# 互联网金融反欺诈从 0 到 1

**全文总计 2.3w 字**

备注：部分内容来源于网络，如有侵权请私信管理 Vivian ID：wmyd80，谢谢。

目录

## 第一章 概述

### 1.1 业务现状

随着消费金融行业的兴起，欺诈风险日益成为阻碍行业的黑洞。尽管业内机构和监管部门对欺诈风险有极高的重视，欺诈案件依然是层出不穷。面对日益严峻的形式，从业人员需从源头做好每一步的风控工作。欺诈与反欺诈的较量，从来都是腥风血雨，剑拔弩张。用一句话概括就是：欺诈风险猛于虎，反欺诈刻不容缓。

近年来消费金融行业乱相，风控部门面对多重严峻考验，恶意欺诈、重复授信、多度消费等。

其中金融欺诈事件不断升级，使银行、消费金融公司等金融机构遭遇利益和声誉损失。过去的金融欺诈事件主要发生在小微贷款和信用卡诈骗业务领域,而随着电子技术和互联网技术的不断发展,金融欺诈逐渐渗透到一些其他的银行业务领域。

随着经济的发展，欺诈案件近些年逐渐呈现增长快、形态多、风险高等显著特点。

欺诈风险多环节渗透，从营销、注册、借贷、支付等可以说涵盖了风控贷前、贷中、贷后全流程。

## 1.2 欺诈定义

1.2.1 欺诈的法律风险（来源于百度）

第一百九十三条 有下列情形之一，以非法占有为目的，诈骗银行或者其他金融机构的贷款，数额较大的，处五年以下有期徒刑或者拘役，并处二万元以上二十万元以下罚金；数额巨大或者有其他严重情节的，处五年以上十年以下有期徒刑，并处五万元以上五十万元以下罚金；数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处五万元以上五十万元以下罚金或者没收财产：

（一）编造引进资金、项目等虚假理由的；

（二）使用虚假的经济合同的；

（三）使用虚假的证明文件的；

（四）使用虚假的产权证明作担保或者超出抵押物价值重复担保的；

（五）以其他方法诈骗贷款的。

1.2.2 欺诈定义（来源于百度）

虚假申请是指贷款申请人在提交申请材料时候，刻意伪造、盗用、隐瞒等手段对自身资质进行包装行为。备注：虚假申请未必都是恶意借款。（这个后面详细解释）

## 1.3 欺诈分类

1.3.1 欺诈分类（欺诈主体）

按照欺诈主体分类，分为第一方欺诈、第二方欺诈、第三方欺诈。欺诈主体不同，防范风险的形式也是不同。

第一方欺诈：即欺诈主体是申请者本人。

第二方欺诈：即欺诈主体是申请者亲戚朋友。

第三方欺诈：即欺诈主体盗用被人的身份信息进行欺诈。

1.3.2 欺诈分类（作案人数）

1.3.2.1 个人欺诈

这个很好理解是单独作案，一般常见的反欺诈手段法院执行名单、三方黑名单、三方欺诈分等等，相对容易识别到。

1.3.2.2 团体欺诈

这个就是团伙作案，关联了身份证信息、通讯录异常数据、IP 登录异常等等，使用社交关系图谱识别。

1.3.3 欺诈分类（表现形式）

按照欺诈表现形式分类，分为恶意借款、团伙欺诈、内外勾结、代办黑中介（黑产）、交易欺诈等。

1.3.3.1 恶意借款

指一部分故意借贷不换的老赖借款人。在网络借贷行业中，由于违约成本较低，征信体系不完善，存在部分借款人没有还款意愿，甚至有部分恶意借款人故意拖欠借款本息。说的通俗点就是人家来借款就压根儿没想着还钱。

1.3.3.2 团伙欺诈

除了单个个体进行骗贷外，团伙性质的黑产分子也是借贷结构经常面临的高风险根源之一。普通团队的欺诈者，通常是投机取巧型，对于骗贷会做充分的准备，期望一击必中。团伙成员的背景往往不同，但一般会有互补性，比如某成员有养卡经历，某成员是羊毛党，某成员懂得风控知识，组成团伙后分工不同，合作意
识较强。就怕流氓有文化，说的这些人。

普通团伙进行骗贷的一般流程是 ：

a 收集口子

b 买/养资料

c 探测规则

d 实际操作

1.3.3.3 内外勾结

是指信贷平台的内部工作人员与外部人员勾结，通过伪造资料等手段非法套取资金、骗贷形成的道德风险。发生内外勾 结的机构往往是内控工作出现重大漏斗。

我之前在某大型互联网金融甚至专门成立了廉政部，听起来像是港片里面的廉政公署，阿 sir 的感觉。该部门同事都是一些有经侦、刑侦公安背景的同事，专门查处这些违规的员工。虽然每周都是通报邮件，查处多少，开除多少。但是大家都知道如果不是金额特别巨大，基本都不会移交公安机关，毕竟立案也是有标准的。而且前端销售人员伪造个资料，或者伪装申请人的联系人接听个电话。这样的情况太常见了，有些时候前端业务部门施压，最多就是扣除当月绩效，通报批评而已。水至清则无鱼，这是我之前听到业务部门老大说的最经典的一句话。

1.3.3.4 代办黑中介（黑产）

黑中介是一群懂得风控技术、了解平台弱点、掌握信贷客源的人。黑中介本身不申请贷款、也不会放贷，而是帮助用户包装资料、炒作信用、骗取额度的黑产者。他们往往具有相当高的技巧，能够巧妙规避平台风控，能够远程给客户操作。通过这种方式他们从信贷客户处获得高额手续费。可以说黑中介是反欺诈从业者最难对付的敌人。

黑中介比团伙欺诈更有规模，更有组织性纪律性。通常是寻找一大波“肥羊”或者“白户”获取这些借款人的信息，哄骗能够借款而且还不用还款。去多家平台借款，但是下款到手后，只是给借款人一小部

分。

比如告诉你可以借款五万款，无抵押信用的，还不用还款。黑中介把申请资料各种工作证明、流水、房产证等进行伪造包装，去各个平台申请。到手可能是十万款，但是只是给借款人五万款。

互联网黑产发展到今天，已经形成了分工明确的上下游产业链，互通有无，术业有专攻。地理和人员分布广泛、关系网复杂，所以往往可以躲避风控的针对性的打击。而互联网反欺诈由于其特殊性，仍然相对割裂，同业间的交流仍然较少，意味着每个企业的反欺诈人员都是以一己之力对抗一个产业链。

## 1.4 信用风险与欺诈风险比较

在信贷业务风控中，信用风险和欺诈风险是相辅相成的两个维度。虽属不同的风险界定范畴，但是均涵盖在整个信贷信用风险管理生命周期中。

信用风险，评估的是客户的还款意愿和还款能力，要控制在一定范围的风险，权衡成本收益损失三者之间的关系，并不希望信用风险为零，信用风险框定在一定范围之内，再去设计产品。

欺诈风险（属于操作风险），彻底铲除零容忍。

信用风险是一场大规模正面战进攻战，相对有章可循，例如使用金融属性类数据（收入、负债）等来识别用户的还款能力和意愿。或者是像是警察执行巡逻。

那么反欺诈风险更像是一场小规模防守战，需要不断跟进欺诈风险事

件，快速响应，套路手法千奇百怪。

根据信贷场景的不同，信用风险和反欺诈风险侧重点不同。如金额较大的抵押类的业务通常更注重信用风险，金额较小的分期类业务通常更注重欺诈风险。

# 第二章 互联网反欺诈常见手段解析

## 2.1 名单库筛选（黑白名单）

## 2.2 生物识别

## 2.3 规则引擎

## 2.4 专家规则

## 2.5 机器学习

### 2.1 名单库筛选（黑白名单）

名单库筛选就是我们常说的黑白名单，经常作为互联网反欺诈的第一道过滤网使用。

一般通过平台内部进行积累，或与其他合作机构合作进行获取。黑名单在很大程度上避免了重复欺诈行为的发生，也是一种逻辑简单、成本较低的反欺诈手段。

当然，黑名单覆盖群体较小、需要时间积累，也存在准确率较低、名单库易污染等缺点。同理，白名单一般指平台内部的优质客户列表，建立白名单库可以有效且降低公司的成本和信用风险，提高放款效率。

通过内部积累、外部获取的各种人员、手机号、设备、IP 等黑、白名单对欺诈行为进行判断，是一种实施简单、成本较低的反欺诈手段。与此同时，信誉库也存在着准确度低、覆盖面窄的缺陷和不足。

黑名单的优缺点十分明显，优点就是简单方便，各行各业各产品的反欺诈都可以用黑名单，缺点就是无法发现新骗子。

## 2.2 生物识别

之前在针对于贷前风控手段识别中，曾经详细的说明。目前活体识别对于欺诈风险的识别是非常简单直接有效的。

2.2.1 人脸识别

2.2.2 声音识别

2.2.3 虹膜识别

## 2.3 规则引擎

目前大部分规则是模型，比如从贷前准入、认证、支用等。这些规则引擎，是经常要更新的。在业务流程过程中做部署，配置简单，维护方便，可检测到新的欺诈缺点是需要经常性维护，而有时经验也会出错，更新的速度慢，对新的欺诈模式不敏感，更多依赖有经验的专家策略去发现新的漏洞。对用户各种数据的采用聚类分析、交叉验证、勾稽关系比对、强特征筛选等手段，通过风险决策引擎进行决策判断。

1、新用户欺诈检测

2、老用户欺诈防范

我们常说黑名单的升级版本是规则引擎，还是拿退货险举例。之前，保险公司拿着一个清单来比对哪些人可以购买退货险，经过一段时间的积累，保险公司发现，退货比例超过 80%的用户极可能再次退货，疑似骗保。或者连续退货超过 5 次的用户的骗保嫌疑也非常大。于是乎，保险公司设定了一个阈值，规则如下：

1. 连续退货 5 次的用户，拒绝其购买退货险。

2. 退货比例超过 80%，拒绝其再次购买退货险。

很明显，只要符合这两种规则的任何一个，就会被保险公司拒之门外。这相比于黑名单，可以检测到新的欺诈者，算是进了一大步。但是，规则引擎却无法检测到新的欺诈模式。

规则引擎通常可配合黑名单一起使用，通过规则引擎抓到的坏人被列到黑名单中。

规则引擎的规则是如何生成的？答案是：经验！这听起来有点不靠谱，万一经验错了怎么办？正因为经验的不确定性，规则通常需要投入大量的精力维护，不断更新、修改、删除、添加等等。

## 2.4 专家规则

首先先纠正一个误区啊，专家策略真的不是简单拍脑袋，其实反欺诈策略往往基于策略人员以往的经验和踩过的“坑”，并以研究欺诈者的行为和心理为基础而制定。和建模评分卡一样，前期业务初期，数据量较少。通常都是依托于专家策略进行业务冷启动，等数据积累到一定量时候再进行建模决策引擎。专家策略通常较为成熟，申请环节

一旦触发反欺诈规则即被认定为欺诈行为。

专家规则是目前较为成熟的反欺诈方法和手段，主要是基于反欺诈策略人员的经验和教训，制定反欺诈规则。当用户的操作请求和操作行为触发了反欺诈规则时，即被认定为欺诈行为并启动拦截，常见的如各种聚集度规则等。

专家规则的优势在于实现较为简单、可结实性强，但缺陷在于专家规则存在有严重的滞后性，对于新出现的欺诈手段和方法无法及时的进行应对，往往需要着付出大量损失后才能总结教训提取新的规则。此外，由于人脑的限制，专家规则只能使用一个或几个维度的标量进行计算和识别，往往存在有较大的误报率。但是不得不说的一点就是，专家策略也是有一定局限性。那就是误杀或者说错杀，而误杀率的高低取决于专家策略人员的经验水平。并且其专家反欺诈策略需要根据业务随时更新，并要严格保密。

专家规则严重依赖于策略人员的经验和教训，不同水平的策略人员制定的专家规则效果也会纯在较大区别，主要可以作为互联网反欺诈的应急响应手段和兜底防线。

贷前反欺诈一般都是先有专家策略进行冷启动，等数据积累到一定程度的时再慢慢地对数据进行挖掘，并对策略进行调优或者构建模型。很多人都觉得专家策略不过是“拍脑袋”，其实反欺诈策略往往基于策略人员以往的经验和踩过的“坑”，并以研究欺诈者的行为和心理为基础而制定。而且，目前的信贷反欺诈手段中，专家策略比较常用

且较为成熟。当借款人的操作请求和操作行为触发反欺诈规则、并达到一定的程度时，即被认定为欺诈行为。合作方可以启动拦截，或进行人工审核，如客户的行为异常监测策略、设备类异常策略、聚集度策略等。

现在欺诈手段日新月异，欺诈人员和策略人员处于攻与防的角色，如果无法在第一时间做出反应，需要事后进行大量的数据分析和挖掘后才能提取新的特征和规则。而专家策略往往存在一定程度上的误杀率，而误杀率的高低取决于策略人员的经验水平，不同的策略人员制定的专家策略也会存在较大的区别，呈现不同的效果。此外，策略需要不定期进行更新，并要严格保密，一旦泄露将对平台造成不可挽回的损失。因此，专家策略实现简单，可解释性强，但会存在滞后性。

## 2.5 机器学习

机器学习反欺诈是近年来比较火的一种反欺诈方法，目前也取得了一定的成果。主要是通过机器学习方法，将用户各个维度的数据和特征，与欺诈建立起关联关系，并给出欺诈的概率。

常见的机器学习反欺诈分为有监督和无监督两种。

### 2.5.1 有监督学习

有监督机器学习反欺诈是目前机器学习反欺诈中较为成熟的一种方法。

它通过大量客户的历史表现数据，进行标签化，并利用相关算法，提取特征，发现欺诈行为的共同点，进行识别。而无监督机器学习反欺

诈则相对较新，只是通过对用户的各纬度数据特征的聚类，找出与大多数用户和行为差异较大的用户和操作请求，并予以拦截。采用无监督机器学习，可以有效地识别团伙欺诈行为， 让欺诈团伙无处遁行。

优势：可处理多维数据，可识别已知欺诈风险 。

局限：需要大量训练数据和大量时间，无法应对变化的欺诈行为，无法识别未知欺诈 。

### 2.5.2 无监督学习

无监督机器学习反欺诈是近来行业内出现的一种新兴思路，也成为一些公司的卖点，但迄今为止尚未出现较为成熟和经过实践验证的解决方案。

相对于有监督机器学习的反欺诈，无监督机器学习的反欺诈方法不需要预先标记欺诈行为，而是通过对所有用户和所有操作行为各纬度数据和标签的聚类，找出与大多数用户和行为差异较大的用户和操作请求，并予以拦截。

理论上，基于无监督机器学习的反欺诈方法可以使得反欺诈人员摆脱被动防守的局面。但是由于无监督机器学习算法对于数据的广度、数据使用的深度都有着极其高的要求，因此无监督机器学习算法的效果仍需等待实践的检验。

优势：不需训练数据，可快速识别欺诈风险。可自我总结规则，补充规则引擎和黑白名单，识别未知欺诈

局限：不适用于个人欺诈场景，较为适合团伙欺诈，需检验模型有效

性。

反欺诈是贯穿于整个信贷业务周期，即贷前识别+贷中监控+贷后修复。

综上，反欺诈的方法虽然很多，没有最好的方式只有最适合的方法。

# 第三章 如何搭建全流程反欺诈体系

## 3.1 业务现状

## 3.2 风控各阶段面临的欺诈风险

## 3.3 风控反欺诈体系建设思路

## 3.4 风控全流程生命周期管理

## 3.5 风控反欺诈方案评估

## 3.1 业务现状

互联网金融，尤其是消费金融行业规模发展趋势都是比较快，主要是基于场景线上的小额分散的业务。一定程度上无法有效和及时识别真正的客户，某些消费场景内面对欺诈团伙和黑产建立有效和多种风控手段和模型。

基于大数据的风控核反欺诈模型起步较晚，大部分公司都在逐渐完善和成熟的过程，基于机器学习的分析概念模型也是都在大量的投入和尝试。需要从大数据上进行挖掘、分析、建模，利用用户身份数据、行为数据、外部数据和黑产数据建立反欺诈平台、规则和欺诈关联网络来提高反欺诈能力和风险识别能力。

信用风险的风控重点在于，甄别客户违约的原因究竟是还款能力还是还款意愿。如果客户真的由于各方面原因，暂时不具备还款能力，这是概率问题。即便发生了，属于个别事件，对于公司整体资产也不会造成巨大损失。但是如果是还款意愿问题，那么就会存在资金损失潜在风险。

目前在整体风险控制工作中反欺诈是重中之重，因为欺诈风险其危害远比信用风险。要大得多，一般来说正常的客户逾期，如果不是故意骗贷，只是暂时资金问题，比如说家中出现突发事件，更换工作时等原因导致资金无法周转而逾期的。这毕竟是少数，而且借款只是逾期，其还款的概率还是比较高的。但是目前互联网金融行业，尤其是消费金融行业大部分的不良都是因为欺诈引起的。

目前消费金融发放的借款都是线上小额分散的，没有线下任何抵押和担保的情况。随着业务发展规模扩大，整个行业面临欺诈问题越来越严重，羊毛党和黑产层出不穷。

欺诈风险目前是整体消费金融的重点，不完全统计目前整个行业超过百分之八十的风险都是来自欺诈风险。形式多种多样，如常见的身份伪冒、中介黑产、伪造材料、 恶意套现等。欺诈主题主体意识申请本人或者亲戚朋友，借用或者盗用别人的身份信息进行欺诈。欺诈主题的不同，防范风险的手段和形式也是不同。

欺诈风险常见的伪冒申请，申请身份的造假，申请人盗取他人身份信息与申请资源，仿冒他们身份骗取贷款。比如黑中介。虚假资料，申

请人与身份或者资质证明材料进行造假，伪造工作单位、工资流水、住宅地址、想通过审批或者获取更高额度。内部欺诈，外部欺诈分子与内部销售人员，甚至风控人员内外勾结，里应外合，泄露公司信审策略和用户信息，非法套现。

## 3.2 风控各阶段面临的欺诈风险

欺诈风险贯穿于整个业务之中，所以反欺诈工作也是而不是我们较为熟悉的贷前准入环节，是在风控全流程中。首先先看下不同阶段面临的不同欺诈风险。

3.2.1 贷前准入（欺诈识别）

在信贷申请环节，反欺诈工作主要为客户身份核验、银行卡核验、运营商核验、黑灰名单以及关系图谱等进行反欺诈策略的提取、测试和框架搭建。

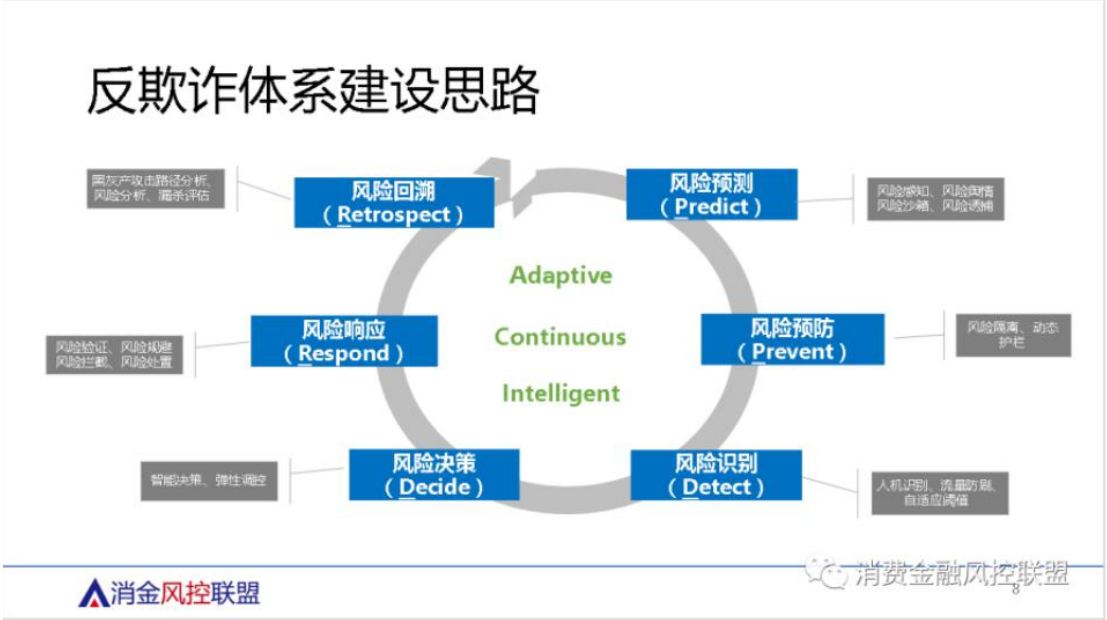
3.2.2 贷中监控（欺诈监控）

在贷中反欺诈环节，反欺诈工作重点集中在贷度监控、风险异常排查以及交易监控等多维度去构建监控框架。

3.2.3 贷后管控（欺诈判定）

在贷后反欺诈环节，反欺诈工作重点在逾期失联客户的排查、失联信息修复以及欺诈发生资产构建贷保全的欺诈框架。

## 3.3 风控反欺诈体系建设思路




反欺诈体系的搭建的思路首先要形成一个完整的闭环。

3.3.1 风控预测

风险感知、风险舆情、风险沙箱、风险诱捕

3.3.2 风险预防

风险隔离、动态护栏

3.3.3 风险识别

人机识别、流量防刷、自适应阈值

3.3.4 风险决策

智能决策、弹性调控

3.3.5 风险相应

风险验证、风险规避、风险拦截、风险处理

3.3.6 风险回溯

黑灰产攻击路径分析、风险分析、漏杀评估

随着互联网技术不断发展，电商行业也是蓬勃发展。但是伴随而来的

是互联网大幅的降低了欺诈成本，提高了欺诈的效率。黑产团伙在互联网的加持之下，欺诈资源更为丰富，欺诈手法多种多样且灵活多变。并且迅速的开始规模化、产业化和专业化专业链条。

因此在构建电商反欺诈体系时候需要特别注意的三点

1、准确性

我们的原则是不放走一个坏人但是也不能冤枉一个好人。电商平台考虑到其获客成本，用户购买体验等因素。其反欺诈体系必须能够在非常短的时间内对欺诈行为进行认定判断。对于注册、登陆、支付等一些场景，必须能够在用户无感的情况下对欺诈行为进行检测认定。

2、自动性

历史我们很多欺诈手段经验都需要有人工介入的环节进行操作。但是由于电商平台特有的准确性要求，决定了互联网业务无法通过人工操作进行反欺诈，必须使用更加高效的自动化操作。

3、数据性

自动化的本质是要求有强大的数据支撑，俗话说巧妇难为无米之炊。没有数据基础谈何自动化，而数据采集、挖掘和分析、建模能力直接决定了互联网反欺诈能力的高低。所以为什么说 TOP 大厂的反欺诈体系如何如何好，就是因为前期积累了丰富的数据基础，而这些一手数据都是真实有效的。

## 3.4 风控全流程生命周期管理

这里说的全流程风险管理，特指的是线上业务，还是以消费金融业务为例。

一个完整风控平台需要包括对借款申请全生命周期进行管理，是一个极为复杂的过程，每一个流程都会影响整体的风控质量。

风控平台是相对独立的系统，信审的案件可以从借款端平台推过来，也可以从第三方平台推过来。案件到达风控平台后，自动创建工作流，根据风控流程处理各流程环节任务。

在此我们没有按照贷前贷中贷后三个环节划分，而是从申请人角度从操作层面上， 把线上业务进行流程划分：注册-登录-申请-审核-放款-催收。为了方便大家理解， 我们简要罗列下每个业务环节的风控点。

3.4.1 注册

身份冒用、集中区域注册、批量注册、注册行为分析、黑名单库、多次注册

3.4.2 登录

异常登录、瞬间转移、暴力破解，账户盗用、模拟器、多冲验证

3.4.3 申请

黑名单、规则效验、第三方认证、身份确认、资料效验、人工介入

3.4.4 信审

自动决策、欺诈风险、还款能力、评分、名单、人工处理

3.4.5 放款

虚假交易、套现风险、欺诈风险、黑名单、异常操作、行为分析

3.4.6 催收

提前催收、信用评级、自动催收、人工处理、信用评估、行为识别

## 3.5 风控反欺诈方案评估

反欺诈方案好不好，是否准确，需要不断评估并进行优化。相应的数据指标暂不提及，仅针对于常规评估方案讨论~

3.5.1 预测

在业务开展前，根据用户风险情报库进行反欺诈评估，现阶段的限制因素，实施的滞后性。同时，建立反欺诈风险情报库，不断总结风险点，完善用户风险情报库。

3.5.2 分析

将欺诈行为划分风险等级，根据不同的风险等级采取相应的措施。

欺诈风险等级：

低级风险：匹配单一低风险策略，正常操作，后续重点关注。

中级风险：匹配多个低风险或者中风险策略，需进行二次校验，若判定

高风险客户直接拒绝。

高级风险：匹配多个中风险或者高风险策略，直接拒绝。

为避免误杀，需要定期对反欺诈规则进行更新验证。如反欺诈风险模型调整，反欺诈数据分析等。

3.5.3 总结

欺诈分析需要全方位的分析，需要选取全量业务数据进行欺诈行为分析。分析的准确度占比、误杀数据占比、遗漏数据占比等。

全面评估，更好的优化反欺诈分析模型，提高反欺诈方案准确度。

# 第四章 反欺诈平台解析

目前欺诈团伙已经形成完整的地下产业链，反欺诈平台需要跟平台沉淀的用户数据， 环境数据，第三方数据结合生物探针技术采集的用户行为数据，建立用户、环境、行为画像以及基于用户、环境、行为的关系网络，通过对业务数据建立多重模型来甄别对异常用户的识别能力和反欺诈能力。

4.1 数据来源

4.2 数据分类

## 4.1 数据来源

4.1.1 内部获取：申请人在申请过程中填写的数据和以及埋点时采集的行为数据和日志数据。

4.1.2 外部购买：第三方合作数据及购买，如人行征信数据、学历、多头借贷等数据。

4.1.3 外部获取：互联网公开数据，需要靠技术团队实现获取。

## 4.2 数据分类

4.2.1 基本信息：一般是身份基本信息数据，如姓名、身份证号码、手机号码、银行卡号、学历等。

4.2.2 信用信息：一般是征信数据，如借款信息、账户信息、还款信息和逾期信息等。

4.2.3 消费信息：银行卡详单、电商网站如淘宝京东等购买信息等。

4.2.4 社交信息：一般需要客户授权获取，如通讯录信息、通话记录、QQ 和其他平台交互信息。

4.2.5 行为信息：一般是依靠埋点抓取，如申请和填写信息、GPS、时间点、地点等。

4.2.6 第三方信息：一般是外部获取的，使用前需要甄别真实度及准确度。如多头借贷、黑灰名单、授信信息等。

# 第五章 反欺诈模型搭建

## 5.1 反欺诈模型分类

## 5.2 欺诈团伙特征及应对

## 5.3 反欺诈评分模型和反欺诈规则比较

## 5.1 反欺诈模型分类

但我们获取了多方数据后，可以根据对用户行为、语义、关联网络等组成一个巨大 的数据关系图谱。利用这些数据建立的模型风控体系对用户的欺诈概率、还款风险等进行强有力的预测和判断。

5.1 反欺诈模型分类

5.1.1 社交图谱模型（用户画像）

利用手机-设备，手机-手机（通话）关系，常见的是将所有用户及外部已知风险手机号容纳在一张图中，通过图中的风险标记以及图中的异常关系结构。用户数量上来的时候，社交关系很容易破亿，这个时候就要使用图数据库。

5.1.2 多头授信模型

通过对客户与各类结构的通信关系，发现一些体现多头风控异常机构，如客户总和催收机构联系。

5.1.3 黑产攻击模型

通过分析手机的高风险人群及中介通话数据，挖掘出一张高风险人群联系密切的关系网，有效识别申请动机不良的客户，发现黑产攻击苗头。

5.1.4 欺诈团伙特征分析及应对

欺诈团伙在发现系统规则漏洞时，往往会在短时间内发起大量欺诈交易，必变在受害者反应过来前尽快变现。

这种交易的频次通常会在时间分布上形成异常的波形。通过模型可用很好的预测时间的时间分布特征，叶贝斯框架的生成式模型能够解决不同空间分布维度下细颗粒的时间分布问题。通过这两种手段可以将时间和空间分布上存在异常的交易行为与正常的交易行为区分开。

## 5.2 欺诈团伙特征及应对

所谓道高一尺魔高一丈，在互联网金融行业，欺诈团伙日益严重并且

难易防范。5.2.1 团伙欺诈特点

5.2.1.1 专业性

目前欺诈团伙利用科技手段不断去试探各平台的风控规则，从而制定相应的欺诈手段。

5.2.1.2 集中性

欺诈案件一般是短期批量集中产生，欺诈团伙一旦发现欺诈的可能性，会在短时间内，利用地下渠道获取身份信息，批量操作。我们之前说的薅羊毛也是这样表现形式。

5.2.1.3 多变性

欺诈团伙的欺诈手法经常变化，让各个平台防不胜防。

5.2.2 反欺诈团伙技术思路

面对欺诈团队的重要挑战，目前反欺诈团伙技术思路如下：

5.2.2.1 黑名单库：最为简单直接有效的方式，利用已有发现等算法得到的欺诈相关程度预测。

5.2.2.2 构成网络：将交易，交易信息项（地址、电话、设备 ID），用户等定义为节点，同属一个交易的节点间形成边，对边根据业务经验或者按照其他规则赋予权重。

5.2.2.3 特征工程：提取网络饱和度，网络直径，关联度，中心度，群聚系数等特征。

5.2.2.4 加入模型：提取的特征可以作为模型或者规则的输入。

5.2.2.5 欺诈预警：在无标注数据的情况，及时发现异常的网络拓扑

结构，作为欺诈的早期预警。

IV 值预测方法及使用方法，具体业务请根据场景而定。

小于 0.02，该特征基本没有预测能力，不建议使用评分模型。

大于等于 0.02 且小于 0.1，该特征的预测能力较弱，不建议使用评分模型。

大于等于 0.1 且小于 0.3，该特征的预测能力中等，建议使用评分模型。

大于等于 0.3 且小于 0.5，该特征预测能力较强，建议使用评分模型。

大于等于 0.5，该特征的预测能力过好，不适合搭建评分模型，建议使用规则系统。

## 5.3 反欺诈评分模型和反欺诈规则比较

公司将评分模型应用到反欺诈场景时常与信用评分混淆。本质上，二者的预测目标是不同的，反欺诈模型预测的是欺诈的可能性，信用模型预测的是还款的可能性。

### 5.3.1 反欺诈规则

优点：可解释性强，可以迅速调整，应对欺诈手段变化

局限：复杂的规则体系难于维护，难易利用弱特征，对强特征依赖，容易被攻破

### 5.3.2 反欺诈评分模型

评分模型在金融领域应用相当成熟，信用评分模型是最常见的应用，

建立独立的反欺诈评分模型很有必要。

反欺诈评分模型和反欺诈规则系统有很好的互补性，在风控平台中，一般是建议同时建立起反欺诈规则系统和评分模型。

## 第六章 常见反欺诈策略

反欺诈这个话题比较大，能力有限仅谈一下实际工作中遇到的东西。这里主要谈一下中小微贷款的申请反欺诈，不谈交易类反欺诈等。我个人认为只要涉及到与“待确认条件不符的”都是反欺诈里的内容。常见的反欺诈手段有这么几种。

1、申请人年龄、学历与当期情况不符合准入条件。GPS 信息属于禁止范围之内。

2、人脸识别中识别率过低，身份证与申请人不符合某一阀值。

3、通话详单欺诈与疑似欺诈。例如手机实名不符、通话费用过少、某段时间内通话累计时长过少、通话详单中姓名认证不符合、通讯录呼入呼出交叉对比不符合条件、通讯录中含有敏感词关键字、通讯录数据数量过少等

4、多头借贷。银行类机构或非银类机构借款数量过多、逾期过长、未还款次数过多。

5、人行征信。人行白户或者信用卡逾期严重。

6、机构拒绝。银行类或非银类非准入条件被拒次数过多，某时间段内申请过多。

7、设备拒绝。涉嫌诈骗类设备、虚拟设备、虚拟交易过多、以及延伸出来的，设备申请、逾期、拒绝等过多。

8、欺诈团队的设备虚拟与团伙诈骗的集中性。但是对于高明的欺诈团队我个人无能为力。

9、其他的还有一些，比如 IP 验证服务或者反欺诈或者 GPS 信息反欺诈。

10、三网数据的一些反欺诈以及三网涉不良信息等。

11、比如申请用户的手机号、身份证在多平台申请或者发生逾期。通讯录 TOPX、常用联系人也是如此。在延伸一下 1、2、3 度人脉的相关联反欺诈（用知识图谱做的三度人脉反欺诈效果还是不错的。有能力的朋友们可以尝试一下）。现在很多产品都愿意获取社保数据，因为社保数据相对来说不太容易造假（听业内好朋友反馈的信息，笔者未曾亲自验证过。）对于某些场景下的，例如司机验证，货车验证、商户验证的信息，笔者没有使用过也无法给出明确的答案。因反欺诈内容比较多。对于纯线上的交易，结合各种数据可以识别大部分。对于线下交易以及重要资产的重点都已银行类征信数据为准。

这里就不一一举例了。实在是能力有限不敢造次。说明一下，很多反欺诈及疑似欺诈的阀值调整是很有技术含量的，如果没有一些经验瞎设置是非常令人佩服勇气的一件事情。还有一件事情，对于欺诈团队，如果在 P2P 欺诈了，那么 3C 欺诈类、医疗美容欺诈依然有效。毕竟欺诈团队也是打一枪换一炮的。只要有留痕了，总会被发现的。从接三方数据角度来说，重点分为：通讯类、设备类、X 要素类。如果有条件多接几家不是坏事。哪怕一万个里面能防住一个也算是减少损失了。

另外：黑名单不同于欺诈。黑名单有些数据是不可共用的，但是欺诈的数据相对通用性比较大，个人建议采用。

总之吧，反欺诈任重而道远，取各家之所长才能为产品更好的服务。反欺诈体系里面的专业内容及方法论。不管是从流程还是数据层面，但是他也有自己的短板。BATJ 中的 J 还些许了解了一些。对了，B 有反欺诈吗？我都不知道 T 的反欺诈讲的是啥。J 的反欺诈，至少用户的购买地址多半都是真实的。毕竟反欺诈大数据 BATJ 还是存在非常好的基础的，相信未来他们会做的更好。

# 第七章 风控反欺诈之设备信息

## 7.1 现状

## 7.2 定义

## 7.3 常见元素

## 7.4 设备指纹历史应用场景

## 7.5 设备指纹目前应用场景

## 7.6 好的设备指纹产品特性

## 7.7 设备信息集成方式

## 7.8 设备指纹生成方式（技术实现方式）

## 7.9 分享举例

### 7.1 现状

随时互联网金融行业的发展，面临的黑产挑战越发严峻。而设备指纹

在风控反欺诈中发挥着很重要的作用。今天仅针对于反欺诈之设备信息的全貌和关键细节介绍，应用场景不做深入解析。

反欺诈是风控的一个重要环节，也是一个很重要的技术范围。现在的贷款领域，多是采用获取用户设备指纹，获取通讯录，以及运营商报告，甚至其他外卖，网约车，社保，公积金，淘宝等的历史消费信息，依赖此进行审核，从而确定是否放贷以及提额或者降额标准。而在线交易本身很难进行唯一性身份确认，需要其他信息辅助判断，用户是否为本人操作等各种行为确认和行为分析。设备信息的应用就显得尤为重要。

## 7.2 定义

用我们个人身份证举例子，可以把手机设备理解成一个人，姓名（设备名称），身份证号码（设备序列号），身份证没有没有冒用（设备盗用篡改假冒等）。

所以说设备信息就是用于唯一标识出该设备的设备特征或者独特的设备标识。

## 7.3 常见元素

一般都是基于某些设备信息，通过一些设备指纹算法会将这些信息组合起来，作为该设备的唯一标识符，常见的元素如下

7.3.1SIM 卡信息

7.3.2WIFI 信息

7.3.3 硬盘信息

7.3.4 内存信息

7.3.5 摄像头信息

7.3.6 软件版本以及其他硬件信息

设备指纹一般都是基于以上内容，进行一个唯一 hash 值得构建，但是这方面就会有偏差，ios 的设备有些信息是无法获取到的，安卓会好很多，但是有人会说

H5 呢，怎么办？这个就各个公司不一样了，有能力的，可以采用一些底层协议，

比如通过构建一个 http 请求，tcp 层甚至链路层去分析协议，从而构建唯一 hash， 有些还可以通过渲染一个图像，记录像素情况，耗用情况以及渲染时间，甚至渲 染过程，从而构建唯一 hash，其目的一般是为了标识唯一设备。就比如每个人都有不一样的指纹，重复的概率低之又低，如果有个全人类的指纹库，那么根据指纹就能找到对应的人。

设备指纹的目的，一方面是嵌入 sdk，获取众多设备甚至手机 app 使用情况等信息，一方面就是标识这个设备。这样，同一个设备在不同平台，甚至不同人基于同一个手机去贷款，就很方便标识出来了。具体使用上，不同公司是不一样的，有的关注 GPS，有的关注 ip，有的关注硬盘信息甚至 wifi 列表，这个就看如何应用。

## 7.4 设备指纹历史应用场景

早期，在一些对安全要求非常高的线上场景中，例如网上银行在线交，常常使用纯 U 盾这样的纯硬件技术去追踪业务主体。虽然这很安全，但是随着互联网的发展，这种“控件”+“U 盾”的结合方式已经越来越落伍。

7.4.1 用户体验非常差

需要冗长安装、更新流程，普通用户难以操作，使用不够友好。

7.4.2 移动互联网的发展

而 iOS，Android 等移动互联网入口都不支持控件。

7.4.3 使用范围的狭隘

不仅仅在移动端，某些控件在 pc 端适用范围都很小，很多只支持 PC 上的 IE 内核浏览器。同时 Chrome 和 Firefox 等份额较大的桌面浏览器也在逐步淘汰控件的使用。

7.4.4 漏洞风险加大

基于控件的本地溢出漏洞层出不穷，用户很容易中木马或者 被钓鱼，反而给系统的安全造成严重危害。

由于业务场景实际需要，设备指纹产品应运而生。设备指纹技术可以为每一个操作设备生成一个全球唯一的设备 ID，用于唯一表示出该设备特征。

## 7.5 设备指纹目前应用场景

防垃圾注册、防撞库、防薅羊毛、反刷单、精准营销、支付反欺诈、授信反欺诈、用户画像分析、复杂关系网络等，涉及领域电商、支付、

信贷等。仅依赖 IMEI 和 IDFA 这种易篡改很那满足业务快速发展的防控需要。

互联网金融业务流程中常见的业务流程

7.5.1 授信审批

7.5.1.1 注册：可疑设备感知，恶意注册防范

7.5.1.2 申请：手机信用卡、网络发卡识别信用卡欺诈申请（高风险申请）

7.5.2 交易监控

7.5.2.1 登录、密码找回：可以设备感知

7.5.2.2 支付：支付交易密码

7.5.2.3 欺诈交易：支付是否常用设备等

7.5.2.4 团伙欺诈：刷信用、刷流水、薅羊毛、刷单、洗钱

7.5.2.5 敏感交易前的可疑设备感知

## 7.6 好的设备指纹产品特性

从用户体验角度上，用户无感知，具有免安装、动态更新、跨平台兼容、防篡改等。

7.6.1 准确性

准确率高，不同设备生成的设备指纹保证不会重复，确保设备指纹生成的唯一性。个人的常用设备总是有限的，一段时间内一般不会超过 5 个以上。

7.6.1.1 主动采集要素、精准识别设备

7.6.1.2 多维度要素综合决策

7.6.2 设备系统升级或少量参数变更，设备指纹码不会发生变更。

7.6.2.1 结合被动采集要素。多维度决策增强稳定性

7.6.2.2 适配时间、空间、操作变化

7.6.3 安全性

不会再网络传输中杯篡改、注入导致生成设备伪码。

7.6.3.1 识别终端环境风险

7.6.3.2 防篡改、防盗用、接口反作弊

7.6.4 易用性

7.6.4.1 支持本地话部署或者云模式

7.6.4.2 业务系统埋点成本低

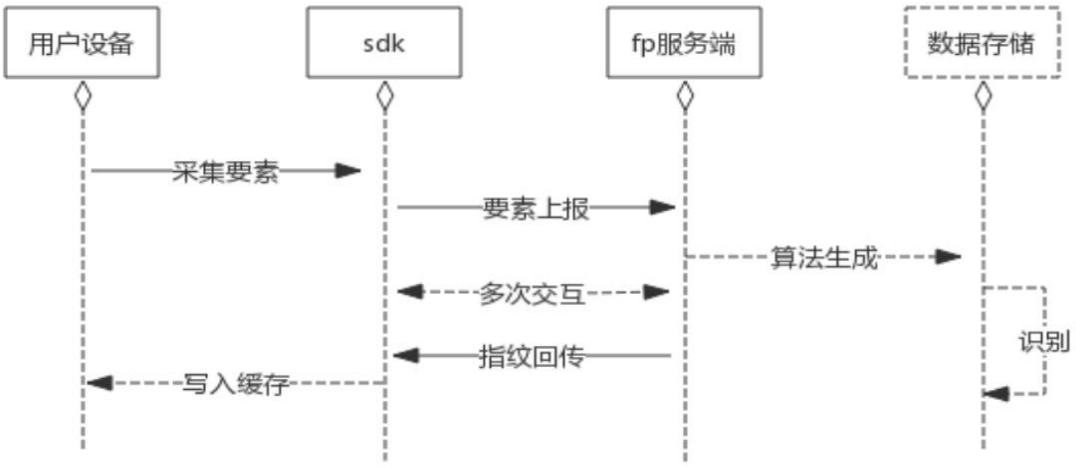
7.6.5 适用性

7.6.5.1 服务消耗资源少

7.6.5.2 本地化部署延迟 100ms 之内

## 7.7 设备信息集成方式

集成方式：浏览器（即 web/wap）植入 JS 集成，APP 通过 SDK 集成实现。如上图，客户端集成非常简单，只需要几行代码，核心在于采集要素传输加密和服务端算法加工。




备注：图片来源于网络，侵删

采集要素即设备中的硬件本身信息以及软件设置信息。

采集要素示例（部分）：CPU 指令集、蓝牙 MAC 地址、硬件信息、制造商、设备显示的版本包、厂商信息、屏幕分辨率信息、系统版本、系统总内存、系统总容量、SD 卡总容量、系统可用内存、系统可用容量、SD 卡可用容量等。

常见的要素示例如下：

IMEI：International Mobile Equipment Identity，存储与手机里的国际移动设备标识串号。

IDFA：Identifier For Advertising，iOS 独有的广告标识符。单要素应用场景有： 比如你在淘宝里搜索了某个商品之后，你在用浏览器去浏览网页的时候，那个网页的广告就会给你展示相应的那个商品的广告。

UDID：Unique Device Identifier，唯一设备标识码。

MEID 号： 移动设备识别码(Mobile Equipment Identifier)是

CDMA 手机的身份识别码，也是每台 CDMA 手机或通讯平板唯一的识别码。通过这个识别码，网络端可以对该手机进行跟踪和监管。但只适用于 CDMA 制式的手机。

## 7.8 设备指纹生成方式（技术实现方式）

### 7.8.1 主动式

主动采集设备 N 多信息，比如 UA、MAC 地址、设备 IMEI 号、广告追踪 ID 等与客户端上生成唯一的 device_id。局限性有：不同生态的平台对用户隐私数据开放权限不同，很难统一生成唯一识别码，且无法实现 Web 和 App 跨域统一。 主动式设备指纹另一个局限性，由于强依赖客户端代码，这种方式生成的指纹在 反欺诈的场景中对抗性较弱。

### 7.8.2 被动式

被动式设备指纹技术在终端设备与服务器通信的过程中，从数据报文的 OSI 七层协议中，提取出该终端设备的 OS、协议栈和网络状态相关的特征集，并结合机器学习算法以标识和跟踪具体的终端设备。与主动式设备指纹技术相比，被动式设备指纹并不必须在设备终端上嵌入用于收集设备特征信息的 JS 代码或 SDK，其所需要的设备特征都是从终端设备发送过 来的数据报文中提取，这也是其所谓“被动式”的原因。好适用范围更广，一些无法植入 SDK 和 JS 的场景也可以使用。同时跨 Web/App,以及同步浏览器同 一兼容性识别，

主动式设备指纹技术，因为相对来说更为简单直接，所以业界大部分设备指纹技术厂商提供的都是该类设备指纹服务。

被动式设备指纹技术，由于其需要使用机器学习技术构建设备指纹分类算法模型，具有较高的技术壁垒，因而还处于推广起步阶段。

### 7.8.3 混合式

即既有主动采集部分，又有服务端算法生成部分。通过植入 SDK 和 JS，埋点在固定的业务场景，被动触发时的主动去采集要素，并与服务端交互，通过算法混淆加密后，在服务端生成唯一的设备指纹识 ID，同时写入唯一 ID 存于 app 应用缓存或浏览器 cookie 中。一定时间内，用户再次使用对应业务埋点页面时，无需大量重新上传采集要素，只需比对要素变化比例，通过加权比对，计算得出置信度数值，并通过阈值判断是否重新生成设备指纹码。正常用户在使用时理论上是无感知且很少会主动篡改设备指纹唯一 ID。

混合式设备指纹技术克服了主动式设备指纹和被动式设备指纹技术各自的固有的缺点，在准确识别设备的同时扩大了设备指纹技术的适用范围。对于 Web 页面或 App 内部的应用场景，可以通过主动式设备指纹技术进行快速的设备识别；而对于不同的浏览器之间、Web 页面与 App 之间的设备识别与比对关联，则可以利用被动式设备指纹的技术优势来实现。

## 7.9 分享举例

一般来说黑产通过群控手机撸羊毛。单一通过设备指纹虽然不能完全防住庞大、产业化、专业度高的黑产从业者，但可以极大提高黑产和恶意欺诈、骗贷、中介恶意包装等作案成本。比如黑产为了防止被设备指纹规则拦截，采用养设备的方式，即群控的设备农场。

### 7.9.1 广告营销

广告营销场景常常需要结合不同人群的兴趣爱好推送不同的广告，达到精准投放的目的。很多时候需要定位到一个用户的设备，然后画一个基于兴趣的设备画像。对于这个场景的设备指纹，其实可以放弃一部分的“唯一性”，去迎合“稳定性”。 因为这个时候业务考虑更多的是人群总体覆盖度，而不用纠结在是不是每一个人每一台设备都定位精准了。

所以有时候我们会发现在手机的 app 里浏览一个商品，过段时间电脑上就推荐了，这不是什么黑科技，有可能广告厂商用的仅仅是你的外网 ip 当作设备指纹。如果实现精准推送投放的话，比如用户刷抖 y 短视频时，抖 y 的 DSB 会根据你的设备码生成用户标签画像，同时将你的信息实时推给各电商平台，电商平台根据用户在平台搜索过的意向关键词，在导流平台 Push 商品广告，从而实现实时精准营销，提高下单转化率。

### 7.9.2 设备异常环境识别

很多人误解，设备指纹只能做设备的唯一标识，也就是“设备 ID”的追踪。但其实设备指纹能做的远不止这些，甚至可以说设备 ID 的

功能只占其全部功能的三 成左右。当下国内最典型的是“账户”和”营销”这些场景，也是黑产获利最多的场景。

这些场景里，黑产往往可以通过伪造新设备或者伪造某些系统底层参数 (比如地理位置，imei 号等等)的方式来绕过业务的限制。上层设备指纹获取的所有参数都是伪造的，基于这些伪造的数据计算得到的设备 ID 就毫无意义了。就像一个美丽的空中楼阁，没有了深入地下的坚实基础。而夯实基础关键在于”系统环境异常的识别”。对于常见的黑产改机框架、改机软件、伪装软件等，设备指纹都一定要做到针对性的识别。只有确定当前的系统环境没有异常，设备 ID 才是可信、可用的。成熟的设备指纹产品，可以识别虚拟机、模拟器、以及代理侦测。

# 第八章 互联网金融反欺诈解析（黑产）

## 8.1 黑产定义

## 8.2 市场现状

## 8.3 黑产常见名词解释

## 8.4 黑产常见产业链解析

## 8.5 风控系统如何对抗黑产欺诈

## 8.1 黑产定义

黑灰产即黑色或灰色产业，就是那些利用非法或作弊的手段牟取利益的产业。传

统意义上的黑灰产，是指那些利用非法手段攻击网络空间、危害网络安全或财产安全并从中获利的产业，比如我们经常听到的勒索病毒、木马刷量、控制肉鸡刷量、电信诈骗等等。随着黑产的普遍化，技术门槛越来越低，有一些存在于灰色地带的行为，例如电商平台的现金券被普通用户大量“薅羊毛”，都属于黑灰产的范围。

## 8.2 欺诈黑产市场现状


备注：图片来源于网络，侵删

据不完全统计，目前的黑产市场已达到千万亿元的市场规模，几百万的黑产从业者，千亿元的经济损失，以及大量的个人信息泄露。

其中根据金融机构历年的数据统计，线上无抵押信用类信贷业务的欺诈命中比例最高。信用卡汽车金融消费分期场景消费对于风控的把控

流程将会高于无抵押信用类的无场景消费。

## 8.3 黑产常见名词解释

为更好的让大家理解，这里整理收集了下目前市面上常见的欺诈黑产“黑话”以及使用语境，仅供大家参考~

8.3.1 黑料

在黑产中，被反复清洗，有金融价值的用户信息。主要指银行卡账户、密码、身份证号码、及绑定手机号码四大类信息

8.3.2 内料

境内卡的四要素

8.3.3 外料

境外卡的四要素

8.3.4 下料

非法途径搜集四要素

8.3.5 洗料

洗料在这个行业有很多细分工种，主要指的是资金转账、套现、洗白。如洗拦截料，通过植入木马病毒拦截用户手机验证码完成套现

8.3.6 挂马

制作，出租木马病毒

8.3.7 刷货

通过复制银行卡的方式来实施盗刷的过程

8.3.8 收菠菜

黑产从业者得到的数据进行整理，除了丰富社工库之外，还利用这些数据对其他网站进行试探性登录，从而获得其他网站上的账户信息

8.3.9 拖库

黑产通过社工手段或技术手段盗取目标网站客户资料书数据

8.3.10 洗库

黑产将用户账户中的财产或虚拟财产通过各种黑产渠道进行变现

8.3.11 撞库

黑产将拿到的数据进行整理，利用这些数据对其网站试探性登录，从而获得其他网站账号信息

8.3.12 社工库

社工库是黑客将获取的各种数据库关联起来，对用户进行全方位画像

8.3.13 虚假号码

所有用于代替他人接收验证码的手机号码

8.3.14 接码平台

即羊毛党和卡商进行验证码短信交易的渠道，类似淘宝平台提供平台服务，赚取分成

8.3.15 打码平台

提供批量自动化识别各类验证码的专业服务平台，提供手机号码，获取注册，解封，换绑短信的验证码平台

8.3.16 安卓模拟器

具有一键新机的功能，每次启动所有的系统参数都会变化

8.3.17 伪基站

搜取一定半径范围内手机卡信息，通过伪装成运营商的基站，冒用他人手机吗发送诈骗信息

8.3.18 猫池

猫池厂家负责生产猫池设备，并将设备卖给厂商使用。猫池是一种插上手机卡就可以模拟手机进行收发短信，接打电话，上网等功能的设备，在那个厂行业也有广泛应用，猫池设备可以实现对多张手机卡的管理

8.3.19 改机工具

刷新设备指纹，解决单台设备注册上限的问题

8.3.20 卡商

卡商指通过各种渠道，如开皮包公司，与代理商打通关系等，从运营商或者代理商那里办理大量手机卡，通过加价专卖下游卡商赚取利润的资源持有者

8.3.21 养号

将批量注册的小号，不断发作品关注用户，修改头像，主要目的是为了降低账号被封的概率

8.3.22 白号

指接入接码平台直接用手机号码注册的账户，也称直登号

8.3.23 活粉

带有作品、个签、个人头像，模拟真实用户操作的一批账户

8.3.24 死粉

又称僵尸粉，这类账号，知识带有简单的个签和个人头像，账户活跃

度低

8.3.25 刷粉

短时间内提高账号的粉丝数量

8.3.26 压门

犯罪分子冒充身份，对受害人进行行骗，一旦有人上当，作为压中了

8.3.27 菜商

菜商指的像卖菜一样出售个人信息的人

8.3.28 马

或者说病人，骗子的目标

讲完上面的黑话，举个例子：

对话一

A：兄弟，最近手头有料没?

B：刚好搞了一些，都是内料、外料都有，正准备找人刷货。

A：刷货多老土啊，还得买设备，而且现在都是芯片卡，也不好刷。我刚好认识一个挂马的，到时给你洗拦截料，方便快捷还安全。

B：技术真是日新月异啊，你不说我还真不知道。

对话二：

A：有没熟悉的卡商，找他买两千张卡。

B：这么多卡忙得过来吗?

A：你怎么那么笨阿，不是有猫池么。

B：对对对，要是做不过来还可以找打码的帮忙。

A：现在前期资金不够，我们设备有限，你看看找个认识的，整个改机工具，我们也好批量注册。

对话三：

A：上次买的那批卡注册的白号怎么样了？

B：那批现在在养号，咱们之前的号可以出货了。

A：那些活粉好好养着，那些死粉有人需要刷粉的可以卖一卖。

## 8.4 黑产常见产业链解析

8.4.1 特点

随着时间推移，技术的发展，目前的黑产组织有规模生产、技术专业、团伙作案三大特点。

8.4.1.1 规模生产：批量制作，变换模式，复杂攻击。

8.4.1.2 专业技术：技术迭代，运用先进的技术改进攻击方式。

8.4.1.3 团伙作案：团伙协同作案，分工明确，高效运作。

8.4.2 黑产产业链

分为上游、中游和下游。各个环节分工合作，紧密相连。

上游是基础性环节，分为开发研制和资料贩卖。主要是为了提供黑产作恶的基本工具。如打码平台，刷机工具，代理 IP，或者一些盗取的账号密码库。

中游是诈骗实施环节，如点心诈骗、短信群发、在线推广等。

下游则是洗钱销赃环节，实施现金取现、洗钱等。

以下我们根据不同场景为大家介绍~

8.4.3 黑产常见产业链（羊毛党）

8.4.3.1 上游（手机号码贩卖+物料收集）

8.4.3.2 中游（验证服务+网赚平台）

8.4.3.3 下游（实施欺诈+活动套利）

双十一临近，各大电商平台迎来了最强大的敌人羊毛党。无论是优惠、促销、打折、秒杀活动，或是补贴大战，发放红包等，都是羊毛党大显身手的地方。羊毛党特指那些在营销活动中凭技术或人工手段，钻漏洞获取非法利润的欺诈团伙。目前，随时科技的进步，羊毛党逐渐从分散的个体发展为团伙集体，已形成有组织、有规模的职业羊毛党。以某电商平台举例，平台-邀请账号-被邀请账号和真实顾客。黑产通过批量注册获取大量账号，参与邀请活动（可能是砍价、拼团等），将低价购买的优惠商品发送到指定地址归集，再通过自己的分销平台加价倒卖给真实顾客获利。黑产的收益为倒买倒卖的差价和平台补贴的优惠金。同时平台短期内可能会遇到库存被占用、普通用户无法购得优惠商品引起客诉，长期则可能造成用户流失，平台品牌和信誉度受到影响。

8.4.4 黑产常见产业链（互联网金融）

8.4.4.1 上游（身份贩卖+物料收集）

8.4.4.2 中游（身份包装+情报贩卖）

8.4.4.3 下游（黑产欺诈+欺诈实施）

黑产是互联网金融常见的欺诈风险，一般涉及申请人个人资料信息的四要素，即：

姓名+身份证号码+银行卡号+手机号码。常见获取渠道是批量收购，如偏远山区低价收购，或者深圳三和的无业游民批量收购。其身份信息都是真实有效的，并且其成本较低。后续进行身份包装后实施诈骗，也就是骗贷。

## 8.5 风控系统如何对抗黑产欺诈

目前，风控系统的整体框架已经基本成熟了，通常来说，一个完整的风控系统框架应当包括前端准入、规则引擎和验证流程。同时，一个完整的风控流程还需要人工进行数据分析、处理用户投诉、监控舆情等。或者说风控系统从业务数据中挖掘出黑产行为的数据分析系统。

8.5.1 采集数据

俗话说巧妇难为无米之炊，准备快速的识别黑产的基础就是要有足够的各类书籍，包括用户身份信息、行为记录、设备类型、鼠标或者屏幕点击轨迹等。常见的前端应用中，一般采集各类前端数据，如手机型号、硬件类型等、设备指纹。

8.5.2 决策引擎

如何识别黑产，需要我们的规则引擎而定。

举个例子，想要从登录行为中识别出黑产，仅仅知道设备指纹是不够的，我们还需要知道，同一个设备终端在最近一段时间内登录多个账户。这就是我们制定的规则引擎，我们对规则定义，比如同一个设备终端在 1 天之内登录登录了三个账户十异常登录，应当拦截。

我们知道，实时性越高、对黑产拦截得越及时，黑产所能够获得的收益也就越少。那是不是我们都采用同步模式就好了呢？当然不是。相比于同步模式，异步和离线模式在业务接受度和数据分析能力上都更优。

一般的工作模式

以登录场景为例：

在同步模式下，用户输入完用户名密码之后，需要先经过规则引擎的判定，只有正常用户才能够正常登录，黑产则直接被拦截，不允许登录。在异步模式下，用户一开始是可以正常登录的，登录后才交由规则引擎判定，如果最终确定是黑产，则会被封号或者踢出登录状态。离线模式的效果和异步模式一致，不过异步模式通常会在几秒到几分钟的时间内完成判定和处罚，离线模式则需要几小时甚至一天的时间才能够完成判定。

8.5.3 规则管理

因为规则管理有较高的复杂性和独特性。换一句话说就是，想要新建一条规则并执行是一件很容易的事情，但如何高效管理成百上千的规则，让风控人员和业务人员能够清晰地看到每个规则的效果、准确率

和实际意义，是一个很有挑战性的工作。

而高效的规则执行功能所能带来的性能提升，其实并不会特别明显。因为规则引擎的复杂度其实在于特征提取。特征提取完成之后，规则管理基本就是简单的 IF 匹配了。

但是，各个公司的规则形式，以及各个业务对规则的理解都不尽相同，因此，你在使用这些开源风控系统的时候，总会有部分需求无法实现。所以，我才说“规则管理需要较高的灵活性才能够适用于各个业务”。而矛盾的是，灵活性过高又会大大提高规则管理的复杂性，因此，我们必须慎重把握规则管理的灵活性。

### 8.5.4 如何拦截黑产？

事实上，当我们使用规则引擎识别出一个用户行为可能是黑产的时候，不能够直接进行拦截。因为规则引擎的判定结果永远存在“误伤”。有时候为了尽可能不漏过黑产，“误伤”的比例会很高。

比如说，当用户因为忘记密码多次登录网站失败的时候，网站就会怀疑这是黑产在进行操作。这个时候，我们如果直接拦截，就会收到大量的用户投诉。

为了解决这个问题，风控系统中加入了验证流程。采取适当的验证流程，我们可以降低拦截机制对用户体验的影响。所以，在上面的例子中，网站会使用滑块验证码来验证你是否是黑产。

基于业务场景的不同，验证的方式还有很多，比如，核验身份的短信认证、人脸识别，区分人机的图片验证、滑块验证等。很多应用都会

对存疑的用户和行为施加各种验证流程，来保障用户身份的真实可靠。所以，为了让风控系统成功落地，验证流程是我们不能忽视的一个环节。

# 第九章 黑产反欺诈之知识图谱解析

## 9.1 什么是知识图谱

## 9.2 反欺诈中的知识图谱

## 9.3 黑产反欺诈常见的知识图谱

## 9.1 什么是知识图谱

知识图谱就是把所有不同种类的信息（Heterogeneous Information)

连接在一起而得到的一个关系网络。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。

## 9.2 反欺诈中的知识图谱

反欺诈是风控中非常重要的一道环节。很多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，这一点在前面提到过。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。越来越多的金融机构及企业在探索构建金融领域的知识图谱研究，将海量非结构化信息自动化利用起来，为金融领域应用决策提供更精准可靠的依据。

## 9.3 黑产反欺诈常见的知识图谱

### 9.3.1 手机号码维度

电商的用户行为信息主要来源于订单、访问、支付等业务数据。如：新用户注册、营销推广等业务过程中，但是由于电商平台上业务数据信息严重不足不完成，很难基于行为进行风险分析。为了消除“信息孤岛“， 需要引入其它系统的风险数据，当用户访问系统时，参考用户在其它系统的风险数据，对其进行综合风险评估。

### 9.3.2IP 维度

IP 维度可以通过集合、设备等信息，可以有效识别用户的风险。用户访问系统，所有的网络请求都会带有信息，因此天然的成为访问者的身份标识。虽然地址极容易通过技术手段进行篡改，但是由于移动用户的特殊性，识别成为用户身份反欺诈的主要依据。

### 9.3.3 地理信息维度

地理位置信息是指通过定位或者基站定位的定位技术来获取手机或终端用户的位置信息（经纬度坐标），在电子地图上标出被定位对象

的位置。通过结合设备等信息，可以有效识别用户的风险。

# 第十章 案例分享

## 10.1 线上解决方案（案例）

## 10.2 反欺诈案例解析（以零售业务为例）

## 10.1 线上解决方案（案例）

信贷业务从线下到线上的转换，欺诈风险成为互联网金融线上信贷业务的最大挑战。由于场景、客群、数据、信用评估不同，历史中业界常用的人工审查、信用黑名单等传统反欺诈手段面临挑战。传统反欺诈手段存在人工效率低、无法自动发现异常等弊端。今天针对于一些反欺诈常见方法与大家分享。

10.1.1 身份信息

这个步骤主要是确认用户是否本人，即身份核验。身份证 OCR、活体识别（公安后台照片比对）、声纹识别等。即风控三原则中第一个问题如何证明“我”是“我”？

10.1.1.1 四要素认证

10.1.1.2 学历、信用情况

10.1.1.3 运营商通讯

10.1.2 信贷表现数据

10.1.2.1 多头负债

10.1.2.2 多头申请

10.1.2.3 信贷逾期名单

10.1.3 黑灰名单

黑灰名单作为反欺诈的第一道过滤，一种逻辑简单、成本较低的反欺诈手段，在很大程度上避免了重复欺诈行为的发生。其数据来源一般分为内部和外部，即自有平台内部积累数据和外部合作机构获。但是黑灰名单也存在覆盖群体较小、准确率较低、需要时间积累等问题。

10.1.3.1 欺诈客户信息

10.1.3.2 长期拖欠信息

10.1.3.3 中介信息

10.1.4 司法失信信息

10.1.4.1 企业失信信息

10.1.4.2 个人失信名单

10.1.4.3 公安通缉名单

10.1.5 社交数据

10.1.5.1 虚假号码

10.1.5.2 通讯小号库

10.1.5.3 欺诈骚扰库

10.1.6 设备信息

反欺诈规则中是不允许同一台手机/同一个 IP 频繁执行注册或不断切换账号尝试登陆。但是黑产最常使用 PC 端的手机操作系统模拟器，或在真实手机上安装改机工具，随意设置各种终端设备信息，绕过风控规则对设备的限制。

10.1.6.1 设备指纹

10.1.6.2 设备安装应用

10.1.6.3 设备网络环境

10.1.7 关联信息

关系信息也称为关系人图谱的应用是现在反欺诈手段最重要的应用之一。黑产中介通常有卡池批量养卡、养号等操作，批量申请某平台贷款时，其联系人信息（姓名、手机号码等），很容易在生成关系图谱中被发现，从而进行有效拦截。

10.1.7.1 手机号码

10.1.7.2 座机号码

10.1.7.3 单位名称/地址

## 10.2 反欺诈案例解析（以零售业务为例）

黑产遍布于互联网的各行各业，可谓是防不胜防。但是为什么说传统电商更容易受到黑产攻击？这里就要提到反欺诈风险，在传统电商的业务流程环境里面，客户购买行为是真实存在的，有实实在在的场景。但是到了线上就不一样了，我们甚至不能确认这笔交易行为是不是真人在操作。传统零售商在转换成线上业务时，风控措施都是比较薄弱的。一般只有在一定阶段后才会介入风控手段，设备指纹、反欺诈规则、黑产规则等等。但是这些基本都是事后补救措施了。

10.2.1 反欺诈常见风险

交易风险：银行卡盗刷、身份冒用、交易伪造、洗钱套现账户风险：账号盗用、暴力破解、脱库撞库、垃圾注册应用风险：高危漏洞、病毒木马、盗版违规、二次打包。

### 10.2.2 黑产常见产业链（电商平台）

黑产产业链分为上游、中游和下游。各个环节分工合作，紧密相连。上游：一般是基础性技术环节，主要是为了提供黑产作恶的基本工具。如打码平台，刷机工具，或者一些盗取的账号密码库。中游：主要是提供一个交流平台，供账号提供商和交易交流，并不断分享薅羊毛攻略。下游：欺诈行为实施阶段，黑产直接进行欺诈、刷单，并实现变现的恶意行为。

### 10.2.3 羊毛党玩儿法解析（电商平台）

双十一临近，各大电商平台迎来了最强大的敌人羊毛党。无论是优惠、促销、打折、秒杀活动，或是补贴大战，发放红包等，都是羊毛党大显身手的地方。羊毛党特指那些在营销活动中凭技术或人工手段，钻漏洞获取非法利润的欺诈团伙。目前，随时科技的进步，羊毛党逐渐从分散的个体发展为团伙集体，已形成有组织、有规模的职业羊毛党。羊毛党玩儿法很多，我们仅以注册环节举例。主要涉及平台-邀请账号-被邀请账号和真实顾客。黑产通过批量注册获取大量账号，参与邀请活动（可能是砍价、拼团等），将低价购买的优惠商品发送到指定地址归集，再通过自己的分销平台加价倒卖给真实顾客获利。黑产

的收益为倒买倒卖的差价和平台补贴的优惠金。同时平台短期内可能会遇到库存被占用、普通用户无法购得优惠商品引起客诉，长期则可能造成用户流失，平台品牌和信誉度受到影响。

# 第十一章 工作分享

## 11.1 战略高度谈反欺诈

## 11.2 反欺诈工作流程

## 11.3 反欺诈岗位从业建议

### 11.1 战略高度谈反欺诈

我们综合的看反欺诈这个事情，当平台出现了欺诈风险、黑灰产并不是一件坏事儿。一方面证明了其平台的知名度实力，另一方面也是为了反欺诈工作积累。

还是以零售电商为例，平台出现了黑产薅羊毛，但是并不是白薅，需要花钱薅羊毛。试想下这是个什么概念？不花钱薅羊毛和花钱薅羊毛。也就是说黑产如果想在平台薅羊毛，必须要先花钱，这么想想是不是心理上就不是那么深恶痛绝了？当然这是玩笑话。

黑产有时候无法直接从平台上薅羊毛需要先养号，那么这期间首先是对于平台是产生收益，其次是增加其风险特征。我们称之为有价值的黑产羊毛党。

以亚马逊为例，开始时候不区分欺诈风险。先把所有的大数据都圈进来，一点一点养。这样我们就知道好人长什么样，坏人长什么样。坏

人的特征指标是什么，人物画像实怎样的。这就是我们常说的在风险反欺诈体系之中，要筹划建设风险敞口。当然这是需要数据及 IT 支撑才可做到的。

## 11.2 反欺诈工作流程

11.2.1 风险识别

这个环节主要是通过多渠道收集风险点

11.2.1.1 外部分反馈，如客服、信审、催收、事业部等

11.2.1.2 数据反馈，如贷后逾期数据等

11.2.1.3 其他渠道，如投诉，市场动向等

11.2.2 立案调查

这个环节主要是是反欺诈案件调查，是整个环节最重要的环节

11.2.2.1 信息收集

11.2.2.2 涉案信息链补全

11.2.2.3 案件分析调查

11.2.2.4 案件定性

11.2.3 案件处理

11.2.3.1 最大化减少损失

11.2.3.2 最小化减少影响

11.2.3.3 处理措施有效

11.2.4 案件反馈

11.2.4.1 客观评价

11.2.4.2 合理建议

11.2.5 评估优化

11.2.5.1 反欺诈案件库

11.2.5.2 定期风险复盘

11.2.5.3 风险相关政策、标准、流程优化

## 11.3 反欺诈岗位从业建议

首先咱们先看下知名招聘网站的截图，当然啊，工资水平在行业内还是比较可观的。昨天我们提及的反欺诈风险已成为风控工作中面临的最大挑战.甚至说 ，反欺诈风险已成为互联网金融线上信贷工厂模式最大的挑战。目前大环境影响，很多风控领域的同学都在考虑转岗，特此今天根据个人经验分享下作为一名反欺诈专家需要具备哪些技能？仅代表个人观点，欢迎大家下方留言区讨论，谢谢。

我最开始在银行信用卡中心时，曾轮岗到反欺诈岗，信用卡的欺诈风险主要集中在盗刷、异常交易，其特点也是比较显著的，如异地大额刷卡，晚上时段密集刷卡，异常商户刷卡等等。当时的反欺诈岗是7*24 值班制的，根据系统检测的异常交易发现欺诈风险，第一时间与持卡人联系并进行锁卡操作，之后联系分行及信用卡推广员进行实

地调查走访。

现在看来，当时的反欺诈手段更依赖于人工审查 ，对于建模策略方面都是比较 薄弱的。近些年随着科学技术发展，反欺诈风险特点逐渐呈现四化现象 ，即人群团体化 、地区集中化、方式多样化 、工具智能化 。所以相应的对于反欺诈从业者要求更高 。

以下个人总结下关于反欺诈岗位的从业要求，仅供大家工作参考

工作内容

1、熟悉信贷业务流程

2、制定反欺诈流程策略

任职要求

1、懂技术即懂建模评分卡，掌握 SAS、R 语言等方法

2、懂风控即懂风控策略。

其他能力

1、熟悉欺诈手段

所谓知己知彼方能百战不殆，战胜对手的第一步就是深入了解对方。作为反欺诈人员，不仅要对常见的黑灰产手法有充足的经验，而大部分反欺诈行业的人员都从欺诈调查岗位做起的原因，深入一线了解业务。

2、数据敏感度

上文提及的目前反欺诈从业者都是需要具备 SAS、R 语言等方法，起码能够自己能够 SQL 去数据库调取数据，并且能够对于异常数据有一定的敏感度。

3、缜密的逻辑思维

4、跨部门强沟通能力