CAICT 中国信通院

移动数字广告与互联网反欺诈蓝皮报告

中国信息通信研究院泰尔终端实验室

2021 年 5 月

版权声明

本报告版权属于中国信息通信研究院，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国信息通信研究院”。违反上述声明者，编者将追究其相关法律责任。

编制组人员名单

参编单位：中移互联网有限公司、中国联合通信有限公司、中国电信集团云网安全科技有限公司、北京智慧易科技有限公司、石溪信息科技(上海)有限公司、秒针信息技术有限公司、北京数美时代科技有限公司、每日互动股份有限公司、北京热云科技有限公司、北京腾云天下科技有限公司、小沃科技有限公司、杭州朝霞网络科技有限公司、上海游昆信息技术有限公司、北京国双科技有限公司、北京微方程科技有限公司、同盾科技有限公司。

起草人员：王景尧、吴荻、关涛、张少游、陈颖、林荣波、王升富、周磊、闫辉、张旭、李志强、刘力泉、白宝龙、赵义、周芳、徐韵、辛秀、康洁、陶冶、丁宏伟、王颖、闫定国。

前　言

自移动互联网诞生以来，对于真实流量的争夺一直是各方关注的焦点。随着技术的不断演进，以伪造真实流量为依托的黑灰产行业快速发展，双方在广告投放、流量运营、线上交易等各环节互相博弈，使得移动互联网行业健康有序发展面临巨大挑战。

首先，**从国家宏观层面看，**数字经济已成为我国经济发展的重要战略支柱。移动互联网流量作为数字经济发展的重要依托和战略要素，其健康有序发展已经成为了国家战略层面的共识。

其次，**从行业需求变革看，**移动互联网行业的外部环境和基础设施发生了巨大的变革。**其一，**作为流量甄别的基础服务和共性能力，由智能终端和操作系统主导的设备标识体系将不在适用。国内厂商上线的去中心化的标识无法验证真伪。这给移动互联网流量标识中心化验证，反欺诈，特别是广告投放相关流量甄别带来了巨大挑战。**其二，**以手机号码及卡标识为主导的用户标识体系将不再适用。导致，在交易、支付等反欺诈关键环节无法流量识别和身份验证。**其三，**我国普遍依赖于对样本数据进行小规模抽样作为流量投放的效果验证和结算依据。然而，当前监测方的样本数据有限，匹配量少，难以有效、公平的给出投放效果。同时，不同平台之间的数据标准不统一、不透明，样本数据体量相差悬殊，对数据缺少互相认可，广告主、媒体、数据服务商、第三方监测等各方参与者之间存在共识障碍。

最后，**从企业面临问题看，**流量反欺诈呈现木桶短板效应，同

时黑灰产业链呈现抱团效应。一旦互联网平台出现了反欺诈漏洞，企业损失巨大，前期投入化为泡影，同时各种黑灰产团伙便会蜂拥而上。轻则导致互联网平台伤筋动骨，重则直接倒闭。而由于法律法规和监管的滞后性，互联网欺诈受到的威慑和惩戒又往往不足，导致互联网反欺诈压力不断增大。

本蓝皮报告将从以上三个方面为出发点，全面梳理我国移动互联网流量现状、流量反欺诈应用场景、流量反欺诈核心技术及发展趋势，对黑灰产业链进行全面梳理，并在业界首次提出企业反欺诈能力建设体系，并给出相关意见和建议。

目 录

一、 移动数字广告与互联网反欺诈现状及面临挑战.....1

(一) 中国互联网发展现状.....1

(二) 移动数字广告行业发展现状.....1

(三) 互联网反欺诈现状.....2

(四) 行业面临的共性问题及挑战.....5

(五) 蓝皮报告愿景及目标.....6

二、 移动数字广告与互联网黑灰产业链概述.....6

(一) 黑灰产业链发展背景.....6

(二) 黑灰产业链发展现状.....8

(三) 黑灰产业链组成结构.....9

三、 移动数字广告发展态势.....18

(一) 宏观概述.....18

(二) 市场监管将更加清晰化.....20

(三) DMP 市场将快速发展.....21

(四) 社交广告将成投放主流.....23

(五) 2020 手游行业投放特征.....23

(六) 2020 非手游行业投放特征.....28

四、 互联网欺诈场景及态势.....31

(一) 互联网欺诈场景.....31

(二) 互联网欺诈手段及发展态势.....44

五、 互联网反欺诈体系.....46

(一) 反欺诈体系建设原则.....46

(二) 反欺诈体系的构成.....47

(三) 反欺诈体系团队配备.....51

六、 移动数字广告与互联网反欺诈技术.....56

(一) 行业级匿名设备元服务.....57

(二) 行业级匿名用户元服务.....65

(三) 多策略融合的策略体系 69
(四) 全生命周期互联网反欺诈模型 73
(五) 互联网反欺诈技术架构 74
七、 互联网反欺诈发展趋势 85

图 目 录

图 1 2020 年国内欺诈流量流向行业分布 3
图 2 黑灰产业链全景视图 10
图 3 2020 年国内黑卡组成分布 12
图 4 ios 作弊工具分布 14
图 5 安卓作弊工具分布 15
图 6 IP 类型分布 16
图 7 模拟器分布 17
图 8 移动互联网广告行业相关法律法规及规范性文件 21
图 9 DMP 平台 22
图 10 2015-2025 年 DMP 市场规模（单位：亿） 22
图 11 2019-2020 年广告主对移动广告投入比例 23
图 12 2020 年手游买量激活率趋势 24
图 13 2020 年手游买量市场各月付费设备占比走势 25
图 14 2020 年手游买量市场各月及首日激活且付费设备数对比 26
图 15 2020 年投放素材及新增率对比 27
图 16 2020 年投放创意组 Top500 及占比分布 28
图 17 2020 年应用类 App 投放产品数 29
图 18 2020 年应用类 App 各类型投放产品数占比 29
图 19 2020 年 A/B 测试试验行业分布 Top5 30
图 20 2020 年应用类 App 各类型产品新增率 Top5 31
图 21 互联网欺诈主要场景 32
图 22 羊毛党欺诈过程 33
图 23 常见的机刷设备 36
图 24 木马刷原理图 36
图 25 流量劫持原理图 37
图 26 互联网裂变欺诈示意图 40
图 27 网络赌博欺诈示意图 43
图 28 反欺诈体系示意图 48

图 29 反欺诈技术发展的五个阶段 56
图 30 卓信 ID：多策略融合的设备指纹生成策略 58
图 31 卓信 ID 的特点及优势 59
图 32 卓信 ID 全场景的应用能力 59
图 33 卓信 ID 的生成及应用策略 60
图 34 匿名用户标识体系架构 66
图 35 生物探针的优势 71
图 36 多策略融合欺诈风险识别 72
图 37 多策略融合的欺诈数据处理架构 73
图 38 全生命周期反欺诈模型 74
图 39 反欺诈技术架构 75
图 40 反欺诈画像引擎 78
图 41 实时规则引擎 78
图 42 规则引擎结构及执行原理 79

表 目 录

表 1 欺诈造成单账户年均损失和总损失数据预测.....8
表 2 欺诈造成损失占 GDP 比例.....9

CAICT 中国信通院

一、移动数字广告与互联网反欺诈现状及面临挑战

(一) 中国互联网发展现状

2020 年，中国移动互联网用户规模达 13.19 亿，占全球网民总规模的 32.17%；移动互联网接入流量消费达 1220 亿 GB，同比增长 71.6%；电商交易规模 34.81 万亿元，同比增长 6.7%，直播电商等新业态爆发式发展，农村电商迅速崛起，电子商务交易规模已连续多年占据全球电子商务市场首位；网络支付交易额达 249.88 万亿元，移动支付普及率位于世界领先水平；全国数字经济增加值规模达 35.8 万亿元，占 GDP 比重达 36.2%，位居世界第二位。2020 年，中国光纤网络全面覆盖城乡，光纤用户占比达 93.1%，位居世界第一。5G 基站建设数量已超过 48 万个。

同时，网络直播等新业态爆炸式增长，满足疫情期间网民生活需求，网络直播用户规模达 5.62 亿。全国 31 个省区市互联网发展情况的评估结果显示综合排名前 10 位分别是北京、广东、上海、江苏、浙江、山东、四川、福建、天津、重庆。

“互联网+”持续助推传统产业转型升级，各互联网细分领域市场规模稳定增长，行业环境不断优化，新产品、新业态层出不穷，服务模式不断迭代演进，市场格局洗牌革新速度加快。

(二) 移动数字广告行业发展现状

全球商品经济繁荣的同时，广告行业也进入了蓬勃发展：随着科学技术的研发与应用，广播、电视、计算机、移动终端等电子化

产品迅速普及，媒体形式呈现多样化趋势，广告内容也日趋丰富多彩。当前，全球广告市场规模超过了 5600 亿美元。其中，中国市场规模占据了 16%，为 875.3 亿美元，位居全球第二。

全球数字广告市场头部化很明显，巨头媒体占比 76.51%，其中，谷歌 31.1%的市场份额位列第一。中国互联网数字广告以字节跳动、腾讯、阿里巴巴、百度、京东等企业排在前列，占据了整体数字广告市场份额 70%以上。

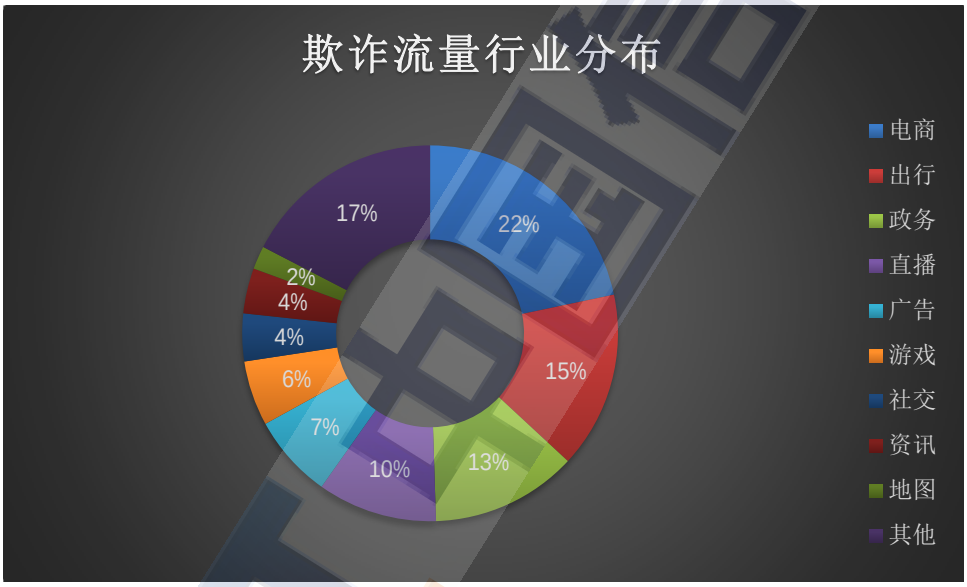
数字广告的蓬勃发展和可观利润也导致了广告流量作弊的广泛存在。整个 2020 年期间，国内互联网假量占比连续多月超过 30%，直接和间接造成的经济损失超过 1500 亿元。

同时，国内安卓生态提供的去中心化的 OAID 方案也无法对设备指纹进行验证校准。行业普遍采用的用户身份标识 IMSI，也随着操作系统升级而无法获取。整个行业面临着新的挑战与变革，亟需引入新的技术解决方案。

(三) 互联网反欺诈现状

移动流量在现代移动营销领域是核心要素，特别是在金融和商品交易领域。近年，70%缺乏防御技术能力的互联网 APP 遭受过不同程度的黑产欺诈，在被黑产常年紧盯的电商领域，“黑产”已经非常成熟的欺诈技术，渗透账号注册、身份伪造、宣传导流、借贷支付多个环节。黑产从业人员已突破 500 万，涉及金额达千亿。总体而言，数字金融、电商、社交媒体是欺诈行为高发的“重灾区”。

整个市场流量“移动化”的背景下，不论是传统线下业务还是原本由 PC 互联网承载的业务，都在逐步向移动端拓展。而其在整个移动互联网业务中，数字金融和电子商务是两个非常重要的领域，与广大居民的日常生活息息相关。与此同时，以上述两个领域为代表的移动流量所涉及的欺诈风险也越来越严峻。在整个互联网行业中欺诈流量无处不在，同盾研究数据显示 2020 年国内欺诈流量流向行业分布如下：



数据来源：同盾研究

图 1 2020 年国内欺诈流量流向行业分布

电商行业：一方面，受疫情隔离影响以及巨头电商平台对下沉用户群的覆盖力度增强，各大电商平台 GMV 屡创新高，各种营销活动层出不群（茅台秒杀、大额优惠券补贴、新手活动等），而与之伴随的是整个以欺诈流量为代表的完整黑灰产业链的枕戈待旦。另一方面，比价平台对于各家电商的持续价格爬虫流量也日益水涨船高。

出行行业：根据全网情报监控，出行行业的主要欺诈流量都流向了航司和 12306 网站，OTA、二级代理商对于航司航班价格接口持续的查询，极大增加了航司的服务器压力同时，导致航司需要向中航信支付高额的费用；对于 12306 则是形形色色的抢票软件衍生的巨大爬虫流量，2020 年受疫情影响虽然整个出行行业欺诈流量同比去年有所下降，排名仍然高居第二。

政务网站：近年来越来越多的公司，利用国家公共平台的信息作为其商业化产品的重要数据来源（大数据征信产品，企业信息查询，车辆信息查询产品等），辅助以良好的交互体验、产品包装实现商业化的目的。这样大规模的数据来源需要大量的机器爬虫来提升入库的效率，失信人员名单查询系统、中国裁判文书网、失信被执行人查询、中国及多国专利审查信息查询、商标查询、车辆违章信息查询系统、国家企业信用信息公示系统、全国组织机构代码管理中心等网站为重灾区。

直播行业：除了传统秀场和游戏直播的主流平台外，2020 年电商直播的持续发酵吸引了更多的流量，以抖音、快手为代表的短视频平台与传统电商形成分庭抗礼之势，欺诈流量在直播行业绝大部分流向虚假人气、点赞关注的场景。

广告行业：虚假流量往往伴随着企业主和广告渠道的结算方式，不论是应用商店的下载，还是信息流广告 CPA\CPC\CPM 的结算方式，都有大量虚假流量的注入来骗取企业主的投放费用。

游戏行业：由于疫情的原因，2020 年游戏行业也迎来了流量的

爆发，同时更多的欺诈行为也充斥其中，主要体现在渠道下载刷量、外挂以及模拟器挂机。

社交行业：作为用户交互最频繁的行业，账户是社交最重要的一环，欺诈流量也是围绕批量注册、养号以及垃圾广告等场景。

资讯行业：主要集中在门户新闻网站内容爬虫、网赚平台的虚假流量。

地图行业：越来越多的应用和场景都需要获取地理位置来辅助于业务决策,所以地图厂商的公开接口越来越多频繁的被脚本调用。

(四) 行业面临的共性问题及挑战

目前，移动数字广告和流量反欺诈问题都面临相关共性问题及挑战。具体原因主要有:

首先，指纹体系目前以智能终端厂商为主导。当前，以厂商为主体的指纹方案已在行业内广泛应用。由于其生成受限于智能终端厂商，故各方标识体系难以互联互通，导致在广告效果监测、移动互联网反欺诈等行业各方需要对接多方标识,增加了对接的复杂度。

其次，我国普遍依赖于对样本数据进行小规模抽样作为流量投放的效果验证和结算依据。然而，当前监测方的样本数据有限，匹配量少，难以有效、公平的给出投放效果。同时，不同平台之间的数据标准不统一、不透明，样本数据体量相差悬殊，对数据缺少互相认可，广告主、媒体、数据服务商、第三方监测等各方参与者之间存在共识障碍。

最后，缺乏行业基础共性能力及解决方案。目前，为解决上述问题，行业内各方都推出了自身的设备标识解决方案或第三方监测方案。但由于商业化的考虑，各指纹无法进行有效的互联互通。使得行业缺乏有效统筹，各自为战，导致行业运转效率极大降低。

(五) 蓝皮报告愿景及目标

本蓝皮报告旨在通过分析当前移动广告和流量反欺诈现状，调研当前互联网标识体系、第三方监测及反欺诈技术的发展趋势，暴露当前欺诈技术和手段可能对企业和个人造成的威胁及损害，提出有针对性的反欺诈措施和解决方案，为行业输出共性能力，最终达到净化互联网环境的目标。

二、 移动数字广告与互联网黑灰产业链概述

(一) 黑灰产业链发展背景

互联网黑灰色产业链是指基于互联网进行的各种黑色、灰色经济活动，并在内部专业分工和供需关系基础上的各个利益相关部分组成的网络型产业链整体。

其中，“互联网黑产”(简称黑产)，是指通过互联网利用非法手段获取利益的行业，比如：利用互联网漏洞实施攻击牟利等。“互联网灰产”(简称灰产)则是指游走在法律法规等不明确的边缘地带，通过打“擦边球”等方式不当获利，如薅羊毛、广告流量造假等。

目前，网络黑灰产业链主要可以分成以下几类：

第一，恶意刷单。广告公司付款请人假扮顾客，用以假乱真的

消费方式提高产品的销量获取好评吸引顾客。分为机器刷、人刷。机器刷指利用群控等设备统一的大量刷单，真人刷单就是雇人兼职刷单。

第二，营销欺诈，俗称薅羊毛。2014 年，广州新成立一家互联网金融公司，为了吸引消费者购买自己理财产品，发行了价值 2 个亿的各类优惠券，被一个 5000 人的“羊毛党”团队抢走。仅仅不到半年的时间，公司宣告倒闭。

第三，恶意广告产业链。通过展示作弊、安装/激活作弊、应用内行为作弊、虚假流程作弊等手段，快速消耗广告主的广告预算，让广告主的广告推广投资回报大大降低。

第四，恶意调用。在企业的某些新功能模块上线之后，出现短信接口被恶意访问调用的情况，增加企业短信服务费，影响企业服务器的带宽与正常请求等。

第五，金融欺诈产业链。由黑市流量作为源头，围绕 P2P、现金贷诞生的上下游产业包括第三方数据商、弹窗广告联盟、第三方催收，还有一拥而上的信贷欺诈、撸贷者、羊毛党等。贷款诈骗有一个完整的黑产链，在上游，有数据、个人信息供应商；在中游，有围绕诈骗活动的一系列网站和 APP 开发、伪基站、VPN 供应商、模拟器供应商等；在下游，有帮助洗钱的团伙。

第六，恶意竞品爬虫。互联网上各种爬虫肆虐，很多企业的核心内容、商品数据都被竞争对手的爬虫盗走，导致搜索引擎排名下降，价格策略失效，给企业造成重大损失。

第七，恶意代码。恶意代码是一种程序，它通过把代码在不被察觉的情况下镶嵌到另一段程序中，从而达到破坏被感染电脑数据、运行具有入侵性或破坏性的程序、破坏被感染电脑数据的安全性和完整性的目的。

第八，账户盗号/恶意注册/撞库攻击。通过账户盗号和撞库攻击，非法获得互联网用户的账号信息，造成用户隐私泄露，非法转移账户内的财产；通过恶意注册进行水军攻击，发布恶意广告，在热门的内容中嵌入非法信息。

第九，恶意占座。恶意占座是航空公司、票务公司等公司普遍面临的风险问题。自有平台和测试网站、代理公司的第三方接口上以及整个业务流程中存在漏洞，网络黑色产业从业者能瞬间抢走官方的低价票，并他用过加价出售给旅客来谋取暴力。

(二) 黑灰产业链发展现状

据中国信通院泰尔终端实验室发布的《移动数字金融与电子商务反欺诈蓝皮报告（2019 年）》预测显示，从 2019 年到 2022 年，互联网欺诈将维持持续增长态势，表 1 展示了未来几年欺诈造成的单账户年均损失和总损失预测数据。

表 1 欺诈造成单账户年均损失和总损失数据预测

年份	疑似欺诈者账号数量（万）	单账户欺诈造成年均的损失（万元）	欺诈造成的总损失（亿）
2019	1250	3.09	3870
2020	1310	3.93	5150
2021	1740	3.41	5940
2022	2300	3.08	7100

数据来源：中国信息通信研究院

如果 GDP 保持在 6.5%的速度发展，则按上述预测，从 2019 年到 2022 年，互联网欺诈可能造成的损 失占 GDP 的比例如表 2 所示。

表 2 欺诈造成损失占 GDP 比例

年份	2019	2020	2021	2022
欺诈造成的损失占GDP的比例	0.40%	0.50%	0.55%	0.61%

数据来源：中国信息通信研究院

实际情况中，还存在大量未被发现的欺诈账号和欺诈行为，同时随着我国数字经济的发展，新的业务和新的欺诈形式也可能同时出现。因此，在实际中欺诈造成的损失很可能比本文推算的更大。

(三) 黑灰产业链组成结构

互联网黑灰产业链上、下游分工明确，配合密切，形成了完备的产业链。经过研究分析发现，互联网黑灰产业链从上游到下游依次可以分成黑产情报信息非法获取、信息流转加工处理、非法变现套利三个核心环节。互联网黑灰产业链全景视图如下图所示。

来源：公开资料整理

图 2 黑灰产业链全景视图

1. 黑产情报获取

对于当今组织化规模化越来越强的黑灰产团伙来说，挖掘攻击情 报往往是获利的第一步，团伙中会有专门角色负责欺诈线报收集，把 相关活动的时间范围、收益变现形式等信息准确、及时地在团伙内传达清楚，线报人员获取情报的来源通常包含黑灰产论坛、信息分享 QQ/微信群、电报群等。

信息获取后，就会有专门的业务渗透人员和脚本人员，了解分析清楚产品逻辑、必需资源和必要工具/脚本，厘清活动性质，如是新账号首单还是老账号拉活，是否涉及地域性，是否涉及绑卡等。进而基于前期分析后做出相关操作决策，如充钱，屯号等，以确保在活动开始前做好准备。

2. 信息流转加工处理

信息流转加工处理由两部分组成，一部分是核心资源，通常包括网络账号、网络 IP 资源和设备资源。另一部分是黑产工具，黑产工具一般指用于自动化加工、处理黑产信息的工具。

3. 核心资源

（1） 网络账号

用户互联网欺诈的账号来源一般由两种，即注册和盗号。

批量恶意注册需要批量手机号短信验证码，此类黑产分为几代:

第一代:虚拟运营商手机号，即 170、171 开头的手机号。虚商从 2013 年发展至今，已有阿里、京东、苏宁等几十家机构拿到了虚 拟运营商牌照。虚拟卡主要应用在临时场景，办卡门槛较低，因此受 到了黑灰产网络欺诈的青睐。尽管其成为较常见的黑产手机号来源，但因为识别简单，防御起来门槛较低。

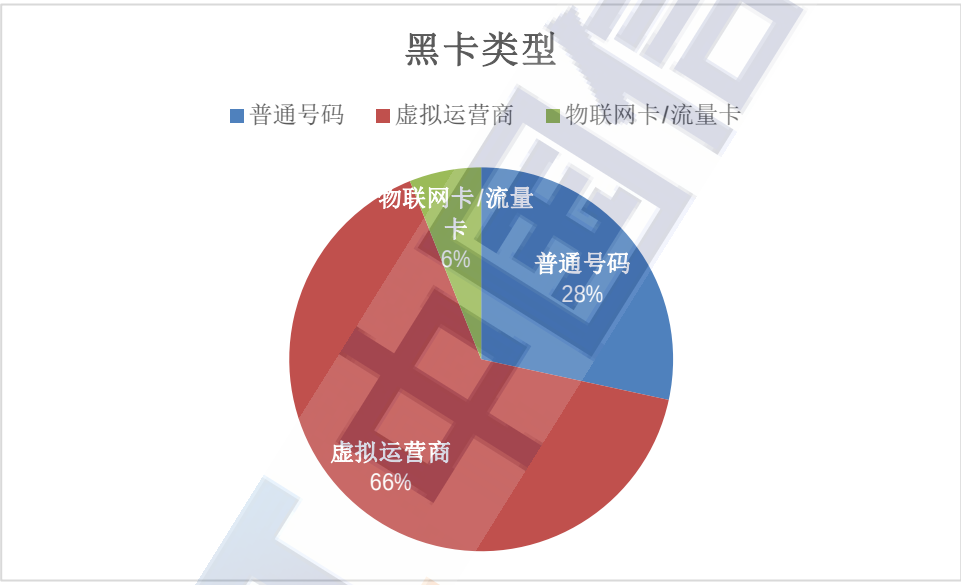
第二代:海外、传统运营商流出的黑手机卡。其往往是处于欠费半停机状态(只能收短信)或 0 月租的号码。当前，越来越多的企业启用语音验证码，也出现不少质量较高的手机卡，可以接听语音。这 类传统黑卡需要配合历史作恶黑库来识别，防御门槛稍高，但效率存 疑。

第三代:注册时使用的手机资源还需要提升接码效率，猫池+卡池的工具组合应运而生，猫池负责解码接短信，模拟正常手机的功能，卡池为猫池提供足够卡源，实现全天无人工值守自动随机换卡，

猫池和卡池的关系有点像步枪和弹夹。该类方案成熟度较高，但成本较高。

第四代:运用一、二代的卡资源，再结合三代的工具，就组成了一体化的接码平台。一体化接码平台可承接各类运营商的手机号，同 时提供专门客户端和高并发 API 接口，采用会员充值制，给黑灰产注 册欺诈提供了强有力的支持。

同盾研究数据显示 2020 年国内黑卡组成分布如下:



数据来源：同盾研究

图 3 2020 年国内黑卡组成分布

在整个黑卡类型分布中，虚拟运营商虽然目前开放的号段不多，贡献却超过 60%，原因有两点：一，虽然是三大运营商下发号段，但是销售管理属于虚拟运营商自己把控，入网门槛相对较低，给了黑产可乘之机。二，真实用户占比逐年上升，业务方无法根据号段直接设置风控规则。

第二个号码来源是盗号，此类黑产同样也在不断变迁:

第一代:木马方式盗号。该产业链有明确的分工，有人设计木马程序，有人专门传播/控制木马，有人收集梳理盗取的号码库，有人负 责有价值的号码变现，即“洗库”。随着移动互联网大潮来临，很多 厂商转型移动端。

第二代:号码及票据方式盗号。当企业级服务的 WEB 端存在时，可利用 XSS 或 CSRF 等漏洞，使得 COOKIE 中登录票据等私密信息的泄漏。在此类登录票据的有效期内，黑灰产可以利用此号码+票据进行盗号，并引发出多次漏洞、蠕虫恶意传播事件。

第三代:前述两代是通过漏洞攻防安全技术作恶，技术门槛高，且对抗激烈。第三代盗号，瞄准了安全链条中最薄弱的一环，人。当 前，基于社会工程学的攻击层出不穷，花样迭出。盗号是社工的重灾 区，无论是批量弱密码扫号还是仿造得惟妙惟肖的钓鱼网站盗号，都 是成本较低且很难彻底防御的攻击手段。

第四代:撞库盗号。黑灰产利用漏洞进行拖库，结合人性弱点(每个人平均能记住的密码不超过 3 个，复用情况普遍)，用手里的“库”进行暴力“撞库”成了盗号的最省力方式，且性价比很高。

（2） 设备资源

用户设备是承载账号的硬件载体，模拟/更换设备是黑灰产的基本方法，分为以下几代:

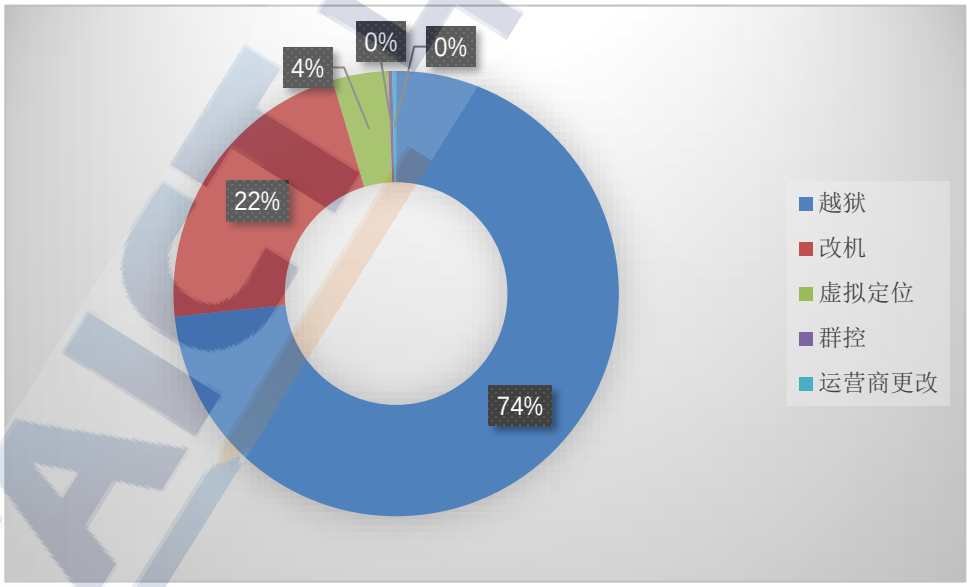
第一代:基于协议破解的假设备。成本较低，但因无设备唯一标识，因此防御方法也相对简单。通过设计设备唯一标识并进行检测，

即可事半功倍。防御重点主要在运营维护客户端版本，兼容历史包袱。

第二代:安卓手机模拟器。一台 PC 往往可以同时执行 15-20 个 模拟器。但该类方法门槛较低，可通过设备风险识别等手段可以较轻 松识别。

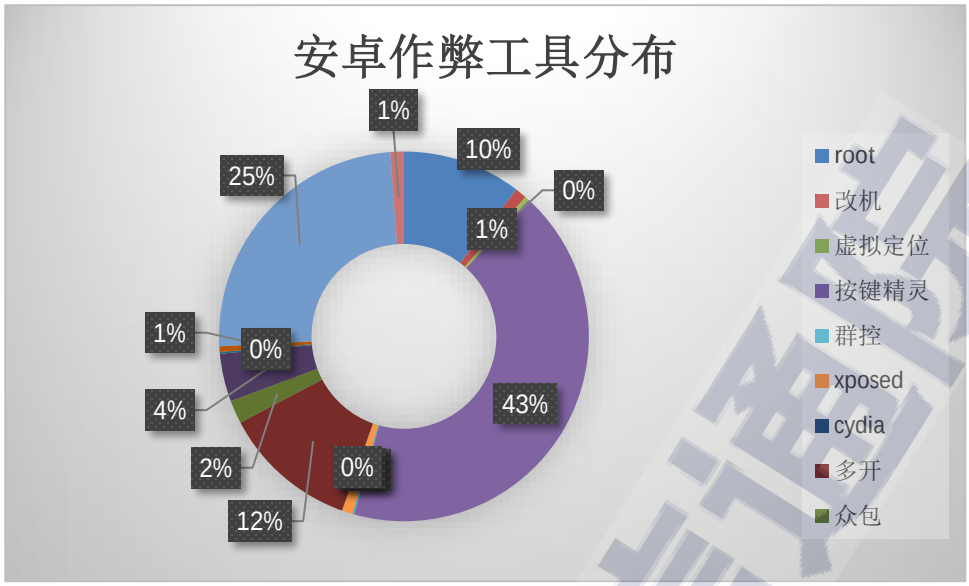
第三代:真手机设备篡改或多开。该类方法基于原生移动环境，通过改机工具来实现模拟换设备操作。当今风控厂商的设备风险识别也基本可以识别到，门槛稍高。

第四代:设备农场。随着羊毛党收益等不断上涨，可以支持到黑灰产启用成本更高的作恶方式，真机设备农场就是典型案例，也即俗 称的手机墙。黑灰产从二手货交易平台回收旧手机，统一刷机，结合 三代的改机工具，批量作恶，给企业风控带来较大威胁。



数据来源：同盾《2020 反欺诈年度报告》

图 4 ios 作弊工具分布



数据来源：同盾《2020 反欺诈年度报告》

图 5 安卓作弊工具分布

（3） 网络 IP 资源

用户 IP 是网络接入载体，更换 IP 也是黑灰产必修课，手法分为 以下几代:

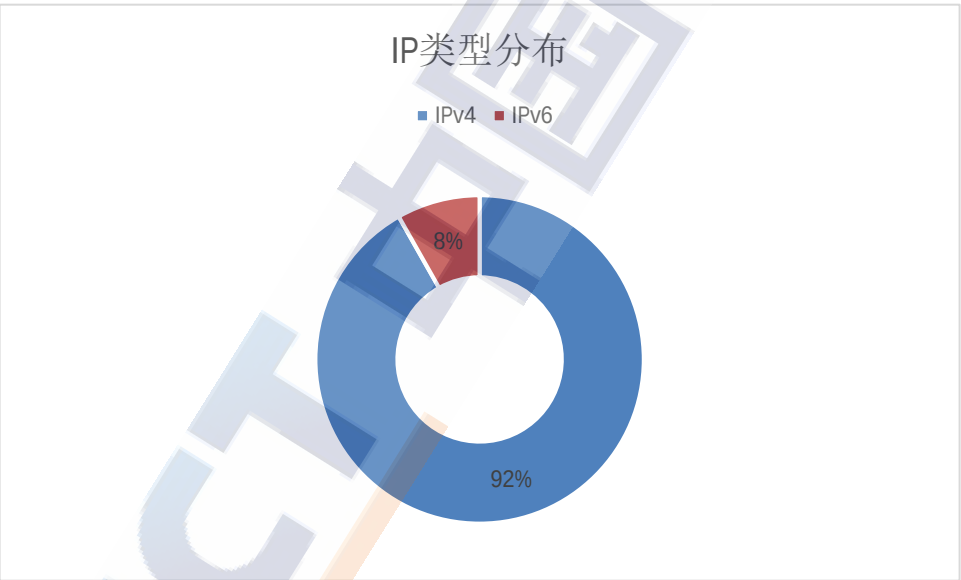
第一代:ADSL 拨号。通过一根网线反复拨号，可以拨到多个相邻 IP 地址段，但无法跨越更大的网段和地域。所以 ADSL 拨号虽然容 易上手，但防御较容易。

第二代:VPN 代理。较传统的代理架设模式，VPN 私密性较好，部分场景用于翻墙，可模仿跨城市的 IP 网段，用初级黑库+行为逻辑 可以进行防御。

第三代:专门用于黑灰产的代理服务器。包含扫描代理、肉鸡代理、私搭代理平台服务等形式，IP 和城市数量较多。但因为鱼龙混杂， 良莠不齐，攻击维护成本较高。

第四代:VPS 混拨。远程在 VPS 云服务器上架设多根网线，软

件实现多线混拨，远程控制 VPS 服务器拨号可以跨城市，速度快，稳定性好，稍有规模的 VPS 拨号厂商，可支持几十个省份上百个城市地域几十万 IP 的混拨更换，是目前黑灰产使用的主流换 IP 模式。同盾研究数据显示：随着全球 IPv6 的逐步普及，在整个 2020 年有近于 8%的攻击涞源为 IPv6 地址，IPv6 逐渐开始被黑产利用，黑产对于 IPv6 的使用，势必在未来的 1-2 年内将攻防态势拉到一个新的高度，因为这意味着黑产将拥有比起 IPv4 来说取之不尽的资源池；行业多年积累的风险库以及丰富的标签将失去作用，我们需要重新构造。



数据来源：同盾《2020 反欺诈年度报告》

图 6 IP 类型分布

4. 黑产工具

（1） 打码平台

打码平台，验证码是人机识别的标配，那么自动破解验证码的

打 码平台服务也成了必需品,从人工打码到深度学习自动识别破解验证 码，效率和收益都在不断提升。

（2） 脚本

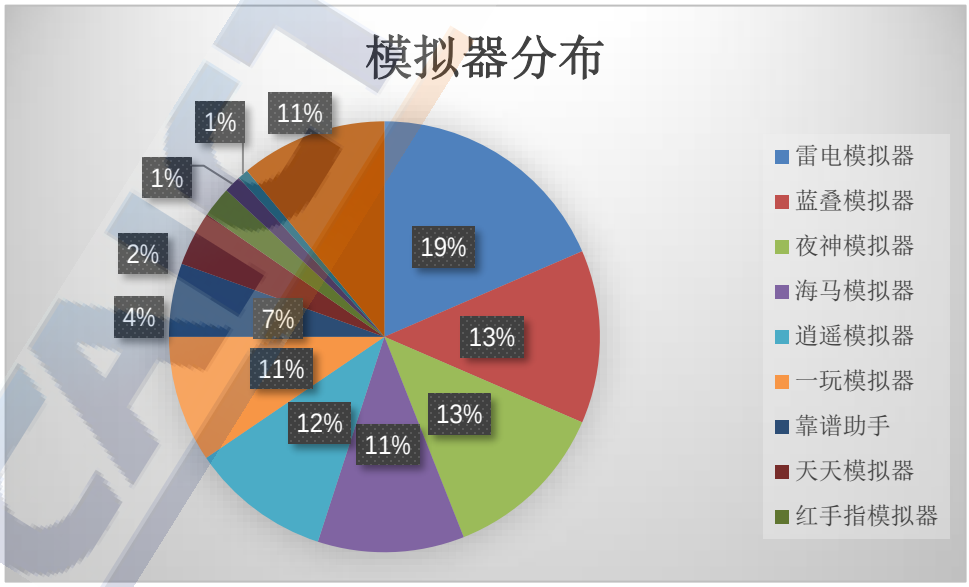
按键精灵+脚本，看似简单，但实际上是流程控制的核心，根据 产品业务流程，设计脚本，通过按键精灵来模拟用户操作，成本低又 能加入各种随机因素保证模拟质量。

（3） 基础工具

资源与基础工具，组成各作恶场景的业务工具，如撞库工具、引流脚本、羊毛软件，把所有核心资源串联起来，提升作恶效率。

（4） 模拟器

模拟器是能在电脑上模拟手机操作系统，并能安装、使用、卸载手机应用的软件，它能让你在电脑上模拟手机整个操作的过程。



数据来源：同盾《2020 反欺诈年度报告》

图 7 模拟器分布

（5） 改机软件

改机软件是一种可以安装在移动端设备上的 APP，能够修改包括手机型号、串码、IMEI、GPS 定位、MAC 地址、无线名称、手机号等在内的设备信息，通过不断刷新伪造设备指纹，可以达成欺骗厂商设 备检测的目的，使一部手机可以虚拟裂变为多部手机，极大地降低了 黑灰产在移动端设备上的成本。

（6） 猫池

猫池是将相当数量的 Modem 使用特殊的拨号请求接入设备连接在一起，可以同时接受多个用户拨号连接的设备。恶意用户可以利用 一台猫池使用多张手机号进行业务操作。

5. 变现及套利

黑灰产在实时互联网欺诈活动成功后，需要将获得非法物品进行变现套利，在黑灰产团伙中，有丰富人脉资源的角色会成为变现套利的中间商，赚取差价。变现套利的方式一般有直接提现，通过暗网平台倒卖变现、黑产服务数据售卖变现等方式。

三、移动数字广告发展态势

(一) 宏观概述

随着 2020 年新冠疫情防控步入常态化，数字经济迎来重大发展

机遇。从需求端的角度来看，除原有的移动互联网核心使用人群外，受疫情影响，“银发一族”、“下沉人群”等被动触网，疫情后用户习惯得以延续，线上生活方式得到发展；从供给端的角度来看，部分行业坐拥“宅经济”红利，在自然流量的基础之上，通过产品、服务、营销上的升级和创新，使新增用户流量得以留存。整体上看，移动互联网流量处于稳步增长态势。

此外，各行业在技术赋能下积极寻求更适合的渠道结构以及更加丰富的营销手段。人工智能、5G 等技术的不断成熟为多样化广告呈现以及广告内容高效生产与推送提供了新路径。短视频媒体也在今年疫情期间迎来发展的高速期。

最后，在后疫情时代，各行业加速数字化转型的背景下，移动营销的大环境也在悄然生变。受整体经济形势影响，企业营销预算普遍缩紧，广告投放更加理性和谨慎，呈现出了一些新的移动营销趋势：

（1）效果营销受到空前重视。2020 年新冠疫情很大程度上改变了媒介与广告投放策略，营销人员更注重数字渠道的营销灵活性，愿意尝试创新的营销形式，更加注重广告效果。由技术驱动的“智能营销”正被行业广泛接受，它基于深度学习算法，可以实现对用户精准推送。同时，通过大数据监测，能够对投放效果及用户留存情况进行及时反馈。

（2）圈层营销正在兴起。“圈层”文化在移动营销领域持续发酵，

它基于兴趣属性，通过某个领域的意见领袖影响整个圈层群体，从而达到裂变式营销的效果。

（3）内容和创意营销的重要性逐步显现。各个行业都在加码内容营销，希望通过优质内容引发用户的情感共鸣，通过新奇的创意增强品牌和产品的辨识度，通过互动性增强用户的参与感，从而达到传播品牌价值的最终目的。

(二) 市场监管将更加清晰化

由于互联网广告主体的虚拟化、多元化、跨地域等特点，造成了网络监管的难度加大，市场上出现不少大量违规行为以及对用户个人信息安全造成威胁的营销手段，移动数字广告市场同样经历了一段挑战市场监管的缺失的无序发展状态。近年来我国政府及相关部门已经加大了监管力度，出台了一系列政策和相关法律法规，规范移动互联网广告活动。在我国坚持扩大内需、激发市场活力和拉动消费的时代背景下，处理好数据安全、个人信息隐私保护与合法利用数据促进互联网广告产业发展之间的关系变得尤为重要，未来针对移动数字广告市场的监管将更加规范化、清晰完善化。

出台时间	文件名称	出具机构	具体内容
2018年10月	《中华人民共和国广告法》2018修订版	人大代表常务委员会	第四十四条规定利用互联网发布、发送广告，不得影响用户正常使用网络。在互联网页面以弹出等形式发布的广告，应当显著标明关闭标志，确保一键关闭
2019年6月	《2019网络市场监管专项行动（网剑行动）方案》	国家市场监督管理总局	深入开展互联网广告整治工作，以社会影响大、覆盖面广的门户网站、电子商务平台为重点，突出移动客户端和新媒体账户等互联网媒介，针对医疗、房地产、金融投资理财等关系人民群众身体健康和财产安全的虚假违法广告，加大案件查处力度
2020年3月	《信息安全技术个人信息安全规范》2020版	全国信息安全标准化技术委员会	新规范不仅修改了“征得授权同意的例外”、“个人信息主体注销账户”等内容，还新增了“用户画像的使用限制”，如：为准确评价个人信用状况，可使用直接用户画像，用于推送商业广告为目的时，宜使用间接用户画像
2020年12月	《移动互联网广告标识技术规范》	中国广告协会、中国信息通信研究院	首个专门用于广告的互联网设备标识规范文件，旨在定义移动互联网广告标识，规范其生成与服务原则、功能要求以及安全要求等，同时提出几种不同的实现方案，供广告主、媒体平台、第三方监测公司等数字营销各市场主体参考使用
2020年12月	《中国互联网广告投放监测及验证要求》	中国广告协会、中国信息通信研究院	该标准增加了对OTT广告监测要求，明确了受众地理位置监测要求和依据，完善了无效流量和广告可见性验证要求，将监测技术工具升级为“数字广告监测及验证统一SDK”

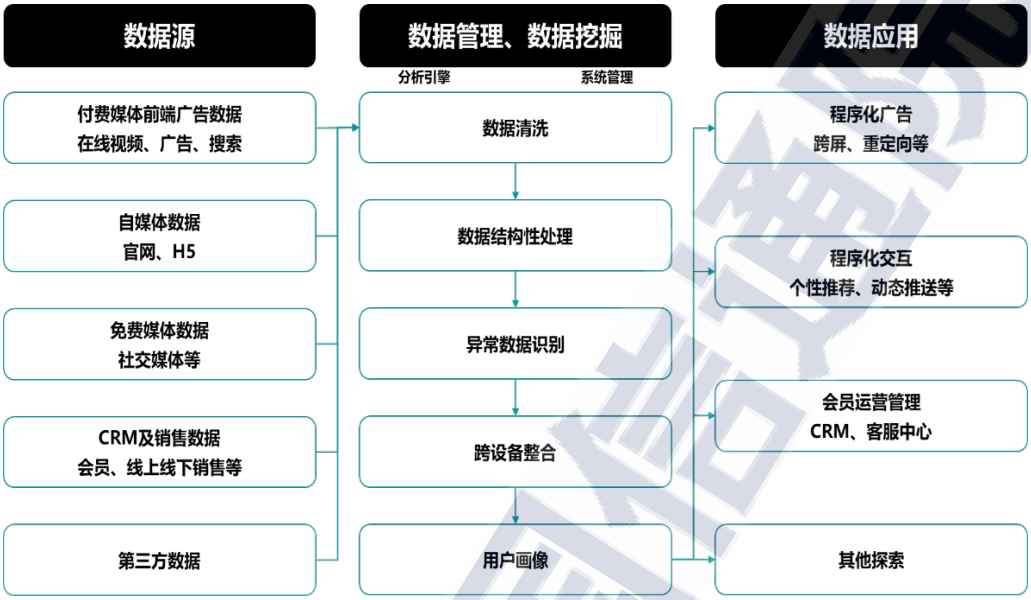
来源：公开资料整理

图 8 移动互联网广告行业相关法律法规及规范性文件

(三) DMP 市场将快速发展

DMP(Data Management Platform)指将分散的多方数据整合纳入统一的技术平台，并对这些数据进行标准化和细分，从而输出能够提供营销决策和运营决策的平台化产品。一个合格的 DMP 服务提供商具备的能力包括：独立性，数据是资产，与个人信息相关的数据的隐私性决定了 DMP 服务提供商的独立性、中立性；业务理解深度，DMP 服务提供商卖的不是 DMP 产品，卖的是数据经营方法论；技术实力，包括建模实力、算法优化实力等等，能够随着客户

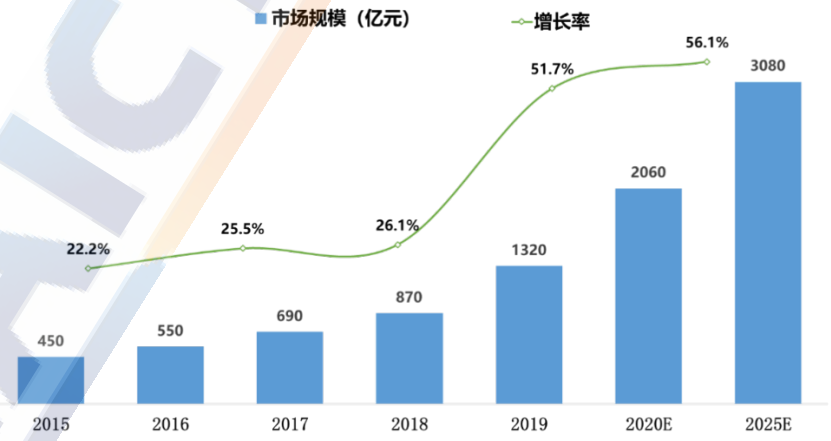
的业务发展提供适配的 DMP 平台服务；数据实力，有真正的第三方自有数据源，并对数据清洗、挖掘有丰富的经验等。



来源：公开资料整理

图 9 DMP 平台

近几年随着大数据技术与程序化广告的普及和推广，DMP 市场高速增长，2019 年市场规模突破千亿，达到 1320 亿，2020 突破 2000 亿。

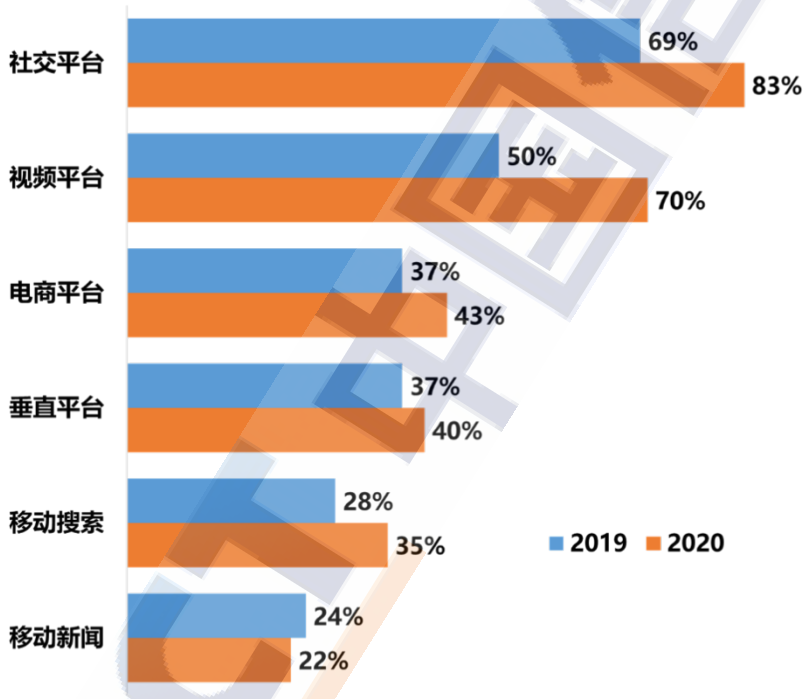


数据来源：Mob 研究院

图 10 2015-2025 年 DMP 市场规模（单位：亿）

(四) 社交广告将成投放主流

移动端社交平台、视频平台的广告主投放比例在 2020 年预计分别为 83%、70%，较 2019 年预算分别提升 14 个百分点、20 个百分点，移动端的社交平台成为广告主投放的第一名。从媒介展示广告到搜索广告，再到社交广告，移动互联网市场永远不缺乏新的广告模式。随着短视频、直播等众多新内容生态爆发，社交广告已经进入到生态繁荣、渠道下沉、用户激增的新时期。



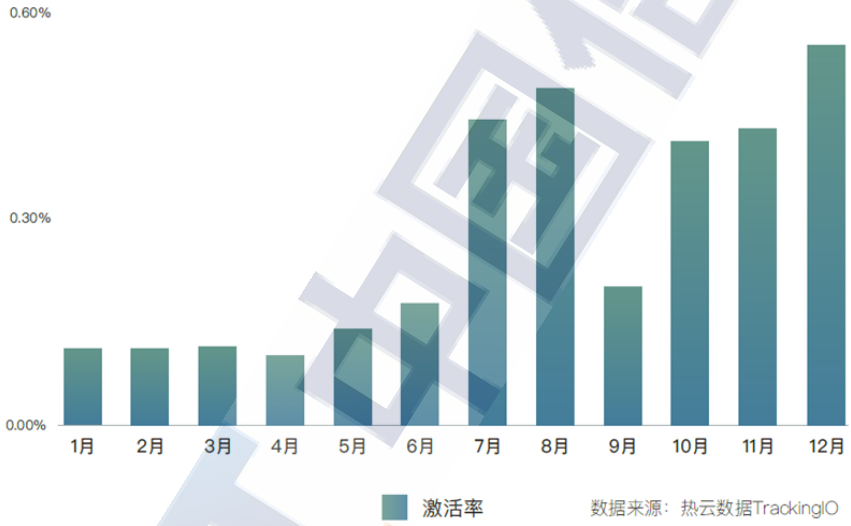
数据来源：iresearch

图 11 2019-2020 年广告主对移动广告投入比例

(五) 2020 手游行业投放特征

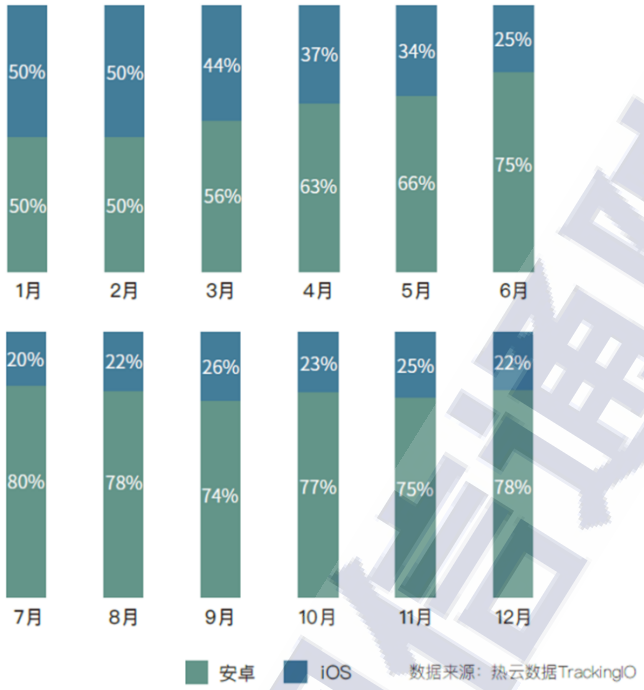
根据热云数据，2020 年手游投放效果数据走势来看，下半年激活率高于上半年，投放效果有所提升。尤其下半年，大厂游戏陆续

上线，主打精品化路线，口碑一路上涨，加上游戏厂商通过跨界营销、内容创意以及投放媒体上的全面覆盖，吸引了众多游戏玩家，增加了下载量。根据 2020 年付费设备占比走势，安卓付费设备占比增势明显，其中，下半年表现尤为突出，均值达到 77%。整体上看，由于今年国内苹果 AppStore 对手游审批趋于严格，Q3 全面下架未提交批准版号的游戏，这或许成为 iOS 付费设备占比下滑的原因之一。



数据来源：热云数据

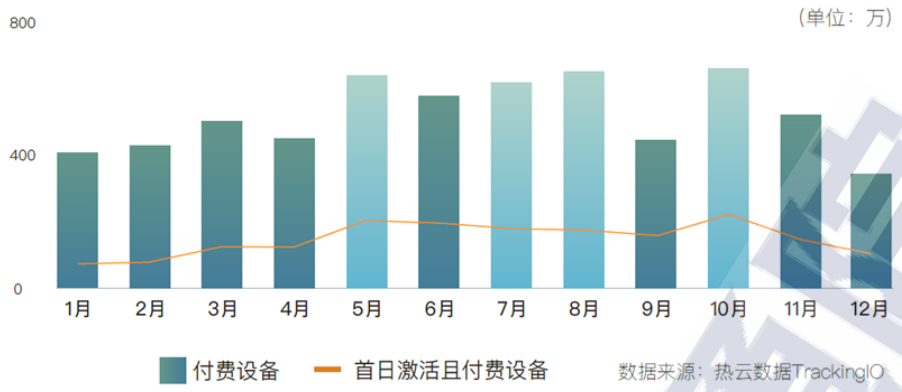
图 12 2020 年手游买量激活率趋势



数据来源：热云数据

图 13 2020 年手游买量市场各月付费设备占比走势

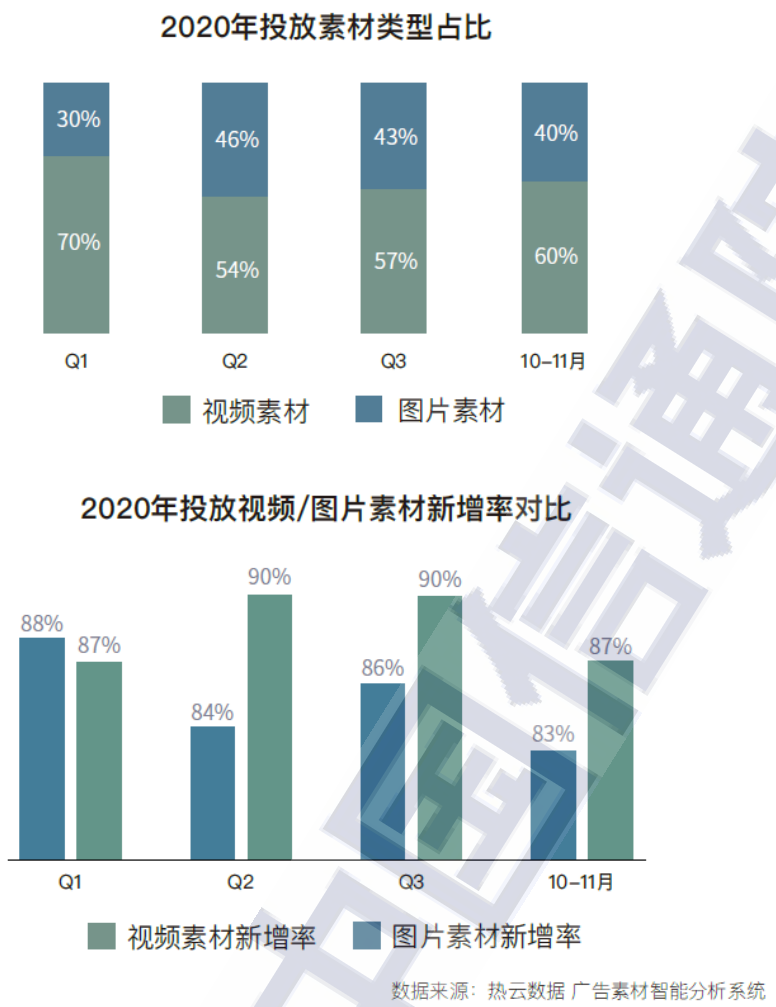
今年手游买量市场平均投放周期为 47 天，与去年的 35 天相比提升较为明显。一方面，由于今年存量产品的投放热度持续高涨；另一方面，休闲、棋牌等轻度游戏凭借疫情和假期期间“宅流量”红利，加大了投放力度。综合各月整体付费设备以及首日激活且付费两个维度来看，假期流量与整体付费设备的数量呈正相关。五一、暑期、十一是整体付费设备较高的时间段。而首次激活且付费没有明确的假期指向性，玩家“冲动消费”随机性较强， 5 月、6 月、10 月是首次激活且付费最高的月份。



数据来源：热云数据

图 14 2020 年手游买量市场各月及首日激活且付费设备数对比

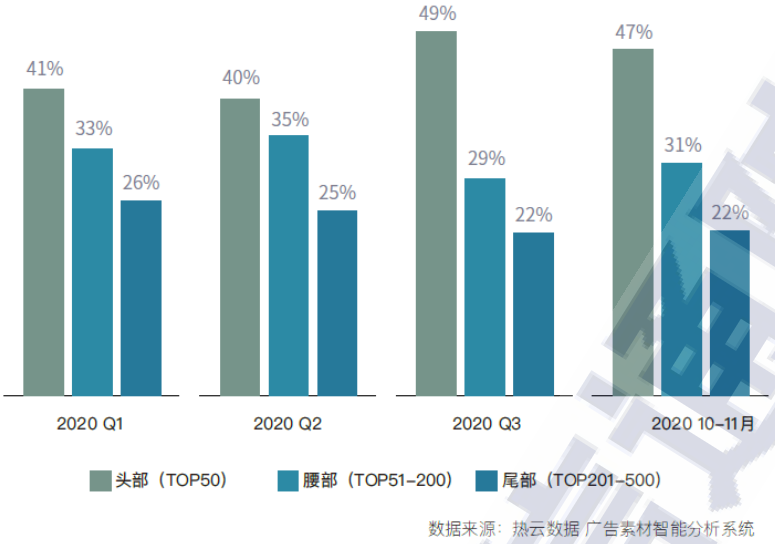
在 2020 年投放素材类型占比方面，今年 Q2 视频素材占比下滑较快，低于 Q1 时期的 15%左右，但之后稳步提升，10-11 月占比已上升到 60%。在视频和图片素材新增率方面，今年 Q3 二者达到最高值，Q4 有所回落，今年视频素材新增率均值为 85%，图片素材新增率均值为 89%。



数据来源：热云数据

图 15 2020 年投放素材及新增率对比

从 2020 年投放创意组数量排名前 500 款手游的数据来看，前 50 款游戏投放创意组数占前 500 款游戏的比例超过 4 成，与 2019 年相比，高出 6%左右，头部化趋势更加明显。其中，Q3 头部产品占比已接近 50%，达到最高点。今年下半年，尾部产品投放创意组数占比下滑至 22%，腰部产品占比在年底有小幅提升。



数据来源：热云数据

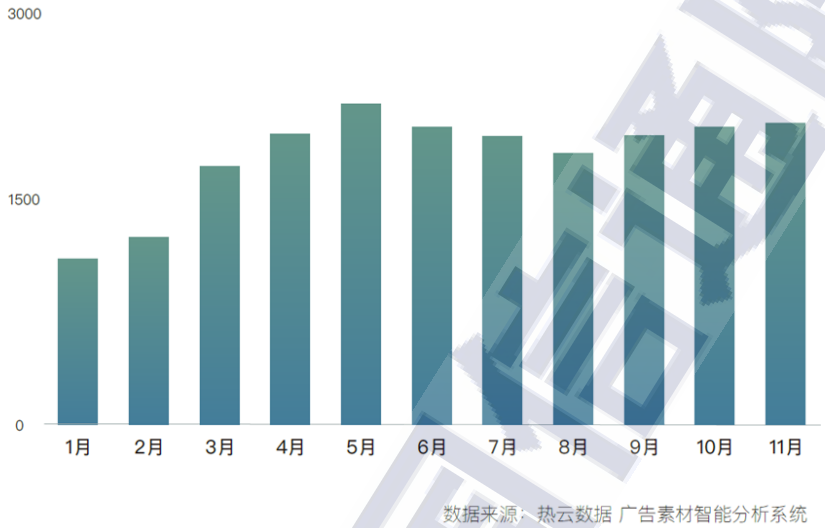
图 16 2020 年投放创意组 Top500 及占比分布

(六) 2020 非手游行业投放特征

2020 年应用类 App 投放产品总数超过 3800 款，新增产品数超过 1800 款，月均投放产品数超过 1700 款。从 1-11 月投放走势上看，与手游类 App 高峰投放期集中在下半年不同，应用类 App 相对平均，4-6 月及 9-11 月分别为上、下半年的投放高点，其中，全年最高投放月份出现在 5 月，产品数量超过 2000 个。从各月投放产品增长率上看，随着疫情逐渐稳定以及复工率的提升，3 月份增速最快，超过 35%，其中工作、网购和生活服务类 App 的提升幅度较大。

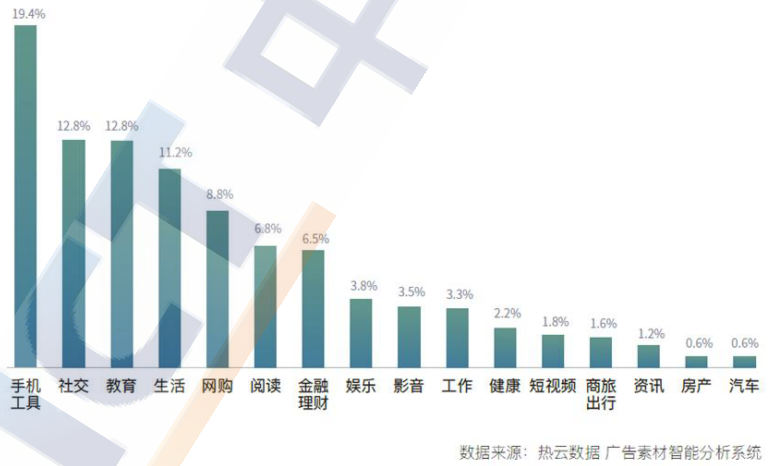
从 2020 年应用类 App 各类型投放产品数占比上看，在今年疫情影响的大背景下，手机工具、社交和教育投放产品数最多，手机工具类排在第一，占比接近两成，社交和教育平分秋色，比例接近 13%。手机工具类由于分类众多，在宅家因素下，个性化设置和安全优化

等 App 的使用率明显增多；社交类 App 则由于特殊时期线下社交受阻，使得线上社交需求获得更大释放；教育类在今年全民网课的形势下用户量激增，教育厂商加大投放以争取更多的新用户。



数据来源：热云数据

图 17 2020 年应用类 App 投放产品数



数据来源：热云数据

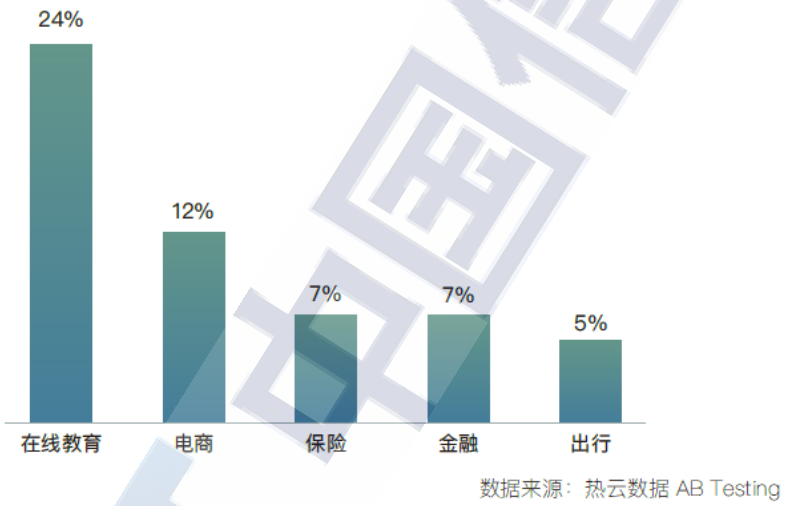
图 18 2020 年应用类 App 各类型投放产品数占比

根据相关数据对比发现，今年应用类 App 买量情况发生较大变化：

1、无论在排名还是占比方面，手机工具类表现尤为突出，排名

由去年的第六上升到今年的第一，占比提升 10%左右。

2、教育类仅次于手机工具，排名上升 4 个位次，占比提升约 5%。虽然教育类在排名提升上不及手机工具，从投放落地页优化试验次数的行业分布上看，教育类占比 24%，已经超过其他行业排名第一。教育行业更加重视获客方面的精细化运营，通过持续的 A/B 测试，不断提升新用户的转化率，并在此基础上进行营销创意的优化，从而形成正向的良性循环。



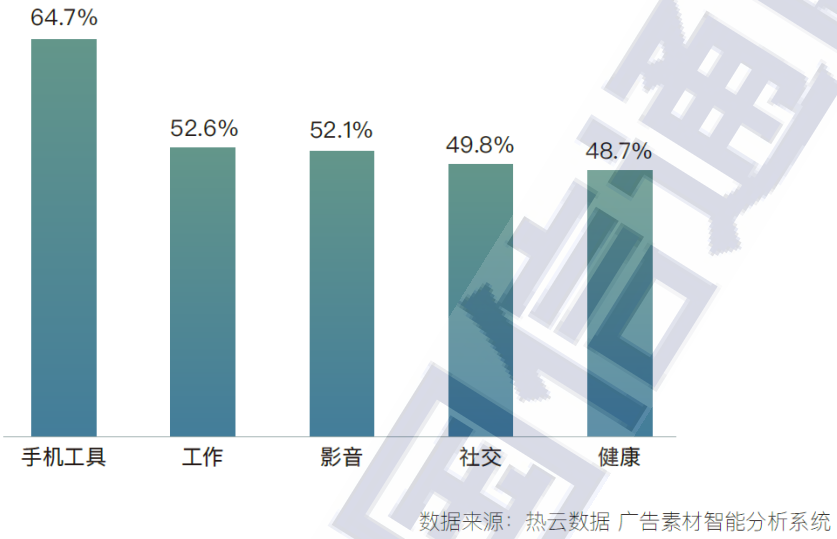
数据来源：热云数据

图 19 2020 年 A/B 测试试验行业分布 Top5

3、与 2019 年相比，金融理财行业排名和占比下滑最快，排名由去年的第一下降到今年的第七，占比下降约 10%。

在应用类 App 各类型投放产品新增率方面，与 2019 年新增率 Top 类型相比，工作类和健康类首次进入前五。工作类一是受疫情影响，居家办公类 App 新增投放较多，二是在就业环境下行的情况下，招聘类 App 的活跃度较强，除全职招聘以外，今年兼职类 App

投放同样有所上涨。同时，在大众健康意识觉醒下，运动健康类 App 新增产品也有所增加。除上述两大类型外，今年新增率 Top 类型基本与去年一致，以手机工具和泛娱乐类为主。



数据来源：热云数据

图 20 2020 年应用类 App 各类型产品新增率 Top5

四、互联网欺诈场景及态势

(一) 互联网欺诈场景

如图 15 所示，黑灰产遍布金融，电商/新零售，社交，出行，游戏，在线教育，互联网广告，短视频，电信等多个领域，多个行业，每年造成的损失高达 5000 多亿，给社会、国家、企业和网民造成的危害极大。在银行转账，信用卡盗刷，刷榜刷单，广告导流，虚假用 户裂变，盗刷积分，渠道流量作弊，营销活动欺诈，虚假交易套利，游戏外挂作弊等多场景下，都有黑灰产的身影。

来源：公开资料整理

图 21 互联网欺诈主要场景

1. 营销欺诈

营销欺诈：指在企业为了争夺市场，在发起各种营销活动（红包、优惠券、奖金）以达到获客拉新、激活用户目的的过程中，被黑灰产利用技术手段不正当获利，导致营销成本急剧上升的场景。

由于当前营销欺诈相关的法律法规尚未成熟，相关的反欺诈技术也还在发展中，营销欺诈成为最常见的互联网欺诈行为之一，常见于金融、电商、教育等行业。

长期从事互联网营销欺诈的黑灰产人群，有一个共同的名字，叫做“羊毛党”，羊毛党的定义如下：

羊毛党：指操纵大量互联网账号，有选择地参与各互联网渠道在线营销活动，通过自动化技术或者人工等手段，违规获取优惠券、代人下单、囤积大量低价稀缺商品（比如飞天茅台酒）等方式，以相对较低的成本甚至零成本获利的黑灰产人群。

羊毛党的主要类型可以分成以下四类：

- 第一类是个人纯手工进行薅羊毛的行为，这类行为往往因涉案金额和规模小，不易受到商家的重视；
- 第二类利用商家网站或 APP，使用外挂程序将薅羊毛过程完全自动化；
- 第三类通过破解后台接口建立虚假客户端进行薅羊毛；
- 第四类是团伙羊毛党，通常是组织者利用 QQ 群、微信群指挥团伙成员薅羊毛，且这类薅羊毛行为呈现与平台、商家瓜分利益的趋势。

羊毛党的欺诈步骤如图 16 所示：首先，利用虚假号码进行人工、机器自动化批量注册互联网账号；其次，利用上述账号进行集中的批量扫货下单、抢优惠券；最后，将买到的明显低于市场价格的商品和优惠券，以较高的价格倒手卖出，赚取差价。

来源：公开资料整理

图 22 羊毛党欺诈过程

界定羊毛党的关键特征是，多频率、有组织地在单次营销活动中多次获取优惠金额的行为，其实质是由于其薅羊毛的行为侵占了其

他用户本应享受的优惠活动，导致给互联网企业和其他互联网用户造成重大的损失。

目前，羊毛党已形成 15 余工种、近 200 万从业人员、产业规模不低于 1000 亿元人民币的产业链，分工明确、合作流程成熟，并且逐渐向隐蔽、专业、精准方向发展。

某母婴电商平台自 2017 年至今一直遭受“羊毛党”攻击，其面向新用户的“大牌奶粉买一送一”等营销推广活动，已是“羊毛党”的稳定收入来源之一。根据线报，这批“羊毛党”通过 QQ 群沟通交流，团伙分工明确，具体角色可分为“技术骨干”、“代购小白”、“奶粉老板”。“技术骨干”有一定技术能力，负责批量注册平台账号和养号，向“代购小白”们销售账号。“代购小白”们得到大量账号后，参与平台营销活动，以低于 50%的市场价格下单奶粉，转寄给“奶粉老板”。“奶粉老板”收货、结算款项，最终不知将这批奶粉流转到哪个销售网点。某品牌奶粉正常电商零售价约 200 元/罐，以“买一送一”活动为例，“羊毛党”单次就能轻松薅走 200 元，根据群内的日交易量，仅这批“羊毛党”就能给该母婴平台造成每月几十万的损失。

2. 流量欺诈

流量是指用户连接网络后，使用互联网产品与在线服务进行交互的活动或者行为，比如下载 APP、观看短视频、购买商品、阅读文章、搜索内容、在线购买保险、在线玩游戏，在线看病等。流量

发生有五个关键要素，即**用户，连接互联网，交互行为，承载流量的互联网产品，交互数据。**

在“数据为王，流量至上”的互联网时代，数据和流量竞争日趋激烈，对互联网公司而言，谁拥有高质量的数据和流量，谁就能拥有更强的竞争力。在利益的驱动下，互联网黑灰产通过流量欺诈（不限于流量劫持、恶意点击、刷单刷量、窃取数据）等违法手段牟取不法利益，不仅危害了互联网企业和公民的合法权益，更是对国家经济发展造成了极为恶劣的影响。

流量欺诈是**渠道流量欺诈**的简称，一般指黑灰产利用技术手段仿冒互联网产品的新增用户，独自或与第三方推广平台合作，共同骗取互联网产品市场运营成本的行为。流量欺诈导致企业的市场营销投入的投资回报率（ROI）大幅下降，增加企业的运营成本。

常见流量欺诈的手段有人刷、机器刷、木马刷、流量劫持等手段。

人刷：指通过奖励积分、优惠券、现金等方式，人肉刷下载安装、注册激活、广告点击而产生虚假流量的方式。

机刷：指通过猫池、卡池、设备农场等机器设备批量地模仿真实用户产生互联网虚假流量的方式。

来源：公开资料整理

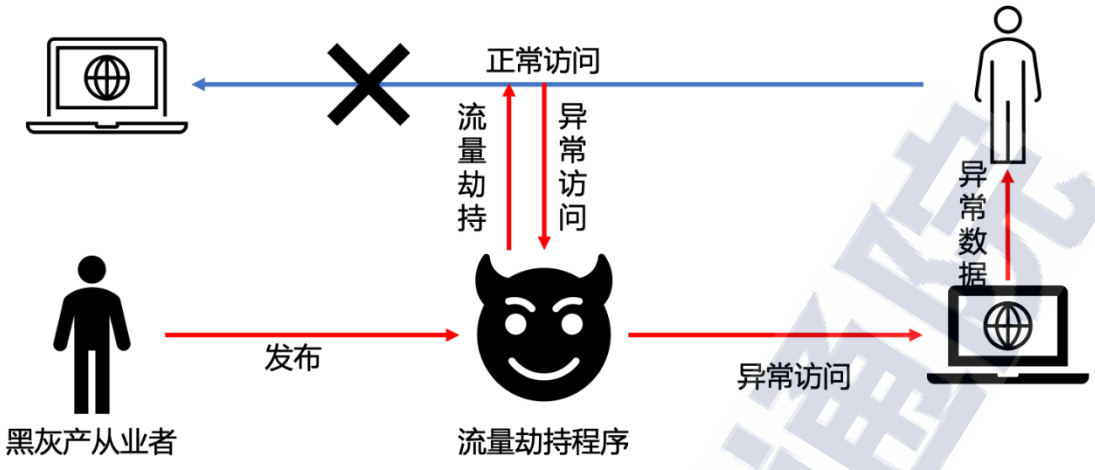
图 23 常见的机刷设备

木马刷：指通过木马的方式入侵用户的手机、智能设备或者互联网应用，在机器设备的后台流量欺诈木马以自动运行的方式模仿真实用户产生互联网虚假流量的方式。

来源：公开资料整理

图 24 木马刷原理图

流量劫持：指通过技术手段改变互联网用户流量活动的目标和对象或者篡改互联网用户获取的数据的违法行为。



来源：公开资料整理

图 25 流量劫持原理图

根据劫持程序作用的位置，流量劫持可以分成终端劫持、链路劫持和服务端劫持三种类型。

终端劫持一般指将劫持程序以木马的方式寄生在手机或者智能终端上。链路劫持一般指将劫持程序以木马的方式寄生在网络设备上，比如路由器，交换机。服务端劫持一般指将劫持程序以木马的方式寄生在应用程序服务器上。

3. 广告流量欺诈

广告流量欺诈指：利用采购到的信息，如设备 ID、IP，通过模拟和创造成广告主接收的数据的形式，虚增出大量非真实的行为产生的流量的行为。

广告流量欺诈又可以细分成以下几类：

(1). 展示欺诈：是指对未产生曝光，或者未完成有效曝光的素材收取展示费用 ，例如媒体将多个展示广告置放在同一个广告位，向广告主多收取多个广告的展示费用;

(2). 点击欺诈：是指未实际产生点击情况，利用机器人或者脚本虚增的点击行为。通过脚本或计算机程序模拟真人用户，又或者雇佣和激励诱导用户进行点击生成大量无用的广告点击，从而吃掉 CPC 广告预算;

(3). 安装/激活欺诈：通过测试机或模拟器模拟下载，以及通过移动人工或者技术手段修改设备信息、破解 SDK 方式发送虚拟信息、模拟下载激活等等；或通过大量发送点击事件，根据 LastClick 原则抢激活上报前的最后一次点击。

(4). 应用内行为欺诈：典型手段是购买欺诈，即用户或玩家在没有付费的情况下得到内容或产品，导致控制面板及报告收入数据过高;

(5). 虚假流量欺诈：包括非人为流量，大量注入的激励流量，挟持设备流量等。

(6). 流量归因欺诈：这种方式是针对 CPA/CPS 流量的作弊方式。作弊广告渠道商收集了很多的设备和用户信息，然后直接往对方广告点击日志服务器发送不同设备的点击信息。这其中如果有一些自然流量恰好在这之中某时间段进行了转化，激活日志服务器采集到对应设备的激活，就会被认为是该作弊渠道商的。这种发送虚假信息来将自然流量伪装成渠道流量的手段可以用在很多环节，比如刷服务器点击行为，刷监测代码等。

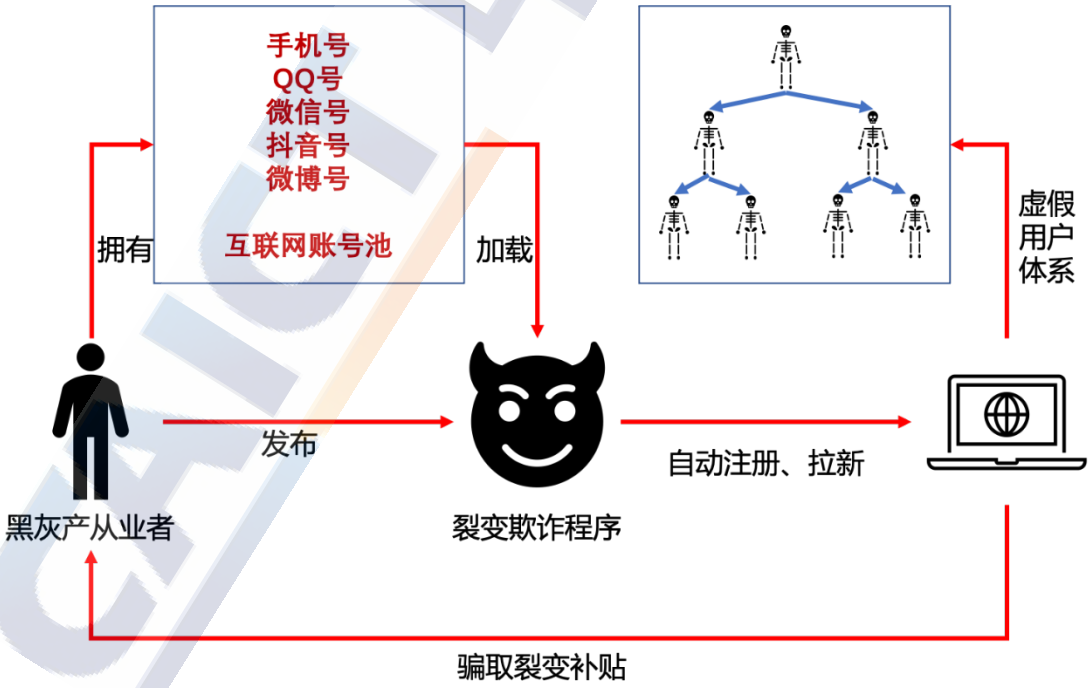
4. 虚假用户裂变欺诈

用户裂变一般指通过对互联网产品的种子用户给与一定的激励

措施，通过他们的社交关系发展一级甚至多级子用户的过程，从而帮助互联网产品达到提升活跃度，促进商品售卖等目的。用户裂变是一种新的营销方法和组织体系，在互联网用户流量日益见顶的形势下，基于社交电商的用户裂变成为了互联网企业的香饽饽。

虚假用户裂变欺诈常见于社交网络、社交电商等可以产生多级分销、裂变的场景。为了获得新用户、促进电商成交、提升 APP 活跃度，互联网企业利用社交网络传播广、传播快的特点，建立多级社交网络分销体系，并且给与分销节点一定的可变现激励。

由于用户裂变有利可图，成为了互联网黑灰产作案的重灾区。一般作案的手法是，通过控制大量的手机号、互联网账号（微信号、微博号、抖音号等），通过自动化的注册、拉新、促活程序，来骗取互联网产品的裂变营销补贴。



来源：公开资料整理

图 26 互联网裂变欺诈示意图

5. 恶意交易欺诈

恶意交易欺诈是指黑灰产利用互联网产品在线交易的便利性，在互联网在线交易过程中的付款、退货、换货等政策环节中，利用互联网产品的技术、政策和机制漏洞，进行非法牟利的场景。

互联网产品在给用户带来交易、购物便利同时，也让大规模恶意交易有了可乘之机。恶意交易欺诈一类以纯粹牟利为目的，还有另一类以恶意破坏、恶意攻击竞争对手为目的。

互联网恶意交易欺诈不仅会给互联网企业和平台造成巨大损失，同时也会给正常交易的互联网用户造成损失和不好的用户体验，严重制约了互联网生态的健康发展。

6. 金融支付欺诈

金融支付欺诈指利用不正当的技术手段，在互联网支付的各个环节谋取不正当利益的违法行为。

随着互联网金融的发展，金融支付欺诈现象日益增加，主要的手段包括:

- 利用系统漏洞，在用户不知情的情况下，划转用户的资金。
- 通过盗取用户的账号、密码，复制手机号等方式，骗取用户的资金。
- 通过一些第三方支付平台推出的商户POS机虚构交易套现。
- 利用木马、窃听等互联网恶意技术手段，盗取互联网用户金融账户、虚拟货币账户内的资金。

7. 网络刷单欺诈

网络刷单欺诈一般指互联网水军、自动刷单软件模拟正常活跃用户的行为，对商品品论、购买数量、网络舆情进行恶意操纵，从而使消费者受到欺骗或者商家受到损失的行为。

网络刷单欺诈常见于互联网电商平台、互联网社交等领域，其主要目的包括刷差评诋毁对手、刷好评误导消费者购买、错误引导舆情走向等。网络刷单欺诈容易导致"劣币驱逐良币"的不良商业秩序，形成不公平的互联网商业环境，严重制约数字经济的健康发展。

网络刷单团伙常见的作案手段是操纵大量的互联网用户账号，通过运营刷手群或直接利用自动化的软件工具来实现对互联网电商平台、社交平台用户的粉丝数/评论数等多项指标进行刷榜造假，与有刷单需求的互联网用户进行非法交易，从中谋取不正当利益。

8. 网贷欺诈

网贷欺诈一般指互联网黑灰产从业者，通过伪造身份证件、伪造征信材料、购买非法数据等非法技术手段，利用互联网批贷系统在贷款资格审核环节的漏洞，违规获得互联网贷款平台贷款资质，并将贷款转移至个人账户，逃避平台追债而拒绝归还贷款的行为。

互联网贷款欺诈的主要欺诈手段有：申领大量手机号码，同时利用这些非常用号码进行大量刷量消费从而提高信用评级；通过技术手段修改伪造身份信息、手机设备信息、位置信息达到骗取贷款并躲避贷后催收的目的；利用公共信用信息更新缓慢的时间差同时

申请多家平台贷款，恶意透支信用度。

9. 话费帐户欺诈

话费账户欺诈是指灰黑产从业者利用运营商部分服务采取“先使用后补费”的特点，通过透支话费购买大量虚拟权益，再将这些虚拟权益在黑市中变现，从中谋取不正当收益的行为。

这些欺诈者会通过多种非法渠道获取大量低费号卡，再利用猫池设备及群控技术进行大规模养号。当所养号卡达到可透支话费的信用等级后，欺诈者就会使用话费购买大量互联网虚拟权益，例如热门游戏点券，Q币，游戏会员以及各个视频平台会员等。这些虚拟权益往往通过非法代充平台进行变现。

话费账户欺诈往往会使互联网企业尤其是运营商承受巨大损失，也会迫使运营商提高话费付费门槛和话费透支上限，影响了正常用户的权益。

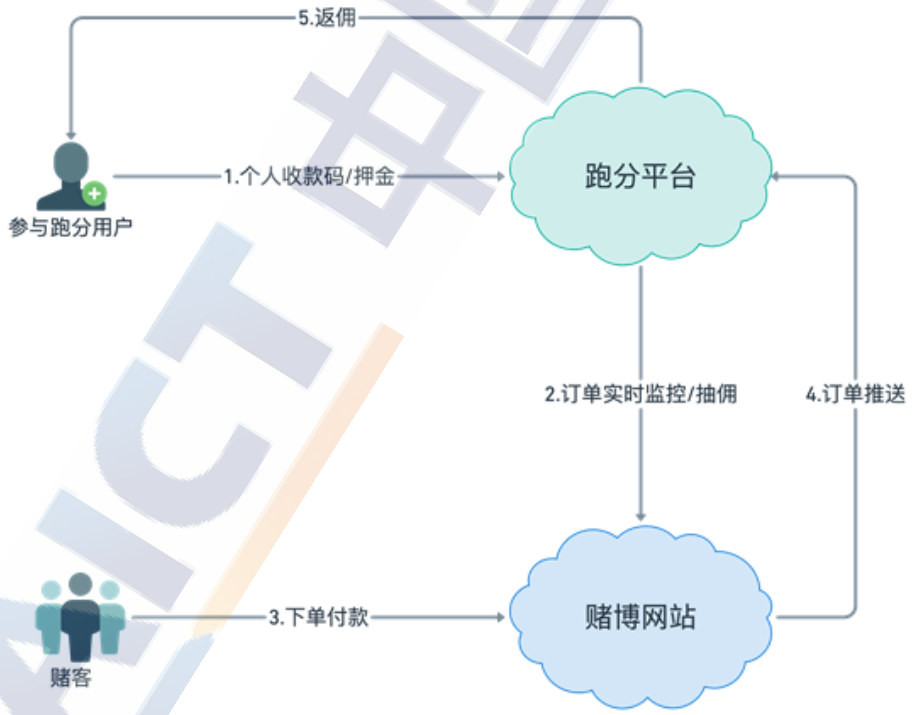
10. 网络赌博

网络赌博，通常指利用互联网，以钱财为赌注，使用某种方式或者工具比输赢来非法获取钱财的博彩行为。网络博彩类型繁多，由于受时间、地点等不确定因素影响，一般还是以“结果”型的赌法为主（例如赌球、赌马、骰宝、轮盘、网上百家乐等）。网络赌博是违法犯罪行为，具欺骗性和危害性，“庄赢客输”“十赌十输”是赌场的“不变规律”。

2019年开始，支付行业进入大整治。随着净网行动的严厉打击，

涉及黑灰产的支付通道被一一封堵，部分黑灰产的不法资金难以通过原来的支付通道流出，业内人士称之为“最强清理”。于是，一条名为“跑分”的产业链全面兴起，目前产业链已有逾十万人参与，三大参与方包括用户、代理和跑分平台。

通过开发“跑分”网络平台，吸纳会员，形成“码农—码商—代理—平台—支付通道—盘口”资金流转闭环路径，利用“第四方支付”为境外赌博网站等非法商户提供资金支付通道，以赚取佣金获利。据不完全统计，跑分链条产品已为黑灰产和赌博洗钱提供了上百亿的资金。这条新的黑色支付链条正在慢慢成长壮大，一条支付暗道已经形成，严重影响整个网络生态的健康发展。



来源：同盾研究

图 27 网络赌博欺诈示意图

(二) 互联网欺诈手段及发展态势

互联网欺诈手段及技术呈现出新的态势，覆盖申请、支付、交易、营销活动、渠道等多个环节。行业监管治理取得了一定的成效，但在整体上形势仍比较严峻，呈现以下一些新的特点:

1. 更先进的欺诈攻击工具

随着整体技术水平的发展进步，大量的物联网卡、虚拟专用服务器（Virtual Private Server，VPS）秒拨更换IP、云手机、iOS模拟器等资源和工具为黑产提供了巨大的便利，从而更高效且隐蔽地发起各式攻击。

2. 黑产 AI 智能化

在金钱驱动下，黑产团伙专业化程度不断提升，大数据分析、深度学习和人工智能技术也被黑产使用。一方面，欺诈方式从早期的简单高频批量操作，进化到在脚本中加入随机时间间隔，避免批量操作过程中呈现明显规律性，从而伪装成正常用户，以绕过平台的简单频度及用户欺诈检测。另一方面，如今黑产利用AI技术，通过机器学习模拟真实用户的行为轨迹，几乎能够在行为层面与真实用户操作习惯基本一致，来绕过平台的传统风控策略。

3. 机刷转向人刷

随着黑产攻防对抗的不断迭代升级，一种看似初级但随着规模效应产生质变的黑产作恶方式在2019年发展迅猛，即通过论坛、微

信群、QQ群等运营的方式，在群里发布黑产任务，常见的如刷粉丝量刷关注等，群里的成员每完成一个任务，即可以获得几毛至几块不等的奖励。由于进行黑产行为的均为真人而非批量的机器行为，平台方往往很难通过传统的技术手段来识别此类黑产。

4. 地域特征明显

江苏省黑产活动居全国首位。根据2019年同盾黑产拦截数据，对国内黑产活动IP归属地区进行研究分析，江苏省黑产活跃比例居全国省份首位，黑产活跃比例占黑产总活跃数量的14%。

Android黑产占比最多，其次为小程序/h5/网页端。根据2019年对同盾黑产拦截数据分析，Android平台黑产活跃比例位居第一，原因归结于Android的开源特点，作弊工具的开发和刷机技术难度低，大部分黑产采用Android设备进行作弊；其次是小程序/h5/网页端应用，据阿拉丁研究院发布的《2019年小程序互联网发展白皮书》报告，从2016年开始，经过三年的基础建设期，2019年小程序日活用户已达3.3亿，小程序平台黑产活跃比例已经超过iOS端。

5. 黑产供应链更加完整，上下游分工更明确

据不完全统计，2019年末国内网络欺诈直接从业者超过40万人，间接从业者超过160万人，以上下游产业链的形式紧密配合，并逐渐由利用技术方式进行机刷，升级为通过运营方式进行人刷。黑色产业链的上游主要负责资源获取以及技术工具制作，资源如手机号、IP、设备等，技术工具如猫池、改机软件、验证码破解、自动化批

量操作脚本软件等。而产业链的下游则是负责变现获利，根据行业不同而形式多样。

五、 互联网反欺诈体系

与传统的反欺诈体系不同，互联网反欺诈体系以数据为基础，通过采集各种黑灰产的行为数据，对黑灰产的设备、行为以及他们之间的关联关系进行建模分析，形成IP或者设备池等黑名单库，如TalkingData AI Shield智能防作弊产品。发现并识别潜在的欺诈风险，然后通过设备封杀、账号封杀等方式来处置欺诈交易行为。目前先进的大数据厂商，会采用建模分析的方式，根据设备特征、广告行为特征、线上使用行为特征、线下行为特征、家庭群组特征，这五维特征模型，评估设备的真实性。

(一) 反欺诈体系建设原则

1. 数据化

与传统的线下反欺诈不同，自动化的反欺诈检测本质上是数据应用能力的比拼。数据采集能力、挖掘能力和分析能力、建模能力，决定了互联网反欺诈能力的高低。

2. 实时性

为了保证良好的用户体验，互联网反欺诈体系必须能够在非常短的时间内对欺诈行为进行识别与认定，并给出判断。对于注册、登陆、支付等一些场景，必须能够在用户无感知的情况下对欺诈行

为进行检测和认定。

3. 准确性

互联网流量越来越珍贵，在进行欺诈行为检测和认定时，不能错杀任何真实用户，否则，不仅会导致互联网产品用户体验的下降，严重时候可能导致客户的流失。

4. 可扩展

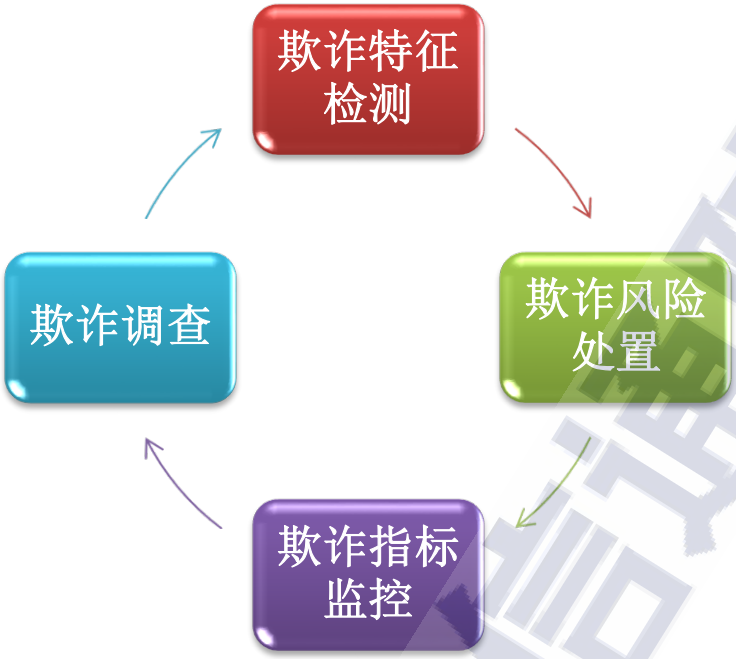
可以很方便对反欺诈体系进行横向和纵向扩展，横向扩展可以支持更多行业和业务类型，纵向扩展可以提升反欺诈算法的时效性和准确率。

5. 可进化

反欺诈体系应该具备一定的自进化能力，可以根据当前的反欺诈态势和特点，应用无监督学习、隐私学习等先进AI算法对反欺诈的能力进行自我迭代升级，以应对不断变化、技术发展快的互联网黑灰产势力。

(二) 反欺诈体系的构成

为了能够有效的管控互联网业务开展过程中的各类欺诈风险，一个完整的互联网反欺诈体系应当包含以下四个部分:



来源：公开资料整理

图 28 反欺诈体系示意图

1. 欺诈特征检测

欺诈特征检测是互联网反欺诈体系的基石，直接决定了互联网反欺诈体系的天花板。从欺诈特征数据的来源角度，欺诈特征检测又可以分为内部欺诈特征识别和外部欺诈情报监测。

内部欺诈特征识别，是指基于企业自行获取或外部对接的各类原始数据，对欺诈行为进行识别的过程。

常见的内部欺诈特征识别可以分为四大类，根据发展的时间长短和成熟程度包括信誉库、专家规则、有监督机器学习、无监督机器学习。

内部欺诈特征的识别涉及技术广泛，需要长期的研究和积累，许多有实力的企业已经在此方面有了很多突破。目前市场上也有越

来越多的反欺诈厂商提供各种类型的反欺诈数据和服务，对于互联网反欺诈体系建设处于起步阶段的企业而言也是一个不错的选择。

外部威胁情报监测，是指通过互联网和线下的渠道，收集与企业相关的欺诈情报和线索，如羊毛口子、资料包装方法、风控规则和系统漏洞等。

孙子曰“知己知彼，百战不殆”，互联网反欺诈体系需要时刻保持对黑产动态的关注，必要时需要深入黑产内部，了解和掌握黑产的最新套路和手段，拿到黑产动向的第一手资料，及时调整和完善自身的策略进行应对。

2. 欺诈风险处置

互联网反欺诈体系应当制定反欺诈策略和规则，明确对于欺诈风险的可接受水平和处置方式。

在确立欺诈风险的可接受水平时，反欺诈团队应当与企业内部各业务部门进行充分的讨论和沟通，切忌单方面确定欺诈风险接受水平。

常见的欺诈风险处置手段包括:

风险消除，对于无法控制和接受的欺诈风险，应当通过制定反欺诈策略或优化业务逻辑进行拦截和隔离;

风险降低，对于无法消除的欺诈风险，应当采取措施，平衡业务体验和风险水平，降低风险级别，如二次验证（牺牲用户体验）、人工审核（增加用户等待时间）等;

风险转移，通过引入第三方，分散和转移欺诈风险，如购买保险、合作商分担等;

风险接受，对于可以带来收益大于损失的欺诈风险，应当予以接受。

再次重申，欺诈风险的处置应当综合考虑业务发展的需要，总体原则是实现业务收益和欺诈损失的平衡。

3. 欺诈特征检测

反欺诈运营工作是互联网反欺诈体系的重要组成部分。互联网反欺诈体系应当建立起全面的欺诈监控指标，对于反欺诈体系的运转情况进行实时监控。

欺诈监控指标应当与互联网反欺诈的需求结合定制。常见的互联网反欺诈监控指标包括:

业务类监控指标，侧重于对业务的进展情况进行实时的关注，如注册量、下单量、进件数、转化率等;

策略类监控指标，侧重于对反欺诈策略和规则的触发情况进行实时关注，如反欺诈规则的拦截率、反欺诈的触发数等;

欺诈监控指标应当随着反欺诈体系的防护对象而及时调整，不同的业务类型如营销、信贷、支付的监控指标也各不相同。

4. 欺诈调查

欺诈调查工作是互联网反欺诈体系必不可少的一环。从复杂的

案例中抽丝剥茧提取欺诈特征、梳理欺诈路径也应当是每一位反欺诈人员的基本技能。

作为互联网反欺诈体系的组成部分之一，欺诈调查承担着验证反欺诈体系的有效性和驱动反欺诈体系优化迭代两个重要作用。

欺诈调查工作包括**事中和事后**两种：

事中欺诈调查指在业务开展过程中将疑似欺诈行为冻结，转欺诈调查人员排除后方可继续进行;

事后欺诈调查指对各渠道反馈回来的欺诈线索和案例进行人工调查和分析，对其中的欺诈行为进行认定，并用于对欺诈特征检测、欺诈风险处置和欺诈监控指标的效果评估。

(三) 反欺诈体系团队配备

一个完整的反欺诈团队一般由调查人员、数据建模人员、反欺诈策略设计人员、反欺诈运营人员和研发人员组成，相比传统的反欺诈方法，互联网反欺诈团队更需要数据建模人员、数据分析挖掘相关研发人员来支撑，提升反欺诈技术体系的竞争力。

1. 调查人员

反欺诈调查人员应当人工对各种已经发生或正在发生的互联网业务请求进行人工的调查、核实。对于在人工调查中发现的漏报欺诈行为，应当及时的止损、追损，如取消订单（互联网电商）、拦截发货（互联网电商）、贷后提前介入（互联网金融）等。

欺诈调查是互联网反欺诈体系必不可少的一环，承担着验证反

欺诈体系有效性和驱动反欺诈策略优化迭代两个重要作用。

此外，欺诈调查能力应当是所有反欺诈人员都必须具备的一个基础能力。在条件允许的前提下，建议互联网反欺诈体系的从业人员都应当具备一定的欺诈调查工作经验，直接参与到各种欺诈行为的调查分析工作中。

对于欺诈调查岗位而言，需要候选人具备以下几个特点：

- ✓ 好奇心强：欺诈的方式方法复杂多变，欺诈调查人员应当具有足够强的好奇心，不断的学习和了解新鲜事物；
- ✓ 逻辑严密：欺诈调查人员应当具备从眼花缭乱的欺诈行为中，结合业务场景和反欺诈体系的现状，条分缕析的将欺诈者的每个步骤梳理出来的能力；
- ✓ 善于总结：同样的欺诈手法会以不同的面貌反复的被包装，欺诈调查应当能够透过现象看本质，总结归纳每种欺诈手法的核心本质，举一反三。

2. 数据建模人员

数据建模人员负责利用系统采集到的客户数据和数据挖掘输出的特征，建立欺诈模型，对客户的欺诈概率进行判断。该岗位的工作可与企业内部其他数据建模工作共享。

模型是获取欺诈特征的重要方式之一。在all in AI的今天，无论是业务层面的反欺诈还是底层技术层面的反欺诈，似乎不提一下大数据、机器学习和AI，似乎都不够潮。目前市场上稍微有点实力的甲方、乙方也都开始喊着AI反欺诈的口号。

不过，作为反欺诈模型的建立和常见的信用模型、营销模型还是有比较大的差异性的，对于从事反欺诈建模岗位的人员要求也有一定的差异性。除了建模工作例行所需要的基本技能，反欺诈建模人员还需要符合以下特点：

- ✓ 善于接受新的思路：反欺诈建模的最大难度在于标签的缺失，这一方面是由于欺诈行为的难以验证，另一方面也是由于欺诈行为的复杂多变性导致的，因此需要反欺诈建模人员对于建模思路和方法的开放性，至少不能局限于有监督建模，要能够勇于尝试无监督、半监督的思路和方法。
- ✓ 沟通能力强：对于反欺诈模型的而言，很多时候建模方法的选择带来的效果提升，可能远不如一个变量的选择，因此需要建模人员能够尽可能的了解欺诈的手法，从建模的角度去归纳寻找更好的变量和特征，切忌闭门造车仅从数据层面求解。

3. 反欺诈策略人员

互联网反欺诈体系需要有大量熟悉互联网欺诈手段和防范方法的反欺诈策略人员。反欺诈策略人员应当实时关注互联网欺诈的动态，及时发现新出现的互联网欺诈手段和手法，并有效的调度和利用既有的资源制定反欺诈的策略，进行防范。

专家规则是欺诈特征检测的另一种重要方式，而且在目前的实际业务开展过程中也承担着相对比较重要的作用。在大厂反欺诈专家和反欺诈策略属于不同的岗位，在小厂区分不是特别清楚的情况下经常一人兼任了，在此一并讨论。

作为反欺诈策略人员，需要能够选择恰当的专家规则或反欺诈模型，平衡业务发展需要，选择合适的风险处置方式，部署反欺诈策略应用于线上生产。反欺诈策略人员需要的特点：

- ✓ 熟悉黑灰产手法：这一条不多说了，知己知彼方能百战不殆，了解对手是防御的第一步。作为反欺诈策略人员，需要对于常见的黑灰产手法有比较充足的经验，这也是前面建议所有进入反欺诈行业的人员都从欺诈调查岗位做起的原因。
- ✓ 基础的数据分析能力：反欺诈策略人员需要能够通过数据分析的方法，总结和发现各种特征对欺诈行为和正常行为的区分度，从而选择可用的反欺诈策略。
- ✓ 逻辑性强：反欺诈体系是个典型的木桶，作为一个防御体系，反欺诈策略需要环环相扣，永远不能寄希望于口子没被发现。

4. 反欺诈运营人员

由于互联网欺诈行为的多样性和灵活性，欺诈手段会不断的出现变化和创新。反欺诈运营人员应当建立起各类反欺诈运营监控指标体系，通过监控指标的变化，不间断的分析指标变化原因，及时发现穿透反欺诈策略体系的欺诈行为并予以应急响应。此外，运营人员还应该与业务部门、产品部门、营销部门保持高度密切的沟通，做欺诈风险和用户体验的平衡。

欺诈运营岗位在很多小厂往往容易被省略，其运营职能往往会被反欺诈策略岗或者所有岗位分担。但是从实战的经验中，个人认为还是有必要将运营工作拉出来单独讨论下。

反欺诈体系是一个覆盖公司各条线、各层级的体系，涉及到有不同利益诉求的部门、不同背景出身的人员，因此运营工作不可或缺。一个好的反欺诈运营人员，能够起到润滑剂和粘合剂的作用，保证互联网反欺诈体系的有效运转和高效协作。

反欺诈运营人员是场上攻防的组织核心。对于反欺诈运营人员来说，以下特点是尤为关键的:

- ✓ 沟通能力强: 反欺诈运营人员需要能够和营销、产品、运营、研发等各部门进行有效的沟通，了解各部门的诉求，平衡风险和业务发展之间的关系，防止顾此失彼。
- ✓ 格局要高: 反欺诈并非简单的将欺诈用户或者欺诈行为一拒了之（事实上也无法绝对的将欺诈用户和正常用户切分清楚），有些时候欺诈行为甚至是对公司有益的（当然此时公司往往不把此类行为定义为欺诈）。反欺诈运营人员需要从公司的利益出发，综合评判对公司收益最大化的解决方案。
- ✓ 数据敏感性: 由于欺诈行为的复杂多变性，既有的反欺诈策略和反欺诈监控指标是绝对无法有效覆盖所有未知欺诈风险的，反欺诈运营人员应该能够从反欺诈各种指标乃至非反欺诈的各类业务指标变化中，敏感的察觉到异常，快速组织起应急响应、欺诈调查等工作。

5. 研发人员

研发人员包括数据挖掘算法工程师和系统开发工程师。

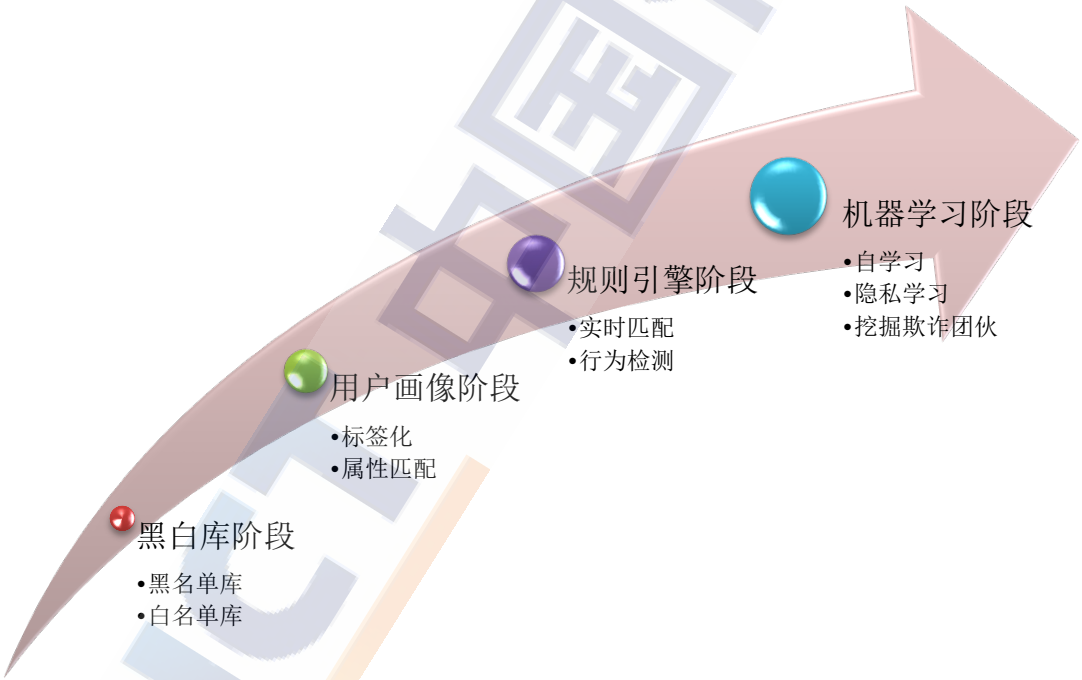
数据挖掘算法工程师: 数据挖掘算法工程师主要负责将系统采集的各种形式的数据进行解析和挖掘，输出各种特征，使其能够被

应用于反欺诈建模和反欺诈策略工作。该岗位的工作可与公司数据分析、用户画像等部门共享。

系统开发工程师：负责各类反欺诈系统的开发和维护、反欺诈策略和模型的实现。

六、移动数字广告与互联网反欺诈技术

互联网反欺诈技术发展经历了黑白库阶段、用户画像阶段、规则引擎阶段和机器学习阶段四个阶段，各阶段的发展特点如下图所示：



来源：公开资料整理

图 29 反欺诈技术发展的五个阶段

(1).**黑白库阶段：**这个阶段的核心就是建立黑名单库和白名单库，一般会从设备、IP、账号、手机号、地理位置、信用等几个维度分别建立黑名单库和白名单库。

(2).**用户画像阶段：**在大数据技术发展的早期，应用一些简单

的文本分析和匹配算法，对用户的特点和行为习惯进行画像，可以通过画像来判断互联网欺诈行为。

(3). **规则引擎阶段：**在用户画像的基础上，建立智能化的反欺诈规则引擎，规则引擎提供了一个灵活的、易用的、实时的、可适应各种变化的反欺诈方法，使反欺诈业务运营和技术研发之间的耦合度大大降低，极大提高了反欺诈的效率。

(4). **机器学习阶段：**规则引擎对已经发现的一些欺诈行为有较好的识别和拦截效果，但是对一些变异的和一些全新的欺诈行为，则显得非常吃力，随着黑灰产技术的不断发展，反欺诈运营人员也经常被黑灰产团伙牵着鼻子走，疲于奔命。为了解决这一问题，基于机器学习的具备自动进化的反欺诈算法应用而生，基于半监督学习、监督学习和联邦学习等技术，可以在小数据量、充分保证数据隐私安全的前提下，实现反欺诈系统的自我进化能力，可以极大降低反欺诈运营的成本。

(一) 行业级匿名设备元服务

1. 多策略融合的指纹生成方案技术

黑产变化十分迅速，现有的风险识别工具高度依赖于T+1离线挖掘，策略生效周期长、时效性差，同时存在柔性处置能力缺失、数据采集受监管限制等缺点，无法高效地完成设备指纹生成和风险识别工作。因此设备指纹、设备标识成为了业务风控的重要解决手段之一。

但是由于ID与设备唯一对应，导致其在进行流量反欺诈的同时未能很好地保护用户隐私；同时，多种解决方案并存，造成了巨大的**重复建设**和新的“碎片化”问题，使得产业无法形成合力、反欺诈成本居高不下。

为解决此问题，行业内出现了相关的解决方案以解决移动数字广告和流量反欺诈的需求。下面以“卓信ID”为例，阐述行业内相关解决方案。

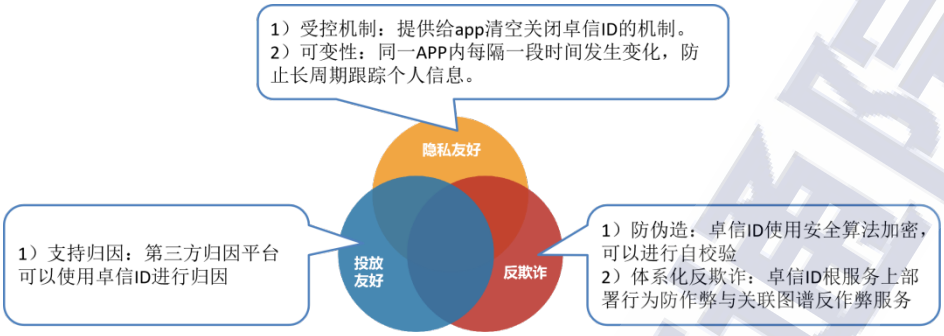
卓信ID的生成基于用户的非敏感信息，由服务端为每个设备生成根ID，该根ID只存储在服务端，此外，服务端还存储了根ID和卓信ID的对应关系，通过这个对应关系用于卓信ID的溯源，解决广告归因等精准营销的应用问题。

来源：中国信息通信研究院

图 30 卓信 ID：多策略融合的设备指纹生成策略

“卓信ID”使用安全算法加密，具有很强的反欺诈能力；不仅

降低开发者同时开发两套ID体系的成本，提升开发者流量识别的效率；还具有极高的隐私友好性，能极大提升终端用户的体验。



来源：中国信息通信研究院

图 31 卓信 ID 的特点及优势

该方案目前已经完成了在脱敏测试样本库（包括黑白名单）中的测试验证。相关测试结果表明，基于多策略融合的设备指纹生成方法“卓信ID”可以应用于全场景、全生命周期、全技术栈的互联网反欺诈体系中，使得互联网企业可以快速、有效建立较为完善的互联网反欺诈能力。

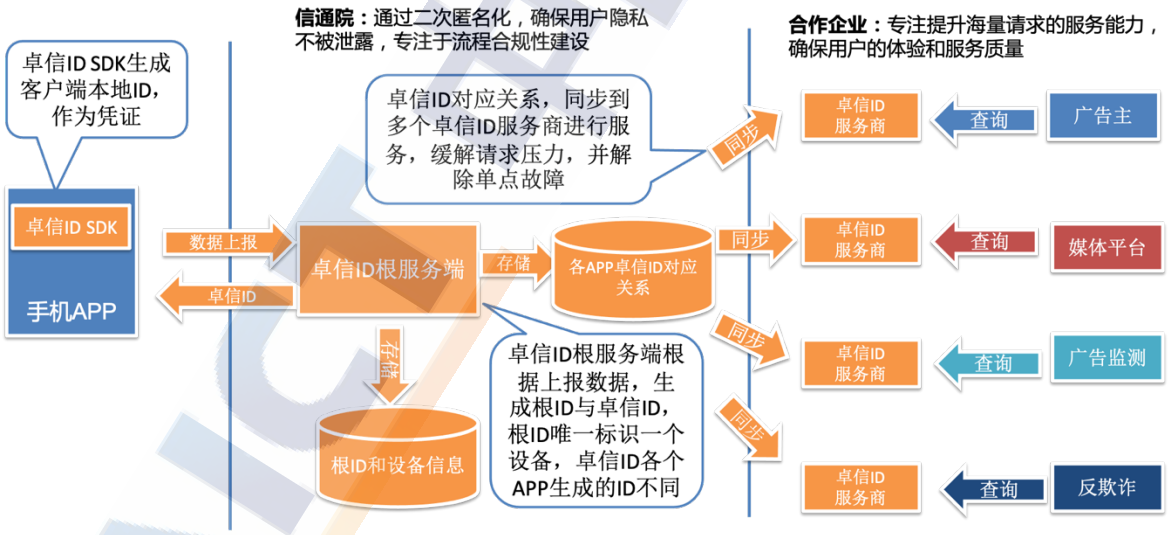
来源：中国信息通信研究院

图 32 卓信 ID 全场景的应用能力

2. 隐私友好的匿名设备指纹运营策略

当前，随着行业内对个人信息保护的关注不断增强，和设备及用户一一对应的设备指纹方面将不在满足合规性要求。因此，卓信ID设计了2层匿名化的策略，同时，提供了受控机制和可变机制，最大程度保护用户隐私。

“卓信ID”参考了DNS的设计理念，在中国信通院设立卓信ID的根节点，仅用来分配和维护匿名化的卓信ID数据。同时，合作伙伴即“卓信ID服务商”设立若干二级节点，通过二次匿名化为移动互联网企业提供效果监测、数据验证、标识查询等商业化服务——即将ID的分配和ID的商业化服务分离，从而共同构建流量反欺诈的服务体系。



来源：中国信息通信研究院

图 33 卓信 ID 的生成及应用策略

同时，卓信ID提供如下机制，保护用户隐私，使其与设备解耦：

受控机制：提供给用户及开发者清空关闭卓信ID的机制。

可变机制：同一APP内每隔一段时间发生变化，防止长周期跟

踪个人信息。

3. 卓信 ID 服务商探索和实践

早期对接卓信ID的业内服务商，对卓信ID应用于广告效果监测行业，开展了大量的探索和实践。

服务商企业普遍反馈卓信ID在ID生成实时性、数据安全性、同设备归因能力、服务商自主性方向，都很好的满足了需求。

（1） ID 生成实时性

广告归因一直都是广告效果监测服务的核心内容，对实时性有极高的要求。而卓信ID的生成获取，是由嵌入服务商SDK的卓信ID的SDK直接与根服务器通信生成的，中间没有其它的转发环节。中间转发环节的减少将有效的减少因数据传输和处理增加的等待时间，减少转发环节还可有效减少系统间网络请求的消耗时间，仅需一次初始化即可获取到卓信ID，有效的保证了对ID生成的实时性要求。

上报初始化事件后即可通过接口直接从本地获取卓信ID，其它的后续转化事件即可以卓信ID作为设备标识进行上报，实现卓信ID在转化评估场景的应用。

（2） 数据安全性

数据安全是行业底线，任何业务的流转都要建立在数据安全基础之上，卓信ID采用的根服务器生成ID、服务商提供查询服务的方

式、二重匿名的方式，很好的保护了数据安全:

一是卓信ID的生成参数不含个人隐私数据，仅采集设备指纹信息，从根本上杜绝个人隐私数据泄露的可能;

二是卓信ID生成参数由SDK直接获取并报由根服务器生成，没有中间转发环节减少了数据暴露的风险;

三是服务商处仅能获取到匿名处理过的ID，无法拿到根ID，且同一根ID在每个服务商处的匿名ID不相同，任何开发者都无法获取到重要的根ID，保证了核心数据的安全性。

四是“卓信ID”具备了受控机制和过期机制，从技术上保证了其与设备之间一一对应的可能性。

（3） 同设备归因

只有通过设备标识符准确确认是同一设备，才能实现广告营销过程中的效果评估及后续转化事件的归因查询。

因为卓信ID会定期升级算法，同一设备在不同时间会生成不同的ID，为了解决归因问题，作为服务商，为开发者提供卓信ID历史列表查询服务:

即当输入某一卓信ID时，接口输出该ID对应设备在服务商处的全部卓信ID，以便开发者进行追溯；开发者可以通过请求该接口获取设备在服务商处最早卓信ID，并将该设备做为主ID，不同事件的主ID一致即为同一设备，实现事件归因。

（4） 服务商自主性

作为服务商，需要给开发者开发优质的服务，在卓信ID查询这个核心服务不变的情况下，赋予服务商更大的自主性，服务商可以提供更多的个性化服务给开发者，使开发者获得更好的体验。

如,热云数据通过提升开发者接口授权流程的便捷性和友好性、通过扩展更大的QPS请求量、通过提供更完备的应用管理工具以及细致的卓信接入指导方案，在开发者中获得了良好的口碑。

同时，卓信ID服务商在相关场景做了大量的探索和实践，具体体现在:

- **异常行为**

通过整合卓信ID和可信设备信息,加入严格的风控模型，可有效识别用户是否在使用设备进行相关的异常行为。如伪造设备信息,虚拟设备,频繁的安装卸载,地理位置异常变化,为客户识别风险设备提供方案，提升客户的App安全性。

- **精准统计与分析**

用户可以借助卓信ID，更精准的做运营统计。如准确的新增设备数，活跃度，换机等运营数据。同时标记可能产生异常行为（是否越狱，调试，模拟器,代理，VPN等风险数据）的设备，有效精准统计数据，方便后续的风控完善,运营提供准确和安全保障。

- **网络 IP 识别**

借助卓信ID与算法，模型综合使用有效的识别IP黑名单。同时对唯一ID做多IP的归因处理,对相关IP做风险评分，网络兼容性分

享，并输出相关的IP画像,风险IP，规避风险IP,提升整体App的风控能力。

- **注册场景(垃圾注册,失信注册,羊毛党注册)**

结合卓信ID与设备信息，IP，邮箱等综合信息与综合评分，侦测是否为垃圾注册和失信注册，侦测手段等异常行为 ，检测当前设备/IP 在某时间段内是否进行了异常多的注册行为；识别是否为羊毛党,避免规避这些风险注册，规避欺诈风险，降低获取成本等。

- **登录场景 (账户盗用,暴力破解,撞库登录)**

结合卓信ID与设备信息，网络，风险评分，时间节点，代理综合信息，判断是否存在账户盗用，暴力破解，撞库登录等异常行为，避免被非法获取用户的密码等重要信息。

- **修改信息场景(异常修改)**

结合卓信ID与陌生的设备与网络信息修改，是否使用代理服务器，修改时间节点，外部综合风控评分来识别是否异常修改，避免规避资金损失，维护声誉。

- **支付场景 (盗号支付/伪冒支付)**

结合卓信ID与金融机构交易反欺诈的规则及风控模型和风险决策引擎系统，并结合基于设备指纹的机器识别技术，发现被监控的机器设备，IP，卡是否在存在盗用冒用的风险;

结合卓信ID与同一张卡号支付发生的移动速率是否正常等规则设定，帮助金融机构识别盗卡支付风险和虚假交易风险;

结合卓信ID与检测提现时是否为用户常用设备/浏览器/登录地/IP，提现时间，提现频度，提现卡号等维度，检测出用户当前的支付是否为正常支付还是盗用支付。

● **提现场景 （异常提现）**

通过结合卓信ID与有效的反欺诈相关规则，可以很方便地侦测或防止那些在异常时间中发生的交易。可以在无需打扰客户的情况下，防范欺诈分子在非正常时间内进行的批量欺诈行为。通过检测提现时是否为用户常用设备/浏览器/登录地/IP，提现时间，提现频度，提现卡号等维度，可以有效检测出用户异常提现风险。

● **绑卡场景 (异常绑卡/失信绑卡)**

通过结合卓信可信ID与金融机构交易反欺诈的规则及风控模型和风险决策引擎系统，结合基于设备指纹的机器识别技术和查询检索外部设备评分，判断当前设备/IP 等的风险评分等级，可有效减少绑卡风险。

● **充值场景 (异常充值)**

通过结合卓信ID与金融机构交易反欺诈的规则及风控模型和风险决策引擎系统，结合基于设备指纹的机器识别技术和查询检索外部设备评分，判断当前设备/IP 等的风险评分等级。通过充值规则和设备使用特征侦测出充值场景的异常行为并发出预警，帮助机构尽快锁定风险。

(二) 行业级匿名用户元服务

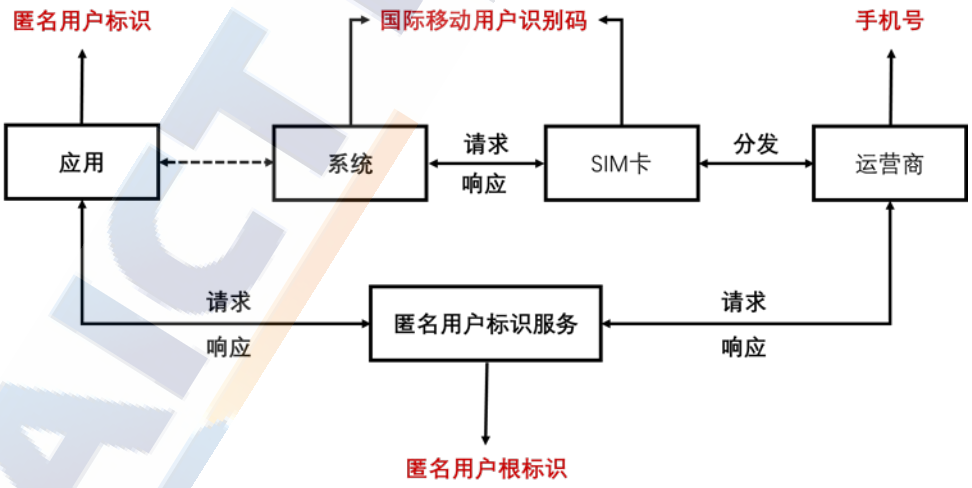
1. 行业背景

随着各国、各行业组织对用户隐私保护的要求越来越高，传统的用户标识体系如国际移动用户识别码（IMSI）等已被部分国家认定为用户隐私的一部分。同时，由于苹果IOS及安卓高版本的限制，IMSI等标识码已无法通过用户授权的方式获取，这也对移动互联网相关业务产生了一定影响。进一步，在黑灰产领域，需通过海量购买硬件设备以模拟真实用户，传统锚定设备的标识体系无法满足反欺诈需求。能够锚定用户身份的标识将产生更大价值。

当前，国内三大运营商正在共建匿名用户标识方案以解决上述问题。

2. 体系架构

移动互联网用户标识体系架构如下图所示:



来源：统一推送联盟标准

图 34 匿名用户标识体系架构

用户标识体系架构共涉及4类实体，包括应用、系统、SIM卡、运营商。为兼顾用户隐私和开发者运营需求，涉及手机号码、国际

移动用户识别码、匿名用户根标识、匿名用户标识四类标识符。

其中:

（1） 手机号码

获取方式：通过注册、实名认证等方式由用户主动提交。

产生方式：运营商分配。

隐私等级：高等级。实名制背景下，与用户身份高度相关。任何主体可根据用户手机号码通过电话、短信等方式触达用户。

重置方式：无法重置。

（2） 国际移动用户识别码（IMSI）

获取方式：经用户权限授予后，开发者可向操作系统获取。目前，安卓高版本限制了对 IMSI 的获取。

产生方式：全球移动通信系统协会（GSMA）分配。

隐私等级：中等级。和手机号一一对应，开发者可使用 IMSI 作为用户标识，开展相关互联网业务。其中，IMSI 包含了用户 SIM 卡的国家、运营商等信息。

重置方式：无法重置。

（3） 匿名用户根标识（AURID）

获取方式：用户首次向开发者授权后，由匿名用户标识服务和运营商交互后获取。

产生方式：运营商分配。

隐私等级：低等级。和手机号锚定。

重置方式：无法重置。

（4） 匿名用户标识（AUID）

获取方式：经用户同意后，开发者向匿名用户标识服务申请后获取。

产生方式：匿名用户标识服务分配。

隐私等级：超低等级。和匿名用户根标识锚定。

重置方式：可被重置。

3. 功能要求

（1） 匿名用户根标识的功能要求

不可逆：通过加密算法生成的匿名用户根标识不能够被反向追踪；

唯一性：匿名用户根标识生成算法保证标识唯一性；

耦合性：匿名用户根标识和用户设备解耦，与用户身份耦合。

锚定性：匿名用户根标识与手机号码锚定。

（2） 匿名用户标识功能要求

不可逆：通过加密算法生成的匿名用户标识不能够被反向追踪；

唯一性：匿名用户标识生成算法保证标识唯一性；

连接性：对于同一用户，在一定时间内，不同应用所对应的用户匿名标识相同;

耦合性：匿名用户标识和用户设备解耦，与用户身份耦合。

受控性：使用匿名用户标识的开发者需提供相关选项，供用户重置匿名用户标识。

4. 安全要求

（1） 访问控制

对于来自应用的请求进行访问控制，以保证过程应是安全可信的。

（2） 存储安全

匿名用户标的存储应保证完整性和隐私性，不可被其他非法实体访问或篡改。

（3） 防篡改攻击

应对程序的完整性、参数内容的完整性和有效性进行检查，以防御篡改攻击。

(三) 多策略融合的策略体系

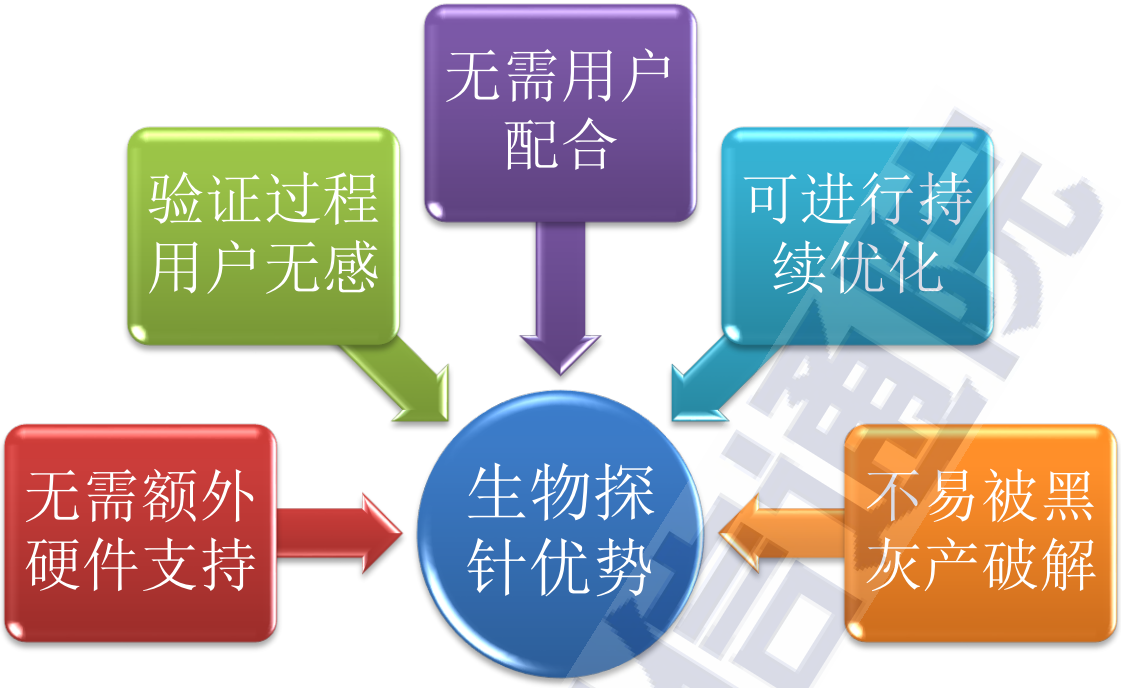
随着黑灰产技术的进步，单一的策略已经很难产生良好的反欺诈效果，多策略融合成为反欺诈策略的发展方向。反欺诈策略体系包括多策略融合的设备指纹生成策略,多策略融合的生物探针技术,

多策略融合的欺诈行为识别，多策略融合的欺诈事件处置，以及多策略融合的欺诈数据分析方法等。

1. 多策略融合的生物探针技术

生物探针技术指采集用户使用手机时的传感器数据和屏幕轨迹数据的技术。智能手机有很多传感器，加速度计、陀螺仪、重力加速度计、磁场传感器计等，这些传感器能够记录用户使用手机时的数据。如：加速度传感器能够记录手机的线性加速度大小，重力加速度记录手机的重力加速度；陀螺仪记录手机的角加速度。每个用户使用手机的习惯表现在用户操作手机时这些传感器的变化以及滑动屏幕时的轨迹上。

应用生物探针技术通过融合用户点击、按压、滑动、滚动、按键等多维度的行为动作数据对用户行为的合法性进行识别，相比其他用户认证方法，有以下优势：



来源：公开资料整理

图 35 生物探针的优势

生物探针技术应用过程中一般包含了数据采集、特征抽取、基于机器学习的生物特征决策算法等核心技术，通过数据采集可以无感收集用户使用手机的行为数据，对然后对数据做特征工程，将抽取到的特征输入到训练好的机器学习算法里，用于判定是否是合法的用户行为。

2. 多策略融合的欺诈行为识别

随着黑灰产技术的进步，单一的黑灰产欺诈行为识别策略已经很难凑效，当前主流的欺诈风险识别方式是融合了设备风险识别、行为风险识别和关联分析挖掘等多种风险识别策略，通过对策略的融合，可以有效提高风险识别的准确率。

来源：公开资料整理

图 36 多策略融合欺诈风险识别

设备风险识别主要通过建立设备的黑白库和设备的画像来实现；行为风险识别一般通过生物探针、规则引擎、机器学习等技术来实现；关联风险识别则需要应用到知识图谱、无监督机器学习、联邦学习等新的技术。

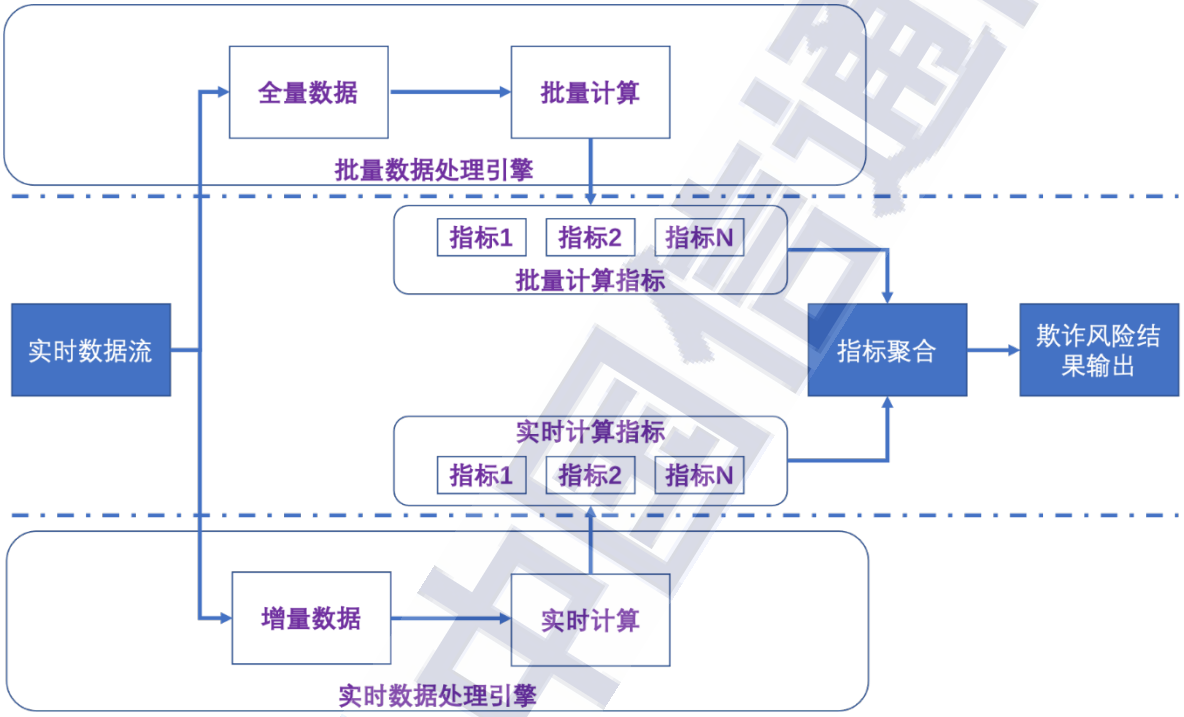
3. 多策略融合的欺诈风险处置

随着黑灰产与反欺诈之间的对抗越来越激烈，单一的欺诈风险处置策略已经很难有较好的效果。多策略融合的欺诈风险处置一般融合了 IP 封杀、账号封杀、设备封杀、手机号封杀、黑白库上链等综合手段，多维度封锁互联网黑灰产产生破坏的可能性，提升反欺诈的成功率。

4. 多策略融合的欺诈数据处理架构

在进行欺诈风险识别时，需要同时对历史数据指标和实时数据指标进行聚合处理，以确保风险识别的准确性和有效性。很多历史数据指标是基于过去一个月甚至一个季度的数据分析出来的，若果历史数据指标计算应用实时的数据处理架构，将会给反欺诈系统造成巨大的计算压力，无法满足反欺诈的时效性要求。

因此，融合历史数据指标和实时数据指标的数据处理架构更适合欺诈数据的处理，多策略融合的欺诈数据处理架构由批量数据处理引擎、实时数据处理引擎和指标聚合算法三个核心模块组成，其架构示意图如图 30 所示。



来源：公开资料整理

图 37 多策略融合的欺诈数据处理架构

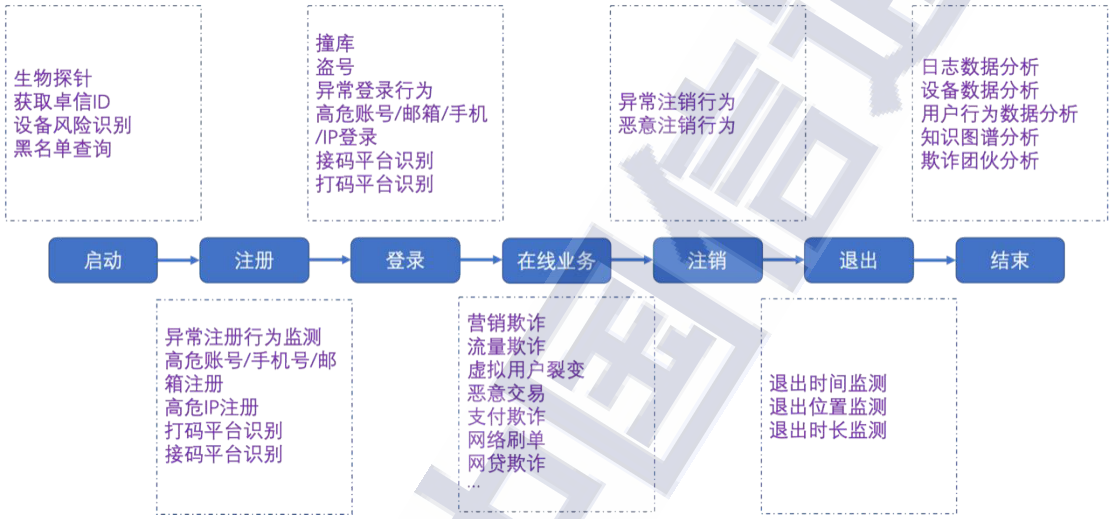
(四) 全生命周期互联网反欺诈模型

由于互联网欺诈工具繁多，场景丰富，技术发展迅速，传统单场景的、单技术手段的反欺诈模型已经很难取得较好的反欺诈效果，因此，建立全生命周期的互联网反欺诈模型成为互联网反欺诈技术发展的必然趋势。

全生命周期反欺诈模型涵盖从 APP 启动、账号注册、登录、产

生业务行为、注销账号、退出及事后数据分析的 APP 流量全过程。

通过建立全生命周期互联网反欺诈模型，可以实现不间断、全场景、全技术覆盖、立体多维的互联网欺诈防控体系，让防控速度更快，防控效果更加精准，最大限度帮助客户减少互联网欺诈造成的损失，促进互联网数字生态健康可持续发展。



来源：公开资料整理

图 38 全生命周期反欺诈模型

(五) 互联网反欺诈技术架构

互联网反欺诈技术架构应该同时支持实时、批量的欺诈数据分析架构，同时能够兼容黑白库、用户画像、规则引擎、机器学习、联邦学习等多种不同的防控算法策略。同时，技术架构应该有较好的横向和纵向扩展性，横向扩展可以支持更多的算法策略和业务场景，纵向扩展可以不断优化迭代现有算法体系，提高防控的准确度。

来源：公开资料整理

图 39 反欺诈技术架构

图 32 是互联网反欺诈的技术架构，从上至下分别为：设备风险识别层、行业反欺诈解决方案层、欺诈场景识别层、智能决策引擎层、数据缓存层和数据持久层。

设备风险识别层：该层的主要功能包括生成获取卓信 ID、通过生物探针获取用户行为数据、获取设备的活跃时间、获取设备 IP、获取设备地理位置信息、与设备绑定的智能验证码系统。

行业反欺诈解决方案层：针对不同行业，会建立不同的反欺诈解决方案，尤其在数据层和行业有关的一些垂直数据，以及和行业有关的一些特殊欺诈识别规则。

欺诈场景识别层：不同的欺诈场景，应用到的反欺诈模型、决

策算法以及相关的底层数据可能都不能。

智能决策引擎层：该层是反欺诈系统的核心，其技术是否先进，决定了反欺诈算法是否高效，是否精准，是否具有自进化能力。智能决策引擎涉及到的一些核心技术包括：实时指标计算、批量指标计算、实体画像引擎、黑白库维护引擎、基础 API、实时规则引擎、机器学习算法等。

数据缓存层：该层主要用于解决决策引擎和持久层数据读写速度不匹配的问题，智能决策引擎可以先将持久层数据库中的数据加载到数据缓存层，来提升决策引擎读取数据的效率，进而提升反欺诈系统的运行效率。

数据持久层：用于存储支撑决策引擎计算所需的各种数据，包括基础数据，黑白库、画像数据、规则数据、知识图谱和指标数据。

1. 基础 API 服务

基础 API 服务提供决策引擎与数据库之间的数据交互服务，一方面可以将决策引擎计算的结果存储到数据库中，也可以将决策引擎所需数据从数据库读取到内存中。

当基础 API 服务比较复杂时，可以应用微服务架构，来提升 API 服务的可维护性、安全性、可扩展性、稳定性和吞吐量。

2. 黑白库维护引擎

黑白库维护引擎通过对黑白库中已经存在的实体进行多维度综

合判定，如果黑库中已经存在的实体不再满足黑库的各项指标要求，则需要将实体从黑库中移出，如果黑库中的实体满足了白库的各项指标要求，则需要将实体从黑库移出同时将实体存入白库；同样的，如果白库中的实体不再满足白库的各项指标要求，需要将其从白库移出，如果该实体满足黑库的各项指标要求，则需要将其存入黑库。

3. 计算引擎

计算引擎一般可以分成批量计算引擎和实时计算引擎。批量计算引擎基于海量历史数据进行滚动计算，其特点是数据吞吐量大，时效性一般为 T-1。实时计算引擎基于实时数据流进行准实时计算，其时效性要求一般为秒级甚至毫秒级。

批量计算引擎的工作步骤一般为：增量或者全量从业务库中同步计算所需数据，建立维度表和事实表，根据度量和维度对数据进行建模，定时对计算各种指标的结果，并将结果存入到指标数据库。

实时计算引擎的工作步骤一般为：从消息队列中实时读取当前消息，根据实时指标的计算模型，对内存中当前的结果进行更新，同时将结果同步到硬盘上的指标数据库中。

4. 画像引擎

画像引擎是应用自然语言处理、实体识别、标签识别、关系识别等算法对实体进行打标签的工作模块。一个典型的反欺诈画像引擎的组成如 5-11 所示。

来源：公开资料整理

图 40 反欺诈画像引擎

5. 实时规则引擎

实时规则引擎是将各种数据（包括各种指标数据、实时数据）与欺诈识别规则进行实时匹配计算的工作模块。典型的实时规则引擎的组成如下图 34 所示:

来源：公开资料整理

图 41 实时规则引擎

规则管理模块负责规则的增加、修改、查询、删除等反欺诈规则的维护工作。

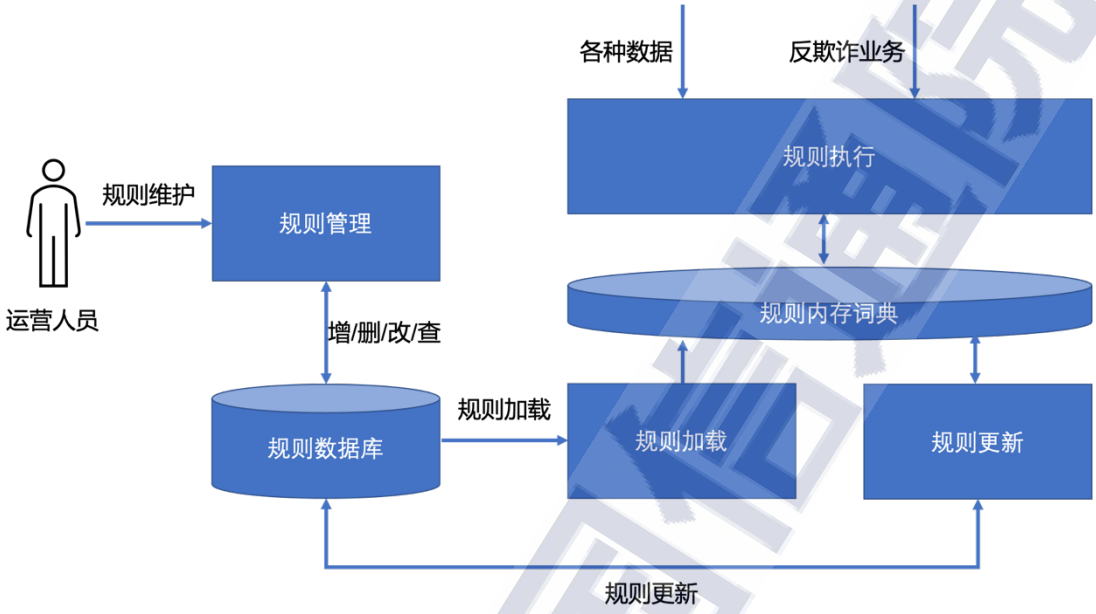
规则管理模块负责将数据库中的反欺诈规则加载到内存中。

规则更新模块负责定时对内存中的规则进行更新，规则更新模块每隔一段时间会依据规则 ID 去查询磁盘上规则的时间戳，如果时间戳发生变化时，则会将最新的规则加载到内存中。

规则执行模块将规则中的各个变量应用最新的数据进行初始

化，并依据判读规则的逻辑计算执行结果。

实时规则引擎的结构和执行原理如下图 35 所示。



来源：公开资料整理

图 42 规则引擎结构及执行原理

6. 机器学习

通过规则引擎来识别互联网欺诈行为，存在几个明显的缺点，比如：对策略人员的经验要求高、经常被黑产牵着鼻子走、误杀误伤的概率大、无法给出欺诈的风险概率等。为解决这些问题，近年来机器学习在反欺诈领域越来越受欢迎。

机器学习是一门交叉学科，涉及概率论、统计学、逼近论、凸分析、算法复杂度理论等多门学科。专门研究计算机怎样模拟或实现人类的学习行为，以获取新的知识或技能，重新组织已有的知识结构使之不断改善自身的性能。它是当前人工智能的核心实现方法之一，它主要使用归纳、综合而不是演绎，是使计算机具有智能的

一种有效途径，其应用遍及人工智能的各个领域，将机器学习应用于反欺诈领域，可以增强反欺诈系统的自学习和自进化能力，避免被黑灰产牵着鼻子走的情况,极大提升反欺诈系统的效率和准确性。

在反欺诈领域常见的机器学习算法有：有监督机器学习、无监督机器学习、深度学习以及联邦学习。为了识别欺诈团伙和欺诈实体的内外部关联性，今年将知识图谱也引入到机器学习算法中，提高欺诈识别的准确性。

（1） 有监督机器学习

有监督机器学习在连续数据集上表现就是回归分析，在离散数据集上的表现就是分类。有监督机器学习用于反欺诈业务，首先需要有大量的反欺诈运营人员对欺诈的特征和对应的可能欺诈行为进行标注，然后需要应用这些数据对反欺诈模型进行大量训练，模型稳定后才能应用到具体的反欺诈业务中。并且，一旦场景发生变化，或者主要特征发生变化都需要对模型重新训练。因此，有监督机器学习应用过程比较复杂，应用成本较高，并且模型的可扩展性和可进化能力较差，适合一些特征比较稳定的反欺诈场景。

（2） 无监督机器学习

为了解决有监督学习的问题，无监督学习应运而生。无监督学习无需对大量样本进行训练学习，无监督学习的典型应用场景是聚类。聚类的目的在于把相似的东西聚在一起，而我们并不关心这一类是什么。因此，一个聚类算法通常只需要知道如何计算相似度就

可以开始工作了。聚类算法一般有五种方法，最主要的是划分方法和层次方法两种。划分聚类算法通过优化评价函数把数据集分割为K个部分,它需要K作为输入参数。典型的分割聚类算法有K-means算法, K-medoids算法、CLARANS算法。层次聚类由不同层次的分割聚类组成，层次之间的分割具有嵌套的关系。它不需要输入参数，这是它优于分割聚类算法的一个明显的优点，其缺点是终止条件必须具体指定。典型分层聚类算法有BIRCH算法、DBSCAN算法和CURE算法等。

将无监督学习应用于反欺诈场景，相比有监督学习，使用成本大大下降，并且自进化能力也得到了增强，能够发现一些未知的欺诈行为和欺诈场景，目前，无监督机器学习在互联网反欺诈应用越来越多。

（3） 深度学习

传统的有监督学习和无监督学习都是浅层次的机器学习模型，浅层模型的一个典型特点，就是假设依靠人工经验选取特征。在模型运用不出错的前提下，如果客群及其环境没有发生较大变化，一套训练好的模型没有必要一次次的重复调优，因为特征是整个模型优化的瓶颈。但是，实际的反欺诈场景中，为了绕过反欺诈系统的检测，黑灰产团伙的行为特征经常会变化无常，因此，传统的浅层次的机器学习方法显得力不从心。

深度学习是无监督学习的一种，模仿人类大脑的机制对图像、

声音、文本等数据进行分析和学习。利用深度学习反欺诈，可以更加高效准确。人工设计样本特征的团队，经常将更多的人力投入到思考和发掘更多更好的特征上。若要发现一个优秀的特征，则要求工作人员反复摸索，并不是一个可拓展的途径，也无法满足于越来越大的数据。深度学习模型改变了这个模式，它和大数据二者则相辅相成，导入原始数据，通过搭建隐层的机器学习模型和海量的训练数据，逐层特征变换，挖掘和刻画客户数据的内在信息，学习更加有用的特征，提升预测的准确性，远远超出了传统风控基于评分卡系统的建模能力。

（4） 知识图谱

知识图谱本质上是语义网络，是一种基于图的数据结构，由节点(Point)和边(Edge)组成。在知识图谱里，每个节点表示现实世界中存在的“实体”，每条边为实体与实体之间的“关系”。知识图谱是关系的最有效的表示方式。通俗地讲，知识图谱就是把所有不同种类的信息连接在一起而得到的一个关系网络。知识图谱提供了从“关系”的角度去分析问题的能力。

基于大数据的反欺诈的难点在于如何把不同来源的数据（结构化，非结构）整合在一起，并构建反欺诈引擎，从而有效地识别出欺诈案件（比如身份造假，团体欺诈，代办包装等）。而且不少欺诈案件会涉及到复杂的关系网络，这也给欺诈审核带来了新的挑战。知识图谱，作为关系的直接表示方式，可以很好地解决这两个问题。

首先，知识图谱提供非常便捷的方式来添加新的数据源。其次，知识图谱本身就是用来表示关系的，这种直观的表示方法可以帮助我们更有效地分析复杂关系中存在的特定的潜在风险。

反欺诈的核心是人，首先需要把与借款人相关的所有的数据源打通，并构建包含多数据源的知识图谱，从而整合成为一台机器可以理解的结构化的知识。知识图谱不仅可以整合设备的基本信息，还可以把设备的消费记录、行为记录、网上的浏览记录等整合到知识图谱里，从而进行分析和预测。这里的一个难点是很多的数据都是从网络上获取的非结构化数据，需要利用机器学习、自然语言处理技术把这些数据变成结构化的数据。

相比虚假身份的识别，团伙欺诈的检测难度更大。这种组织在非常复杂的关系网络里隐藏着，不容易被发现。当只有把其中隐含的关系网络梳理清楚，才有可能去分析并发现其中潜在的风险。知识图谱，作为天然的关系网络的分析工具，可以帮助我们更容易地去识别这种潜在的风险。虽然识别团伙欺诈的方法有很多，但有一点值得肯定的是知识图谱一定会比其他任何的工具提供更便捷的分析手段。

（5） 联邦学习

近日，国际权威研究与咨询公司 Forrester 发布报告——《人工智能变革欺诈管理》,报告列举了多项应用于反欺诈领域的人工智能技术，包括知识图谱、监督学习等，并且首次提到了联邦学习的相

关实践。联邦学习是一种新型人工智能运用模式，通过交换加密的模型参数，帮助企业建立跨组织的机器学习模型，对联邦学习在反欺诈领域所发挥的作用予以了肯定。报告还以微众银行为例，列举了联邦学习在反欺诈领域的相关实践，“微众银行运用联邦学习技术进行商业银行合作，将模型性能提高了 13%”。

由于联邦学习解决了数据孤岛与隐私保护两大难道，成为近年来人工智能领域炙手可热的研究方向，联邦学习技术落地应用项目不断涌现，发展迅速，已经有不少企业利用联邦学习技术做出了实际成绩。

在国内，首倡联邦学习概念的微众银行通过将联邦学习用于反欺诈、智能服务、营销、零售等多个领域，取得了显著效果。其中自研的智能评分引擎在纵向联邦学习技术的基础上，联合开票金额与央行的征信数据等标签属性共同建模，将小微企业风控模型区分度（AUC of ROC）提升了 12%。

在实践落地应用之外，微众银行积极推动联邦学习生态建设，牵头国际标准制定、举办学术国际研讨会、并开源了全球首个工业级联邦学习框架 FATE(Federated AI Technology Enabler)。该框架支持多种主流算法，适配多种多方安全计算协议，简化了使用门槛，对开发者更为友好。目前 FATE 被纳入全球最大非营利技术社区 Linux Foundation、与腾讯云等多家企业和单位达成合作，对壮大联邦学习开发社区做出了巨大贡献。

联邦学习丰富的应用场景，吸引了众多企业参与其中。FaceBook 的深度学习框架 PyTorch，目前已经支持采用联邦学习方案来实现隐私保护，并同步推出 Secure and Private AI，将联邦学习技术应用到了消费者领域；平安科技推出联邦学习平台"蜂巢"；京东在智慧城市领域探索联邦学习的落地应用。

除了头部企业，该领域也涌现了不少创业公司，如 S20.ai、Owkin 和 Snips，都围绕联邦学习创建了新的工具和企业解决方案。越来越多的企业参与到了联邦学习理论标准与行业应用的建设中来，联邦学习势必会迎来更广阔的前景。在隐私保护法律法规日益趋紧的态势之下，数据利用面临重大挑战，也为联邦学习的推广创造了一个机遇。未来 5G 通信以及 AI 芯片等技术手段的突破，使终端设备在通信稳定性和算力方面进一步提升，将为联邦学习进一步发展奠定深厚的技术基础。

在互联网反欺诈领域，大量的多可利用的有效数据，如消费记录、交通出行记录、社交行为等封闭在各互联网企业的数据墙内，难以打通。运用联邦学习技术，可以在保护用户数据的情况下，将能证明设备欺诈行为的不同维度数据纳入联合风控建模，从而对设备的欺诈风险进行全维度模型评估。整个过程，因为同态加密等加密技术的保驾护航，数据始终处于暗箱状态，安全保密。

七、互联网反欺诈发展趋势

随着信息科技的发展，互联网企业和黑灰产之间的对抗也会越

来越激烈，整体而言，互联网黑灰产发展呈现以下趋势:

(1).**产业化程度越来越高。**随着数字技术的发展，互联网黑灰产产业链越来越成熟，上下游分工协作越来越紧密，产业化程度越来越高，单一的反欺诈手段已经很难凑效。

(2).**全球协同趋势正在形成。**黑灰产团体的协作已经突破国界，跨国配合越来越多，尤其是区块链技术出现后，跨国协作越来越方便，跨国灰色财产转移也越来越容易，这样给黑灰产团伙跨国开展欺诈活动提供了原始动力。

(3).**新的一些欺诈技术和工具正在形成。**应用区块链技术，让黑灰产团伙之间的配合越来越隐蔽；应用联邦学习技术，让黑灰产团伙之间的资源整合更加容易。

(4).**黑灰产造成的损失也越来越大。**互联网黑灰产团伙无孔不入，不仅威胁个人的财产安全，也威胁到企业的财产安全，甚至威胁政府和国家的安全。如 2020 年 12 月份的勒索病毒 DoppelPaymer 造成的损失达 3 亿人民币。

(5).**数字化升级的同时，黑灰产欺诈能力也在提升。**互联网欺诈新技术、新功能、新变种层出不穷，越来越多利用组合模式的传播手段和多种高级技术躲避查杀，致使破解难度越来越大，而且破解速度远远跟不上新病毒的推出速度。

为了应对日益猖獗的互联网欺诈活动，降低互联网欺诈造成的损失，为数字经济健康发展营造更加安全的环境，应该从以下几方面加强互联网反欺诈能力建设:

(1).政府应该加快互联网反欺诈相关法律法规建设，从法律层面

避免黑灰产有钻空子的可能性。

(2). 互联网企业应该联合起来，采用联邦学习、区块链黑白库共享等技术手段，提高联合抵御互联网欺诈的能力。

(3). 大力发展新的互联网反欺诈技术，推动互联网反欺诈技术的创新。

(4). 应用多层次、多维度、多场景、多数据、多算法融合的反欺诈防控体系，让黑灰产团伙无立足之地。

(5). 建立全球系统的反欺诈防控体系，联合主流的全球化互联网企业，在反欺诈领域达成共识，共同推动反欺诈体系建设。

中国信息通信研究院 泰尔终端实验室

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62300325

邮箱：nbd@caict.ac.cn

网址：www.caict.ac.cn