威胁猎人 THREAT HUNTER

威胁猎人 · 2026 行业威胁专题研究（公开发布版）

绕开电信网的诈骗新物种：2026 涉诈黑灰产脱网演进与跨行业外溢研究报告

从「伪造律师函」「无码上门快递」到「汽车召回」骗局的全链路透视

2026 年 1—11 月，在运营商拦截收紧与工信部第 74 号令落地的强监管背景下，假冒催收黑灰产并未消退，而是完成了一次彻底的“脱网换代”：话术升级为高仿真《律师函》，触达从短信两级跃迁至苹果 iMessage 与「无码纯链接 + 付费电联上门快递」，底层更依托“一服多盘”的通用黑产基建，将既有作恶能力迅速外溢至「汽车召回」等真实公共事件场景。本报告基于威胁猎人全年持续监测，还原其对抗演进与基础设施全貌，为金融借贷、物流快递、汽车行业及社会公众提供前瞻风险预警。

威胁猎人 · 数据泄露与黑灰产风险研究 | 监测周期：2026 年 1—11 月

目录

卷首｜核心发现与 2026 年演进总览

一、强监管下的“猫鼠变局”：短信堵死后，假催收为何没有消失？

1.1 政策与运营商双重合围：短信群发的 ROI 崩塌

1.2 剧本升级：从“电话施压”转向“制式律师函流程引导”

1.3 精密伪造拆解：复用母版、信用代码末位篡改与 H5 登录页反筛

二、通道逃逸两级跳：从 iMessage 到「无码纯链接 + 付费上门件」

2.1 第一跳（线上绕网）：iMessage 补齐图文可信度，倒逼中游标配“苹果过蓝”

2.2 第二跳（物理脱网）：线下快递代发放量，借正规物流背书降低戒心

2.3 10 月底最新对抗变形：取消二维码改印短链，指定付费电联上门专线

三、穿透迷雾：九大专业分工与“一服多盘”通用黑产底座

3.1 产业链全景：九大专业化分工与“越近收款越隐蔽”的留痕梯度

3.2 上游供给真相：6 月低点是平台封群后的阵地迁徙，而非供给萎缩

3.3 通用资源层溯源：同一台服务器承载五类以上涉诈盘口

3.4 域名池与高敏捷对抗：7 月末备货交汇点与封禁后 6 天三代演进

四、跨界外溢警报：当同一套能力撞上“80 万辆汽车召回”

4.1 早于舆情的预谋：7 月同批备域、10 月底车主数据切分交付

4.2 为何穿透力极强：真公共事件 + 真车牌信息 + 假故障理由

4.3 隐藏的金融暗雷：车主与车贷客群重叠，正常申贷演变为消金不良

EXECUTIVE SUMMARY

卷首｜核心发现：2026 涉诈黑灰产的“脱网换代”

2026 年，假冒催收黑灰产完成了一次彻底的“脱网换代”。随着三大运营商收紧引流拦截及工信部第 74 号令于 5 月 1 日正式施行，依靠低成本短信群发施压的传统假催收迅速退场。但威胁猎人 1—11 月的持续监测表明，黑灰产并未萎缩，而是在 6 月前后完成了通道、剧本与基础设施的全面升级：线上转向苹果 iMessage 投递高仿真《律师函》，线下则借正规快递将纸质函件直接送达受害人手中。

更具警示意义的变化发生在 10 月下旬之后：面对警方对涉诈打印寄递窝点的打击与快递网点对“含二维码信函”的严查，黑灰产迅速进化出**「无码纯链接 + 付费电联上门件」**新形态——取消纸面二维码、改为打印短网址诱导手机自带浏览器手动输入，一举绕开物流扫码查验与微信/支付宝反诈红页。深度溯源进一步揭示，假冒催收并非孤立骗局，而是寄生在一套由“设备精准筛料 + 通用建站模板 + 提前百天备货的 2 年期域名池”构成的模块化黑产基建之上；11 月借“80 万辆汽车召回”爆发的车主诈骗，正是这套既有能力换壳跨界外溢的最新样本。

线上通道迁移峰值（6 月）

32,112 条

iMessage 涉诈相关信息量单月跃升，同期短信催收招揽自 5 月 3,418 条峰值骤降。

无码纯链接快递（11 月前 22 日）

环比涨近 5 倍

由 10 月首现的 23 条激增至 114 条，借“手输短链 + 付费上门”双绕物流与扫码防线。

基础设施提前备货（7 月 29 日）

50 分钟 42 域

消金催收与汽车召回同批交错预注 2 年期域名，静默 88–102 天后于秋冬按需启用。

通用资源层抗封敏捷度

6 天 3 代升级

单台源站承载 5 类以上涉诈盘口；仿冒站遭封禁后 5 天内换域、6 天内加装滑块验证并出海。



图 1　2026 年 5—11 月涉诈黑灰产「脱网换代与跨界外溢」全链路关键节点

本报告四大核心研判

1. **形态与门槛重构：**作恶逻辑从“电话/短信说服”升级为“高仿真文书流程引导”，把受害人的判断门槛从“分辨陌生号码”拉高至“核验专业法律文书”。
2. **物理脱网与无码对抗：**黑灰产已完成“短信 → iMessage → 有码快递 → 无码纯链接付费上门件”的四阶跃迁，常规电信拦截与单一二维码查验规则均已出现盲区。
3. **模块化通用底座：**6 月上游泄露低点实为 Telegram 封群引发的阵地迁徙（10 月已反弹至 229 起）；假催收仅是“一服五盘”通用黑产基建上的外挂业务，仅打前端盘口收效甚微。
4. **热点公共事件跨界外溢：**“汽车召回”诈骗证明黑灰产稀缺的不是能力，而是诱发点击的真实公共事件；其通过诱导车贷客群正常申贷，将跨界风险悄然转化为消费金融的新增不良。

PART 01

一、强监管下的“猫鼠变局”：短信堵死后，假催收为何没有消失？

2026 年 6 月是一道清晰的行业分水岭。6 月之前，假冒催收黑灰产主要依靠电话、短信冒充借贷平台催收人员施压；6 月之后，其全面转为投递形式逼真的伪造《律师函》，诱导收件人进入仿冒页面完成“还款”或“验资”。

1.1 政策与运营商双重合围：短信群发的 ROI 崩塌

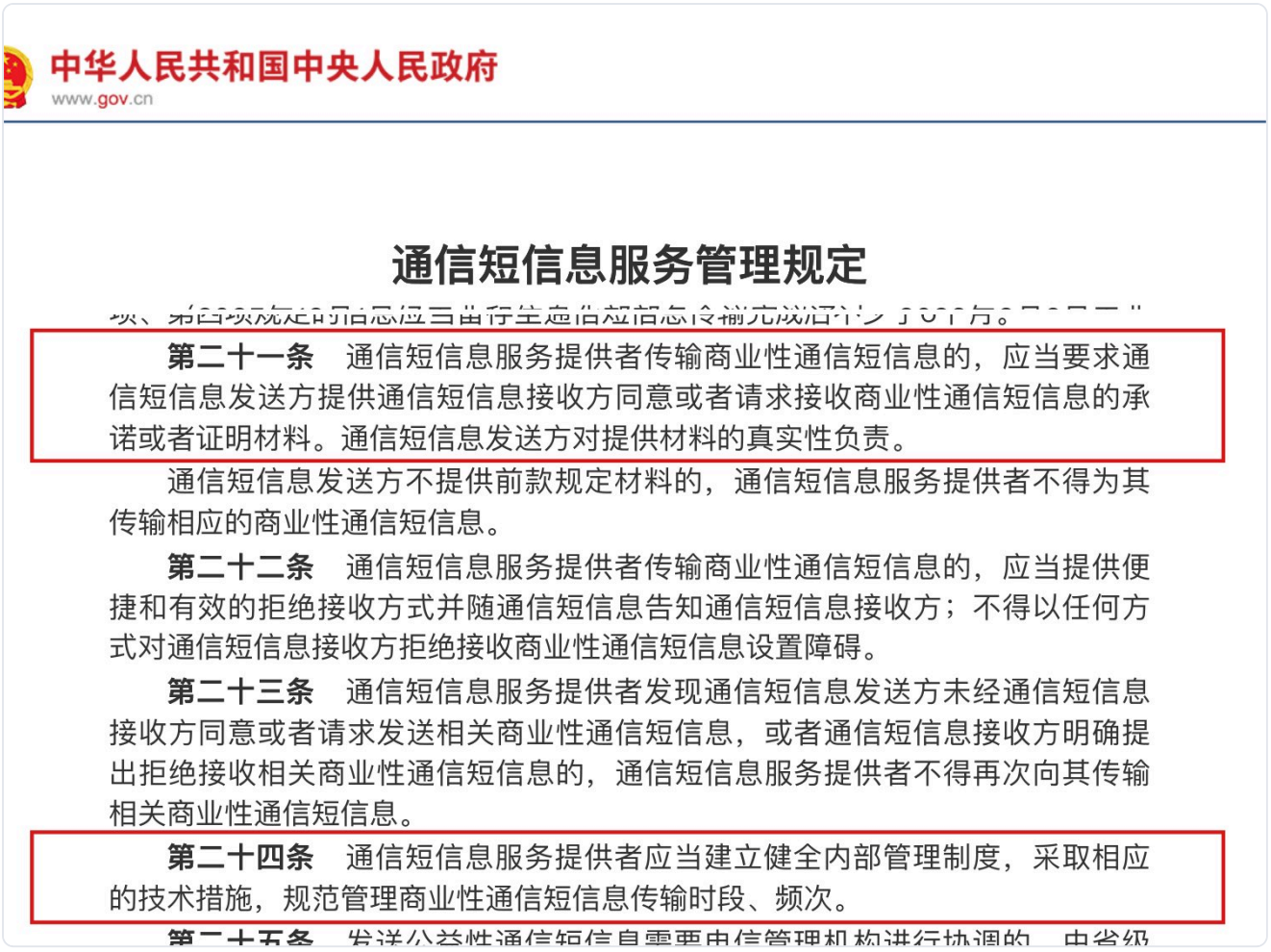
短信曾是此类诈骗覆盖最广、单价最低的触达通道。但 2025 年下半年至 2026 年上半年，这条通道从基础电信企业技术拦截与行业法规两个层面被彻底收紧——其中最具决定性的是 **2026 年 5 月 1 日正式施行的《通信短信息服务管理规定》（工业和信息化部令第 74 号）**。

时间	主体	治理措施
2025-05-20	中国电信	短信含链接、IP 地址或联系方式的，较大概率触发拦截
2025-07	中国联通	短信含联系方式的，须提前报备审核
2025 年内	中国移动	陆续开启「引流信息拦截」，含链接、联系方式触发拦截
2026-05-01	**工业和信息化部**	**第 74 号令施行**：发送方实名核验、端口不得混用、须有接收方同意材料、传输时段与频次纳入规范管理

表 1　2025—2026 年短信通道收紧的四个关键节点

第 74 号令中打击最直接的是**第二十一条**：传输商业性短信，必须取得接收方同意或请求接收的承诺或证明材料，发送方对材料真实性负责；不提供材料的，服务商不得为其传输。催收类短信的接收人从未同意接收此类信息，黑灰产无法提供合法材料，正规端口通道由此关闭。

同时，**第十八条**严禁商业性短信与业务管理、服务性短信混用端口码号，**第十九条**要求传输发送方真实身份并可追溯——过去借服务类端口夹带、伪造签名拉高到达率的灰色做法随之失效；**第二十四条**则要求服务商建立健全管理制度，规范商业短信的传输时段与频次。


中华人民共和国中央人民政府
www.gov.cn

通信短信息服务管理规定

第二十一条 通信短信息服务提供者传输商业性通信短信息的，应当要求通信短信息发送方提供通信短信息接收方同意或者请求接收商业性通信短信息的承诺或者证明材料。通信短信息发送方对提供材料的真实性负责。

通信短信息发送方不提供前款规定材料的，通信短信息服务提供者不得为其传输相应的商业性通信短信息。

第二十二条 通信短信息服务提供者传输商业性通信短信息的，应当提供便捷和有效的拒绝接收方式并随通信短信息告知通信短信息接收方；不得以任何方式对通信短信息接收方拒绝接收商业性通信短信息设置障碍。

第二十三条 通信短信息服务提供者发现通信短信息发送方未经通信短信息接收方同意或者请求发送相关商业性通信短信息，或者通信短信息接收方明确提出拒绝接收相关商业性通信短信息的，通信短信息服务提供者不得再次向其传输相关商业性通信短信息。

第二十四条 通信短信息服务提供者应当建立健全内部管理制度，采取相应的技术措施，规范管理商业性通信短信息传输时段、频次。

图 2 《通信短信息服务管理规定》原文，红框标注第二十一条与第二十四条（来源：中国政府网国务院公报）

除强监管外，两个市场因素同样加速了短信退场：一是**内容可信度大幅下降**，公众对陌生号码发来的「逾期通知」「法务通知」已普遍警惕；二是**发送成本攀升**，端口收紧推高群发单价且须频繁更换号段。监管、信任与成本三重挤压下，传统短信群发的投入产出比彻底恶化。

1.2 剧本升级：从“电话施压”转向“制式律师函流程引导”

威胁猎人持续监测两类核心黑灰产招揽情报——“催收话术 / 假催”与“律师函”。2026 年 1—11 月的月度走势清晰呈现出新旧形态的此消彼长：

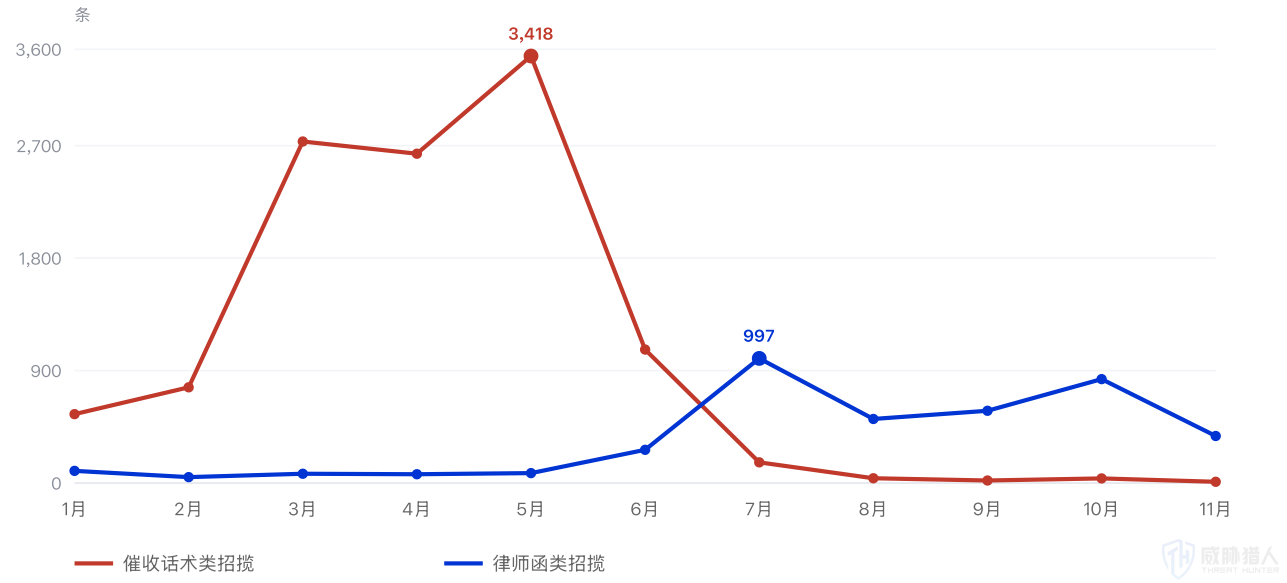


图 3　2026 年 1—11 月两类招揽情报量月度变化：催收话术类招揽在 5 月达 3,418 条峰值后骤降，律师函类招揽在 7 月达 997 条峰值

2026 年 3—5 月，催收话术类招揽分别为 2,734 条、2,636 条、3,418 条，为全年最高区间；新规 5 月 1 日施行仅一个月后，6 月便锐减至 1,068 条，7 月进一步跌至 166 条，8 月以后持续徘徊在数十条低位。反观律师函类招揽，年初尚在百条以内，随后一路攀升并于 7 月达到 997 条峰值，此后始终维持在数百条量级高位运行。

> **核心洞察**
>
> **短信催收考验用户「陌生号码可不可信」，而带公章与文号的假律师函把门槛抬高到了「专业法律文书是真是假」——诈骗由此从口头“说服”彻底升级为无通话的“流程引导”。**

收到陌生号码发来的“贷款逾期、将上报征信”短信时，多数用户凭借常识就能识破；而收到一份抬头规范、加盖律所公章、附有案号与承办律师信息的《律师函》时，普通人往往缺乏专业核验能力，更容易在恐慌中按指引操作。



图 4　旧版短信催收路径：冒充客服施压 → 短信链接打开假账单 → 准备转账



图 5　新版伪造律师函路径：投递制式函件 → 扫码/输链进入假还款网站 → 诱导验资转账

以 2026 年 3 月下旬北京警方通报的一起典型案件为例（表明该手法在 3 月已现个案，6 月后全面规模化投放）：受害人在苹果 iMessage 中收到一份加盖“北京某峰律师事务所”公章的《律师函》图片，载明其欠款 4 万元。受害人扫码进入“还款通道”填写银行卡信息后，黑灰产分三步实施资金收割：

- **第一步（制造报错）**：页面提示“转账未备注姓名，需重新操作”，令受害人误以为首次还款失败；
- **第二步（诱导验资）**：页面提示“需进行银行验资以证明账户正常”，诱导转入更大额资金；
- **第三步（虚构退款）**：验资完成后页面显示“资金将原路退回”，实际款项已被瞬间转移。

整个过程**零通话、无客服对质**，作案者无需在电话中绞尽脑汁说服受害人，只需诱使其沿着一个外观正规的线上流程逐步走完；若受害人未即时响应，数小时后还会补发施压催办消息（如「不回复当严重不处理债务将上门拜访」），形成二次心理逼迫。



图 6　北京警方通报：一个月内接报同类 iMessage 假律师函警情 12 件，涉案超 26 万元



图 7　受害人收到的伪造律师函图片及数小时后补发的施压催办消息

1.3　精密伪造拆解：复用母版、信用代码末位篡改与 H5 登录页反筛

威胁猎人 DRP 情报团队对多批涉案伪造函件开展结构比对后，发现两大高度工业化的共性特征：

一是母版批量复制，文号高度重复。不同受害人在数月间收到的律师函竟频繁出现完全相同的函件文号，明显违背真实律所文号逐件递增的业务规范。这表明作案方持有涵盖京沪等地律所名义的多套成熟母版，仅批量替换收件人姓名与欠款金额即可大规模生成。

二是隐蔽篡改统一社会信用代码末位。已核验样本中，律所名称、文号、承办人均可对应真实主体，但最隐蔽的篡改点集中在统一社会信用代码的末位字符——**将真实的末位数字替换为形近字母（例如将 `5` 改为 `S`）**。这一改动肉眼极难察觉，却足以让受害人“照抄代码去官方渠道核验”的动作直接失效。

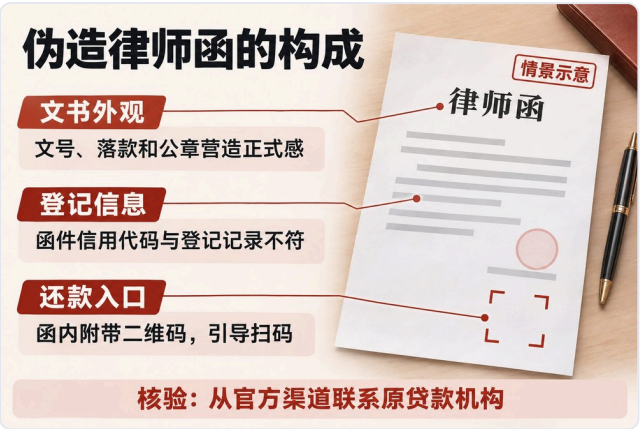


图 8　伪造律师函三大构成要素：制式文书外观、被篡改的登记信息、诱导跳转的还款入口



图 9　统一社会信用代码末位对照：真实登记代码末位为数字 5，伪造函件改为形近字母 S

与此同时，承接受害人的仿冒站点也在同步升级。早期涉案页面往往只是一个粗陋的跳转页，而监测期内已演进为高仿真的完整 H5 应用——打开即为某消费分期产品登录页，提示“输入手机号即可查询账单”。这一改版带来双重杀伤：一方面交互体验逼真，受害人更难从页面识破；另一方面**“登录即校验手机号”成为黑灰产清洗有效数据的漏斗**，能将外流名单实时过滤为高活跃可转化目标。



图 10　仿冒站点升级形态：高仿某消费分期产品 H5 登录页，输入手机号即可查账单（品牌名已脱敏）

PART 02

二、通道逃逸两级跳：从 iMessage 到「无码纯链接 + 付费上门件」

短信通道被封堵后，黑灰产的触达链路发生了两级跃迁：先是通过苹果 iMessage 绕开运营商短信网关，继而借正规物流快递绕开整个电信网络。而在 10 月下旬警方打击与快递网点严查二维码之后，线下投递再度发生剧烈对抗变形。

2.1 第一跳（线上绕网）：iMessage 补齐图文可信度，倒逼中游标配“苹果过蓝”

在运营商严控短信链接的背景下，苹果 iMessage 成为黑灰产首选的线上替代通道。二者的核心差异不仅在于绕开短信网关，更在于**iMessage 支持高清图文直发**——同一套催收话术被封装为带公章的《律师函》图片后，视觉冲击力与可信度呈量级跃升。这也解释了为何通道迁移与形态换代在 6 月同步发生，二者本就互为条件。



图 11　传统短信与苹果 iMessage 在传输通道、内容形态、用户体感及成本结构上的核心差异

监测曲线清晰印证了这次爆发：**2026 年 6 月，iMessage 相关黑产业务信息量单月跃升至 32,112 条**，7—10 月持续维持在 2.4 万条以上的高位，11 月回落至约 1.78 万条；几乎同

步，线下快递代发需求则从秋季开始蓄力，并在 10 月飙升至 2,010 条峰值（约为放量前常态月份月均水平的 4 倍）。

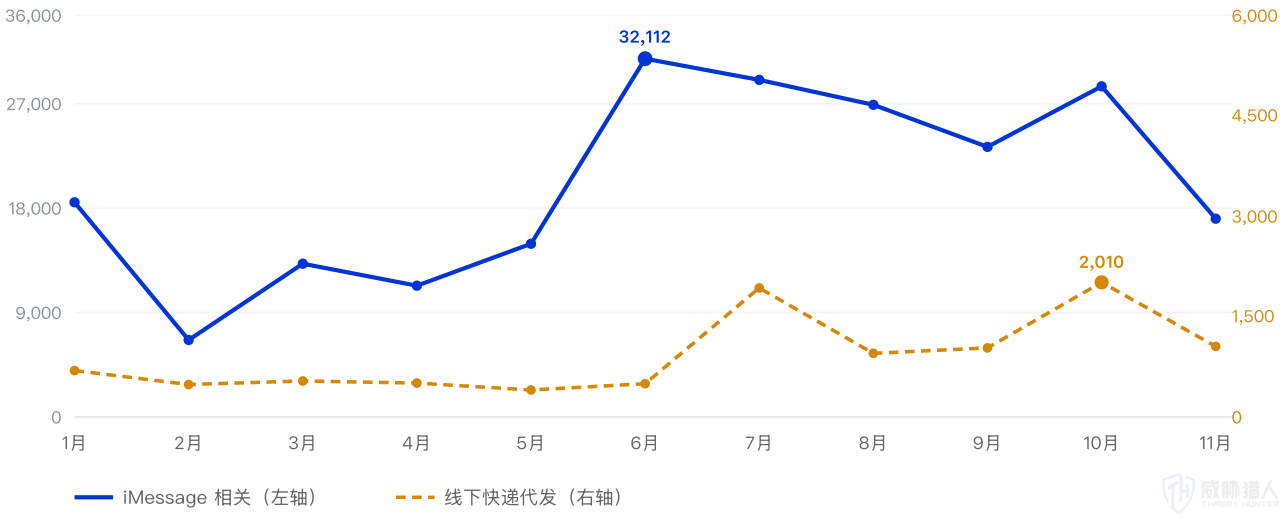


图 12　2026 年 1—11 月 iMessage 相关信息量（左轴）与线下快递代发需求（右轴）变化趋势

下游通道的迁移迅速传导至中游数据交易市场。由于 iMessage 只能触达活跃苹果设备，过去仅作增值选项的“按设备类型筛选”，在 2026 年已演变为跨场景（催收、退费、汽车召回等）的普遍标配。在 10 月监测到的一则二手催收数据售卖帖中，卖家直接把**「筛 im」「苹果过蓝 0 误差」**作为核心卖点单独标注，按月列示覆盖 2025 年 5—12 月合计 42,393 条的精准 iOS 数据包。多一道筛料工序必然抬高单条获客成本，但买家仍愿支付溢价，恰恰反证了 iMessage 伪造律师函模式在黑灰产收益测算中的高转化率。

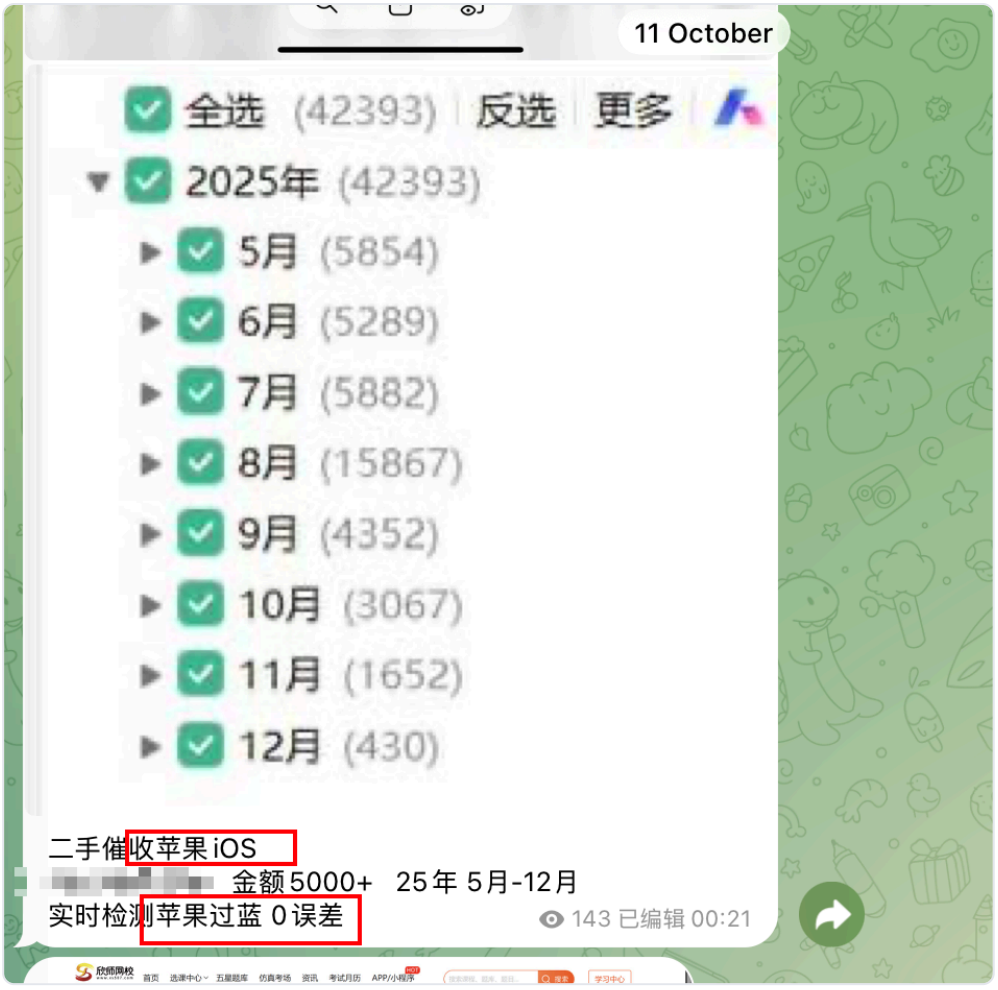


图 13　中游数据交易联动升级：卖家将「苹果过蓝 0 误差」作为标准交付规格公开招揽

2.2　第二跳（物理脱网）：线下快递代发放量，借正规物流背书降低戒心

线上通道无论如何切换，终究仍暴露在互联网与电信风控体系之内；要彻底脱离电信侧拦截，物理投递成为最后一环。2026 年 10 月，指向线下打印寄递的招揽信息暴涨至 2,010 条。

监测到的代发招揽非常直白：黑灰产已形成“排版打样 + 提供数据 + 打印封装 + 代发走件”的一条龙黑产代发服务，恶意滥用顺丰、京东、EMS 及主流通达系等正规快递网络与对应品牌的专用文件封，明确标注「律师函」为专门承接品类，甚至宣称「发 5,000 至 10,000+ 保量」。

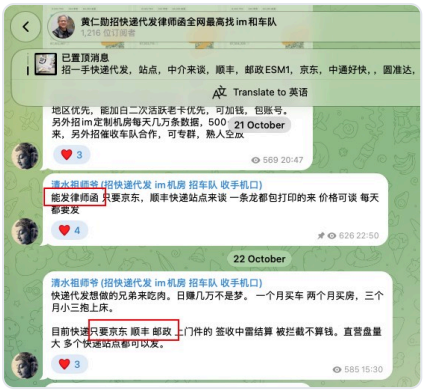


图 14　代发招揽信息：明确标注「能发律师函」并滥用多家正规快递渠道



图 15　配套囤积的多品牌专用文件封与包材

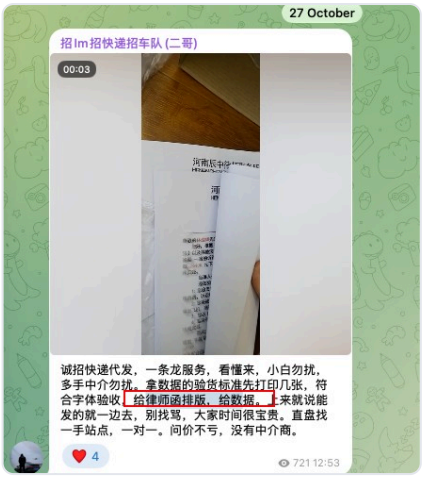


图 16　「律师函排版、给数据」一条龙打样代发服务

这一环节最棘手之处不在于“寄快递”本身，而在于**正规快递的真实面单、可查物流轨迹与签收妥投记录，客观上为伪造律师函提供了极强的真实性背书**，使收件人心理防线大幅瓦解。同时，该触达路径完全运行在电信网络之外，短信拦截、号码标记与网址阻断等常规反诈手段全部鞭长莫及。

2.3　10 月底最新对抗变形：取消二维码改印短链，指定付费电联上门专线

2026 年 10 月下旬以来，随着公安机关集中打击境内涉诈打印寄递窝点（如 10 月 22 日上海警方查获印寄 3,000 余封带二维码假律师函的团伙），以及各大快递网点紧急强化对「A4 纸 + 二维码」涉诈快件的安检拦截，线下投递环节在短短数周内爆发了新一轮剧烈变形——**纸质函件全面取消二维码，转向「无码纯链接」形态**。

> **关键拐点**
>
> **取消纸面二维码不是技术倒退，而是一次精准的“一石二鸟”：同时绕开快递网点的二维码安检拦截，以及微信、支付宝扫码内置的反诈红页预警。**

所谓「无码纯链接」，即伪造的纸质《催收律师函》上不再印刷任何二维码图案，改为在正文直接打印一行短网址文字，诱导收件人手动打开手机自带浏览器输入访问。这一变化瞬间击穿了两道现有防线：

- **第一道防线（物流揽收与分拣侧）**：纸面消失二维码后，快递网点与分拣中心针对「带二维码涉诈信函」的视觉查验、机器抽检与网点处罚机制均难以命中；
- **第二道防线（即时通讯与支付侧）**：诱导受害人手动在手机系统浏览器输入短网址访问，直接绕开了微信、支付宝扫码时内置的高危链接拦截与反诈红页提示。

监测数据揭示了这一变形的惊人扩散速度：明确标注「不带二维码 / 无码纯链接」的催收快递招揽在 2026 年 1—9 月近乎为零，**10 月 21 日首次出现（当月 23 条），到 11 月前 22 天便迅速飙升至 114 条，单月环比暴涨近 5 倍。**



图 17　2026 年 1—11 月「催收函快递代发」与「不带二维码 / 无码纯链接」招揽量走势（11 月截至 22 日环比增长近 5 倍）

与“去二维码”同步升级的，是下游盘口对寄递产品线与网点资源的精准挑拣。为防止普通快件被投入快递柜或驿站而无人拆阅，招揽方普遍放弃低价普件，**不惜抬高单件成本，强制要求滥用主流高端直营快递、邮政 EMS 以及通达系承诺电话联系并送货上门的付费专线产品**，配合对应品牌专用文件封，借由“快递员致电当面递交律师函”制造强烈心理威慑。在结算上，黑产甚至推行「签收或拒签均结算、唯独被快递网点拦截不结算」的规则，并公开寻觅能规避安检抽查的异常发件站点。



图 18　纸质涉诈函件两代投放形态对比：旧版「有码普件」与新版「无码纯链接 + 付费上门件」

PART 03

三、穿透迷雾：九大专业分工与“一服多盘”通用黑产底座

如果只盯着前端的律师函或某一家仿冒网站，极易低估对手的真正体量。威胁猎人穿透前后台痕迹后发现，假冒催收早已脱离零散团伙作案，而是嵌入在一套高度专业化、模块化且跨场景复用的黑灰产通用基础设施之中。

3.1 产业链全景：九大专业化分工与“越近收款越隐蔽”的留痕梯度

按生产与交易角色拆解，该产业链已形成**九个专业化分工环节**：上游供给包含①数据供货、②话术与素材、③文书模板；中游生产包含④建站系统、⑤域名池储备；下游触达包含⑥线上发送产能（iMessage 机房/人工拨号）与⑦线下投递产能；此外还有横跨全链条的**⑧担保层**（收押金、发凭证、裁决纠纷）与**⑨撮合方**（资源拼装、跨场景复用）——后两者的存在，标志着该生态已完全步入组织化、产业化阶段。



图 19　假冒催收产业链的九大专业化分工结构全景图

深入溯源各环节后，一条极具实战意义的规律浮现出来：**越靠近技术供给的一端越容易留下客观痕迹，越靠近收款的盘口运营方越干净。**其中，④建站与⑤域名最为关键——前者在涉案服务器中留下了被多盘口复用的同一套高仿 H5 场景建站系统及开发团队对外署名线索（出于审慎原则，因页面标题署名存在被冒用可能，其真实归属及是否主观明知仍待执法进一步核

实，公开版对此作脱敏处理）；后者则完整记录了批量预注册的时间戳与启停节奏，构成了当前最具可操作性的处置切入点。

核心层级	当前溯源状态	关键依据与实战研判
建站系统	可定位复用模板	涉案服务器承载的 200 余个站点中，多站共用同一套高仿 H5 场景秀建站系统默认标题与售卖展示页，表明其系可批量复制的工具化供给（对外署名是否属实或明知待核实）
服务器与备案	已定位源站	两台核心源站在监测期内持续运行；关联备案主体为两家已注销的空壳企业，表明备案信息本身已不构成真实主体线索
域名资源池	已定位节奏	批量注册的时间戳、有效期选择与静默启停规律高度清晰，是当前最适合率先落地打击与前置预警的一层
盘口运营方	高度隐蔽	事发早期前端页面仅做极简跳转、不承载业务逻辑，收款环节与主站剥离，仅凭前端页面痕迹难以直接回溯资金控制主体

表 2　涉案关键基础设施四层溯源能力评估

3.2　上游供给真相：6 月低点是平台封群后的阵地迁徙，而非供给萎缩

在观察 2026 年 1—10 月消费金融行业数据泄露事件量时，一个容易引发误判的现象是：剔除 2 月春节假期的季节性回落（75 起）外，**6 月录得 80 起的常态低点**。这是否意味着上游数据供给开始枯竭？

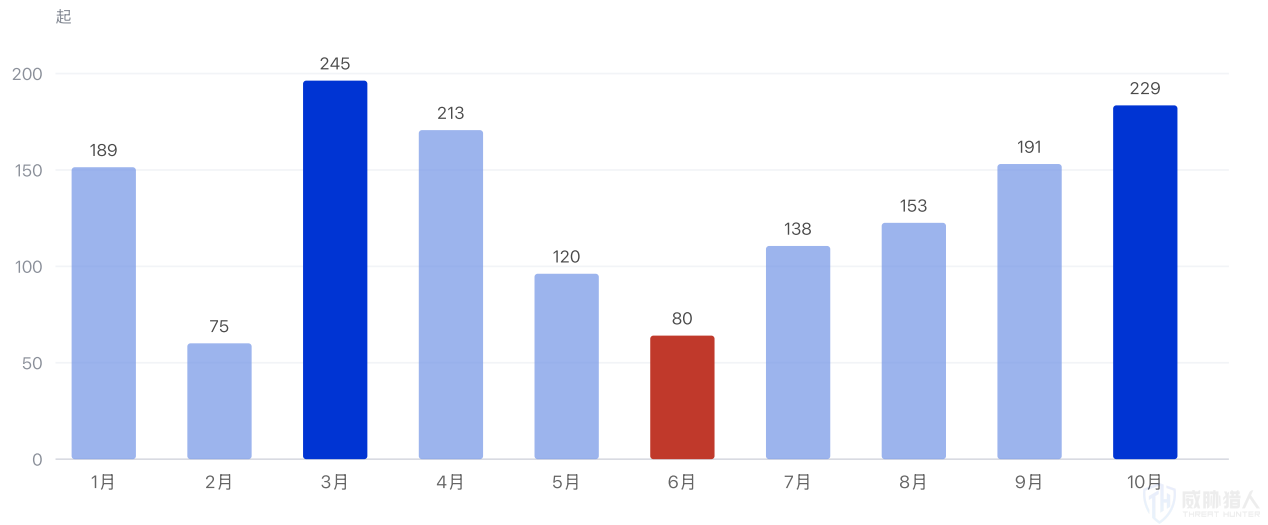


图 20　2026 年 1—10 月消费金融行业数据泄露事件量（起）：呈“双高点”走势，10 月反弹至 229 起逼近 3 月 245 起峰值

答案恰恰相反。时间轴比对与一线调研证实，**6 月异常低点与 2026 年 5—6 月 Telegram 对大批黑灰产频道和群组实施集中封禁在时间上高度重合**。威胁猎人抽取 5 月事件量最高的十个头部数据交易团伙对比发现：6 月十个团伙数据交易量全线下挫，其中六个降

幅超 70%（含三个直接归零）；但同一月份内，一批新群迅速由个位数起量至百起以上规模，承接了原有客流。

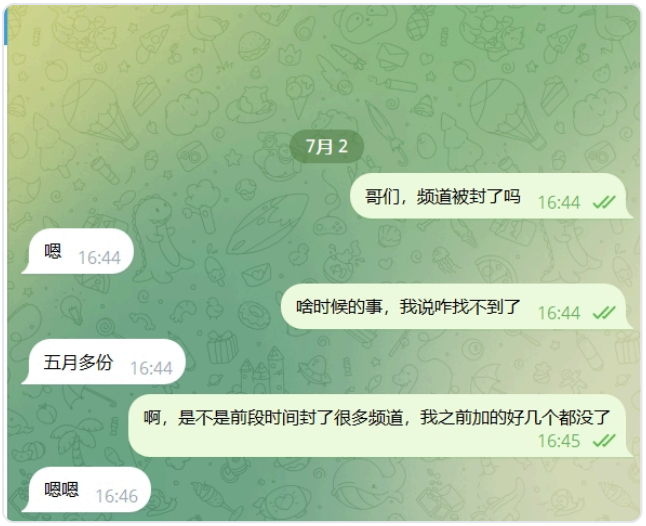


图 21　黑灰产从业者在对话中直接确认原交易频道已遭 Telegram 集中封禁

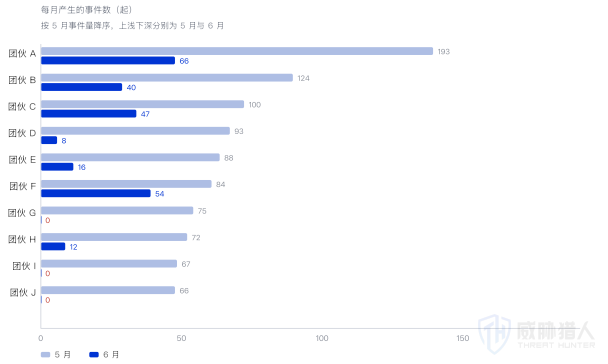


图 22　2026 年 5 月事件量最高的十个数据交易团伙在 6 月全部收缩（统计口径为数据交易事件）

老群停摆与新群起量同步发生，揭示了三层真相：第一，集中封群造成了短暂的阵地重建真空期，形成 6 月的“假性回落”；第二，后续数月黑灰产在持续处置下进入“组建—被封—再组建”循环，且交易模式从“公开报价、按条售卖”加速转向隐蔽的**“私聊详谈”私域化形态**；第三，**7 月起泄露事件量逐月修复，10 月已回升至 229 起**（紧逼 3 月 245 起的上半年高点），上游数据供给不仅未萎缩，反而仍在持续放大。

3.3　通用资源层溯源：同一台服务器承载五类以上涉诈盘口

既然建站系统属于可复用的通用工具，其背后支撑的业务绝不止于假冒催收。威胁猎人从涉案域名回溯至承载源站，发现其中一台服务器共解析到 **287 个域名**（多域可指向同站），已完成页面内容配置的 **12 个站点分属五类完全不同的疑似涉诈业务**：民族资产解冻/虚假扶贫类、全球物联分层拉人头、新基建补贴类、大健康投资类，以及本案的假冒催收入口。



图 23　通用黑产资源层实证：同一台服务器解析 287 个域名、12 个已配置站点，横向服务五类涉诈盘口

一个颇具反常识的细节是：在该服务器 11 月上旬的快照中，假冒催收的页面反而是最简陋的（仅一个 iframe 跳转页，至 11 月 20 日复查才升级为完整 H5 登录页）。这意味着**假冒催收并非该资源运营方的单一主业，而更像是在成熟黑产基建上顺手挂载的一项“外挂业务”**——反过来也印证了：如果防守方只打击前端某一个假催盘口，对底层通用资源层几乎造不成实质伤筋动骨。

3.4　域名池与高敏捷对抗：7 月末备货交汇点与封禁后 6 天三代演进

域名池的运作节奏，是透视对手组织化与长期经营意图最清晰的窗口。通过回溯涉案域名注册日志，威胁猎人还原出极具计划性的**「批量预注册 + 长期静默 + 按需启用」**打法：

业务场景	注册时间	实际启用时间	静默备货周期
消费金融假催收	2026-07-29 06:14—07:04	2026-11-08	约 102 天
汽车召回诈骗	2026-07-29（同一批次）	2026-10-25 前后	约 88 天
某消费分期平台	随打随注册	注册后 4—11 天	4—11 天（临时补注）

表 3　涉案域名注册、静默与启用周期对照

更令人警觉的证据藏在注册时间戳与有效期里：**2026 年 7 月 29 日清晨 06:14 至 07:04 的 50 分钟内，同一批操作横跨两家注册商连续注册了 42 个域名，消费金融催收与汽**

车召回两条线的注册动作逐秒交错插入对方时段，证明二者共用同一采购团队或采购渠道。更关键的是，**提前储备的域名全部购买了 2 年有效期，而事件当天临时补注的域名全为 1 年有效期**——短期“打一枪换一个地方”的零散团伙绝不会为域名多付一年成本，这直接暴露了其长期化、公司化运作的意图。



图 24　2026 年 7 月末战略交汇点：上游数据回升、律师函放量、短信话术退场与域名批量备货同步发生

战略研判

7 月末不是风险平缓期，而是旧形态退场、新武器批量备货的交汇节点；回头来看，6 月低点只是黑灰产换代切换过程中的短暂停顿，而非风险的真正消退。

以单个涉案仿冒站图标特征为种子反查，可迅速扩展出一个庞大的关联域名簇：**84 个完整域名、35 个根域、39 个承载 IP**（页面标题、技术栈与脚本校验值高度一致，按正文特征进一步关联的记录超过 1,000 条）。

在 11 月 8 日至 15 日的短短一周追踪中，这批站点的抗封禁敏捷度展现得淋漓尽致：11 月 8 日 2 个旧域名进入处置后，黑产在 **5 天内秒级替换新域**（11 月 13 日相隔 2 秒注册 2 个新域名，15 日再补注 1 个），**6 天内推动站点完成三代迭代**（第一代基础上线 → 第二代品牌可配置模板 → 第三代新增滑块验证对抗自动扫描），同时将承载主机**从境内云节点整体迁往境外**——换域、升级、出海三管齐下，旨在让被动封禁永远慢人一步。



图 25　涉案仿冒站 6 天三代演进、5 天快速换域及向境外节点迁移时间线（2026 年 11 月 8—15 日）

PART 04

四、跨界外溢警报：当同一套能力撞上“80 万辆汽车召回”

2026 年 10 月下旬起，监测视野中出现了一类表面指向汽车行业、实则精准反噬消费金融客群的新骗局——以“汽车召回”为名的 iMessage 诈骗。它最危险之处不在于手法多新奇，而在于验证了黑灰产将成熟能力“换壳复用到任意热点公共事件”的惊人效率。

4.1 早于舆情的预谋：7 月同批备域、10 月底车主数据切分交付

公众与媒体对“汽车召回短信/iMessage 诈骗”的大规模曝光始于 2026 年 11 月中旬，但威胁猎人情报监测显示，黑灰产的筹备远早于舆情发酵：除了 7 月 29 日与假催收同批交错预注域名外，**10 月 25 日起黑灰产交易市场便已开始密集流通“汽车召回”车主数据包，10 月 29 日全面招揽图文发送机房，10 月 30 日已完成按地区、性别、品牌切分的数据交付。**

日期	一线监测情报原文（敏感信息已脱敏）	环节性质
2026-10-25	「卡 38000　广东人　中国转 **料子汽车召回**」	数据交易
2026-10-26	「卡 20000　广东　邮政转　料子 **汽车召回**」	数据交易
2026-10-29	「**汽车召回图文** 1.3，明天开工来人预约」	发送招揽
2026-10-29	「**汽车召回 im 短信** 能打的机房来，价格全网置顶，有公群可以报备」	发送招揽
2026-10-29	「定制催收 **汽车召回** 教育图文，能打的眼熟机房滴我」	跨场景同发
2026-10-30	「1030-某品牌车主 IM-5001/5002」「1030-广东女 IM-1001」批量数据包	数据交付
2026-10-30	「**汽车车主 IM 刚刚启蒙，好东西趁早**」	推广话术

表 4　2026 年 10 月下旬汽车召回诈骗黑灰产筹备情报时间线

黑灰产行业暗语速查卡（便于理解一线情报）

料子：按特定场景和标签打包出售的目标受害人个人信息数据包。

筛 im / 苹果过蓝：检测号码是否开通并活跃于苹果 iMessage，过蓝即确认可蓝气泡直达。

机房：掌控批量设备与账号、承接群发任务的地下发送服务商。

公群 / 报备：指具备第三方押金担保机制的黑灰产交易群，用于保障上下游结算信用。



图 26　2026 年 10 月 30—31 日，黑产卖家在群内批量交付按地区与性别切分的车主 IM 数据包（已脱敏）

> **外溢本质**
>
> **“汽车召回”从来不是临时起意的剧本，而是黑灰产数据市场里的常备品类。对成熟的模块化黑产而言，稀缺的不是作案能力，而是一个能诱发受害人主动点开链接的真实公共事件。**

4.2　为何穿透力极强：真公共事件 + 真车牌信息 + 假故障理由

与催收场景相比，汽车召回诈骗拥有一项难以复制的“降维杀伤”条件：**它寄生在一场正在全网发酵的真实公共事件之上**。公开信息显示，2026 年 11 月 4 日，国家市场监督管理总局缺陷产品管理中心集中发布了一批涉及多个主流汽车品牌的召回公告，合计召回车辆**超过 80 万辆**。公告发布后的数日内，海量车主正主动查询爱车是否在列，形成了天然的注意力窗口。



图 27　国家市场监督管理总局政务服务平台公开的 2026 年 11 月汽车召回公告列表（黑灰产恶意借用该公共事件窗口）

黑灰产将官方公开召回新闻与手中精准的车主数据拼接，伪造出如下通知文案投向受害人手机：

> 【中国丰田】（重要召回提醒）尊敬的丰田车主：您好！您的车辆（粤：XXXXXX）涉及高田气囊召回，在空气囊展开时，气体发生器可能会有碎片飞出伤及车内人员……中国丰田自 2026 年 10 月 1 日起开高田气囊召回，为了您和家人的安全，请务必重视尽快登入中国丰田官网查询。
>
> —— 深圳反诈中心联合深圳电信 2026 年 11 月 14 日通报的典型诈骗文案（注：系黑灰产冒用品牌名义伪造）

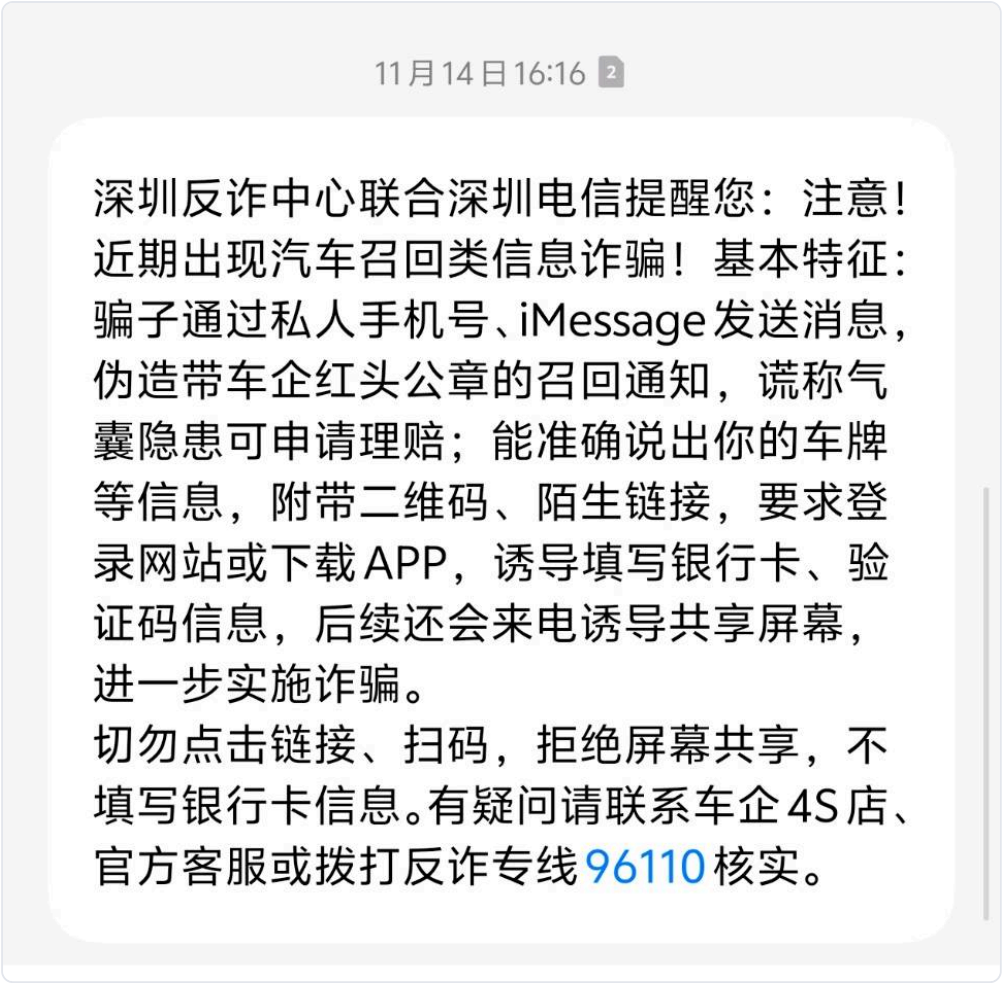


图 28　深圳反诈中心联合深圳电信发布的汽车召回类信息诈骗风险预警（2026 年 11 月 14 日）

拆解该文案可见明显破绽：11 月 4 日官方公布的 80 万辆召回隐患类型为转向、燃油、制动系统及零部件松动，**根本无一项涉及安全气囊**；且文案中“中国丰田”并非规范企业名称，声称的“10 月 1 日起召回”也早于公告日期。但残酷的现实在于：**当受害人一眼核对出自己的车型、车牌完全准确，且新闻里确实正在报道大规模汽车召回时，风险防御链条中最关键的“事件真实性判断”便瞬间失守**，极少有人会再逐条核对故障明细。

4.3　隐藏的金融暗雷：车主与车贷客群重叠，正常申贷演变为消金不良

这起看似属于汽车行业的骗局，为何会直接刺中消费金融机构的痛点？根源在于**汽车消费贷款是消费金融的重要支柱，车主群体与消金在贷客群高度重叠**——处于召回名单中的车主，极可能同时也是放款机构的优质存量客户。

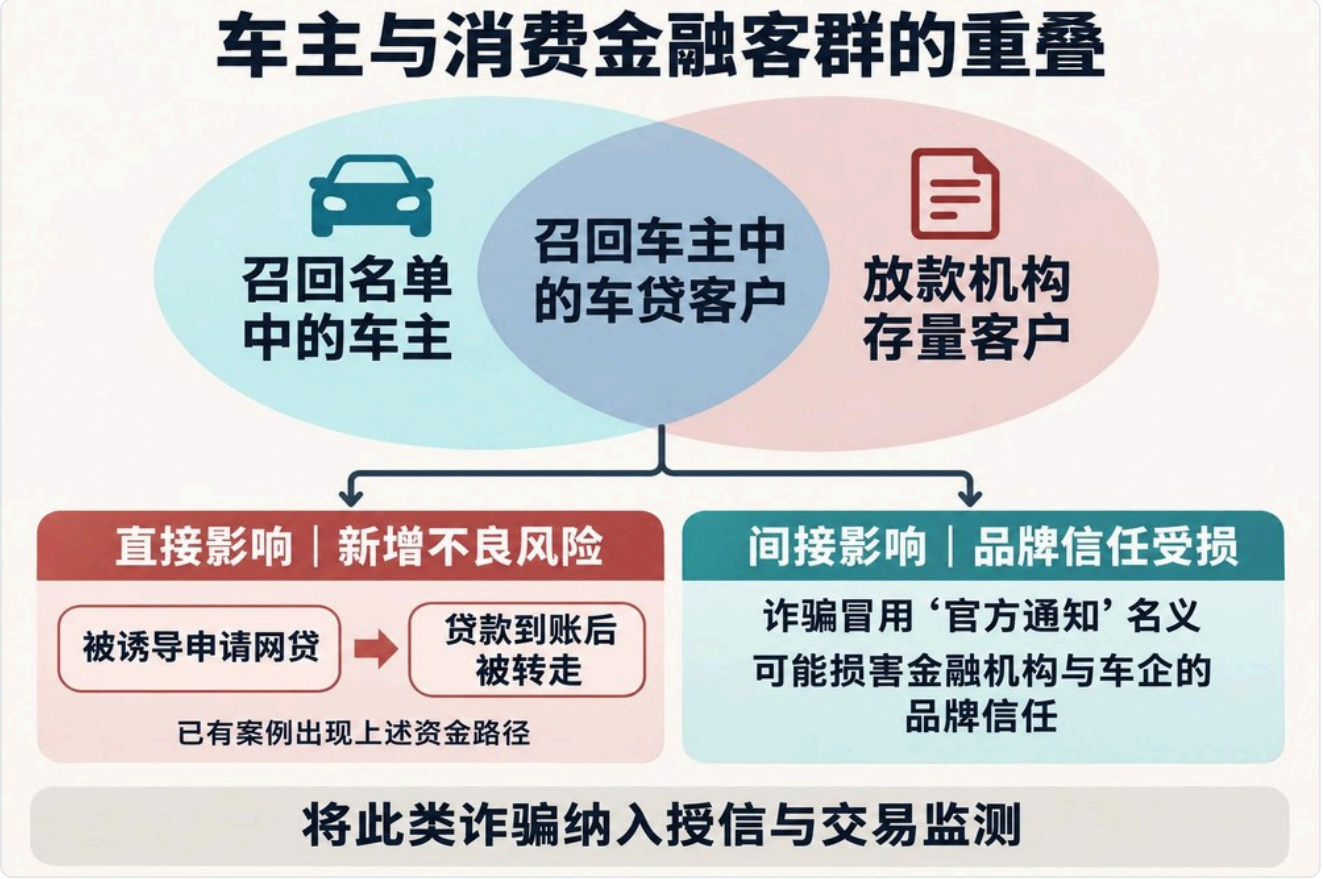


图 29　跨行业风险交集：汽车召回名单与消费金融车贷客群高度重叠

这一重叠正通过两条隐蔽路径向金融机构传导风险：

- **直接金融损失（隐形新增不良）**：实际案例已验证，部分受害人在伪造的“官方召回/理赔/补贴”流程引导下，被诱骗在正规消费金融或网贷平台亲自申请借款，资金到账瞬间即被骗子转走。由于借款人本人资质良好、认证合规、还款意愿真实，**异常仅发生在放款之后，常规授信反欺诈模型几乎完全“失明”**，最终直接沉淀为放款机构的新增不良资产。
- **间接商誉损伤（品牌信任连带受创）**：诈骗借“官方召回通知”精准点名车牌与车型，一旦受骗，被冒用的车企与涉事金融机构往往同步承受客户投诉与品牌信任损耗。

更深远的意义在于警醒所有行业：今天这套由“苹果过蓝数据 + iMessage/无码上门快递 + 预注域名池 + 高仿 H5 模板”组装的能力瞄准了汽车召回，明天只要出现新的社会热点（如社保退费、保险理赔、航班变动、教育退费），黑灰产就能在数天内完成换壳复用，向下一个高价值客群发起精准打击。

研究声明与合规说明：本报告由威胁猎人基于 2026 年 1—11 月持续监测获取的公开风险情报、黑灰产对抗趋势及典型涉诈基础设施特征整理而成，面向金融借贷、物流快递、汽车行业合作伙伴及社会公众公开发布。报告中涉及的黑灰产自述规模、交易报价均源自公开情报监测原文，未经核实；文中提及的正规快递服务、官方召回公告及真实律所名称均系被黑灰产恶意冒用或滥用，与相关正规主体无关。个人隐私、非必要品牌标识及待核实技术署名线索均已按公开发布合规要求作脱敏处理。