遗漏个人与对公账户之间的关联，以及跨行资金流转关系
支付渠道	将风险识别重点放在特殊或异常支付渠道	大量涉诈资金通过手机银行、第三方支付等常规渠道流转	仅依据支付渠道判断风险，容易忽略交易对手身份及前后关联账户
交易场景	主要关注账户之间的直接转账	部分涉诈资金通过零售、批发、餐饮等行业的商户收单渠道流转，交易形式可能类似正常消费	仅关注账户交易，可能遗漏商户收单场景中的风险；仅依据行业类别判断，也可能误伤正常商户

从上述特征来看，涉诈资金链风险识别不能只依赖单一维度。个人银行卡、企业对公账户和风险商户之间的关联关系，以及资金在不同渠道和机构之间的流转情况，都是金融机构开展涉诈风险排查时需要关注的信息。



三、金融反诈资金链画像帮助金融机构补充外部风险识别能力

银行能够基于行内账户信息和交易流水开展风险监测，但对于行外交易对手是否属于涉诈风险主体、资金是否关联其他风险银行卡及企业对公账户，以及交易是否涉及风险商户，仍可能存在信息覆盖不足的问题。

尤其当涉诈资金涉及跨行交易和不同收单机构时，仅依靠本行单笔交易信息，往往难以完整还原相关风险主体之间的关联关系。

针对这一问题，威胁猎人金融反诈资金链画像基于对黑产涉诈资金活动的持续监测，围绕涉诈交易、风险账户及风险商户，为金融机构提供可用于风险核验与关联排查的外部情报线索。

产品主要包括四类风险画像，分别对应不同的资金链识别场景。

表 2　金融反诈资金链画像的四类风险画像

画像类型	能力说明
诈骗交易画像	提供涉诈交易中的收付款账号信息，帮助金融机构识别风险收款账户，开展关联交易排查。同时，可以沿付款方线索发现疑似受害人，为风险提醒、劝阻和资金止损提供辅助依据。
风险银行卡画像	提供涉诈风险银行卡线索，支持金融机构对存量个人账户开展风险筛查，并结合行内交易数据识别相关账户的关联交易风险。
风险对公账户画像	提供涉诈风险企业账户线索，支持金融机构开展对公账户风险核验，以及相关可疑对公交易的关联排查。
风险商户画像	提供涉诈风险商户及关联交易线索，支持金融机构开展存量商户风险排查、交易核验与差异化风险管控。

在实际银行风控业务中，上述四类情报可以与现有账户管理、交易监测及事件核查流程相结合，主要应用于事前、事中和事后三个环节。

表 3　资金链情报在银行风控中的三个应用环节

事前风险排查	事中交易监测	事后事件核查
在存量个人账户、企业对公账户及商户的风险排查过程中，引入外部涉诈风险名单，识别需要重点核验的潜在风险主体，并结合行内信息开展进一步核查。	在交易风险监测过程中，匹配外部风险账户及交易对手方情报，为异常交易识别、风险预警和必要的交易干预提供辅助判断依据。	在涉诈事件调查及风险处置过程中，结合外部涉诈交易、风险账户及关联商户线索，补充跨行账户关联和相关交易信息，支撑事件核查与后续处置。

通过将外部涉诈资金情报与银行现有风险管理流程相结合，金融机构可以在单笔交易识别的基础上，进一步拓展对风险账户、交易对手及关联商户的综合排查能力。

结语

涉诈资金链的隐蔽性，不仅在于资金的多次流转，更在于其利用常规金融渠道和经营场景掩盖风险。

对于金融机构而言，识别涉诈资金风险不能只关注单笔交易或单一账户，更需要结合**交易对手风险、跨行账户关联及风险商户线索**，加强对涉诈资金链的识别与排查。

威胁猎人也将持续关注黑产涉诈资金活动，跟踪风险账户、资金转移渠道及商户收单等环节的变化，为金融行业提供更多风险观察与研究参考。

威胁猎人
THREAT HUNTER

以情报构筑数字化安全基石

关注“威胁猎人”

公司官网：**www.threathunter.cn**

合作邮箱：Marketing@threathunter.cn