互联网金融反欺诈解析

目录

备注：部分概念内容来源于网络

一、全面防范欺诈风险

目前信贷业务的模式都是纯线上无抵押，相应的面临欺诈风险愈发严峻。

随着现在各大机构决策引擎、规则模型日趋完善，历史上常见的欺诈手段，比如说个人申请虚假资料、虚假流水等都可以通过三要素或四要素进行甄别。

更多的现在黑中介手段也是升级，比如养卡 6 个月，然后去申请一笔大额贷款，投入成本大概就是 1-2k。随着社交媒体兴起，一些黑中介也是更换了方式，比如直播或者 QQ 群组等一些招收学徒，学习分享各大平台的口子漏斗。虽然这些黑中介不会直接参与借款申请，但是会收取教学费用之后，帮着一些黑户或者说资质不足的人员进行包装，申请成功后再收取一定手续费用。

如何做到全面防范欺诈风险呢，个人认为主要从以下方面

1、搭建全流程反欺诈管理制度

2、数据监控和欺诈分析相结合

3、欺诈流程和欺诈模型相结合

4、大数据与风控系统现结合

二、什么样的数据可以应用到反欺诈

基于大数据的反欺诈的难点在于如何把不同来源的数据整合在一起，并搭建反欺诈体系。从而有效地识别出欺诈案件。随着黑产技术的发展创新，给反欺诈工作带来新的挑战。互联网金融行业与银行相比，

获取的数据资源来源多样、结构复杂、质量不齐。这些数据资源的获取和整合需要大量时间物力财力成本。

1、按照数据来源区分

1）用户申请提供数据

2）第三方获取数据

3）自有业务数据沉淀

2、按照数据类型区分

1）征信数据

2）多头数据

3）消费/资产数据

4）历史还款数据

3、按照数据使用场景

1）面对客户反欺诈

2）面对员工反欺诈

这里说的内部的销售、管理、客户代表等，是否有意识的通过欺诈的方式，降低公司的收入或给予外部超过合理范围的待遇。

4、注意事项

合理使用外部数据

目前业务场景中，很大程度上，我们内部的数据沉淀最开始都是来源

于外部采集数据。我们都知道，外部采集的数据的是不可能百分百准确的，一定程度上受制于技术手段，安全要求，政策监管等，外部数据不可能反馈给我们准确数据。也就是真实可靠性都是打问号的，那么在此基础上我们的数据分析，反欺诈策略都是相对准确的。

在此，个人工作经验就是，日常使用第三方数据时候不建议采用太多家，因为这些外部数据可能会存在一定不一致或者冲突，因其准确度无法验证，容易影响最终判断。

三、反欺诈模型和信用模型区别

在说反欺诈模型和信用模型之前，我们先说下反欺诈风险和信用风险的区别。

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，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。

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。

那么在反欺诈模型和信用模型比较之前之前，我们根据四个维度对比

看下，

即：目标变量，模型特征，实时性和技术实施

1、目标变量

信用模型：逾期客户，即有违约风险潜在风险的客户，考量的是还款能力。

反欺诈模型：高危及欺诈客户，考量的是还款意愿。

2、模型特征

信用模型：人文特征，信用历史，消费特征。

反欺诈模型：反欺诈风险点，运营商数据，社交关系。

3、实时性

信用模型：离线

反欺诈模型：离线特征+实时特征，申请+交易时实时预测

4、技术实施

信用模型：逻辑回归，GBDT

反欺诈模型：GBDT，神经网络

这里补充一点，反欺诈模型的一个工作难点就是欺诈特征抓取，这里我们常用的机器学习进行特征挖掘。如果欺诈样本较少，那么就要衡量视同无监督技术或者半监督技术搭建。

另外欺诈人群特征变化快，欺诈特征迭代周期短。建议大家在建设反

欺诈模型时候可以进行备选特征监控，一旦发生风险，可及时到达反欺诈模迭代目的。

四、反欺诈之手机设备指纹实施

自 PC 互联网时代起，设备识别就是互联网用户追踪的重要手段。传统的设备识别技术主要包括：IP 地址、cookie 以及移动互联网特有的设备 ID。设备指纹（设备 ID)：设备唯一识别码，用于识别贷款时使用的设备信息，以及检测是否就有代办中介或黑产风险。

被动式指纹，因目前涉及和第三方公司合作，对于数据隐私要求比较高的公式通常不会建议。在合作过程中，第三方合作公司在 APP 某个页面植入木马，客户申请时候可以实时获取到期设备信息，但是同时其客户数据也会被第三方公司抓取。

而主动式设备指纹，通常就是公司内部开发加工使用，在具体每个流程点进行埋点，注册、OCR、人脸识别、个人资料填写、绑卡、提现等等。实施检测，一旦发生客户异常行为，及时接入处理。

以下为收集设备指纹在反欺诈工作中常见形式

1、篡改设备

检测设备原始信息是否被篡改

2、作弊环境

设备中是否安装作弊软件

3、真机识别

利用硬件的核心参数检测设备的真实性

4、设备关系

同设备多账号登录

同设备多电话使用

5、高危 APP

密集使用高危 APP

举个例子

通过监控，发现短时间批量注册，即垃圾注册行为，或者是机器批量操作。可以增加问卷环节提问，或者人工接入。另外加强内部防范，防止内鬼欺诈，明确风控人员权限管理。

五、如何构建全流程反欺诈风控系统

1、数据接入、决策引擎、管理系统三者相结合

1）数据接入

我们之前说的充分的把外部数据，内部数据，业务数据进行清洗整理

分类后参考性使用。

2）决策引擎

最为常见的鞠策引擎有准入决策，认证决策，再说申请环节已广泛应用的三要素/四要素核验。

3）管理系统

这里说的是 IT 系统，包括，查询系统，分析系统，预警系统，配置系统等等。

2、数据分析和反欺诈模型相结合

1）规则判断

常见的规则如身份核验类、多头申请类、第三方征信类等等。

主要分析规则应用前后的数据对比，规则判断的误报率高低，以及对欺诈侦测率的高低。

2）行为特征分析

之前提及的手机指纹识别，此外常用的客户近期借款/消费数据、个人账户登录操作信息等等。

3）设备登录信息分析

按照整个信贷流程区分，欺诈贯穿在每个环节。

注册环节的羊毛党、垃圾注册。

登录环节的暴力破解、撞库、信息盗取等。

申请环节的虚假设备信息、异常登录等。

提现环节的短时间多次操作，设备信息异地异常操作、黑中介批量操作等。

4）关联数据分析

主要指的是社交群体异常数据，利用关系图谱进行分析解读。

六、反欺诈工作落地实施方案

反欺诈方案落地实施主要有如下步骤，准备-实施-部署-监控

1、准备

这里说的准备不仅仅是反欺诈，而是整个信贷周期的准备工作。

1）渠道（流量）

2）风控（数据，模型，策略）

4）人力（团队，业务，风控，客服，催收）

5）IT（APP，信贷系统，决策引擎）

强调一点 IT 支持核心就是底层支撑系统和大数据搭建支撑。

6）资金（资金来源，资金成本，测算成本）

2、部署

1）渠道进件

客户分析

这里说的客户分析主要客户画像分析，对客户进行标签化管理，以便后续进行欺诈排查。

准入规则

渠道监控

虽然说目前都是线上渠道，但是具体细分也是有自有 APP，其他渠道引流等，做到各个渠道监控，一方面是防止黑产，另外一方面为后续客户质量评估提供依据。

2）反欺诈模型

按照欺诈类型分，常见的第一方欺诈和第三方欺诈。

第一方欺诈，主要使用的数据为客户自己提供。

第三方欺诈，主要使用第三方数据，如多头信息，黑名单等等。

这里需要补充下，不同客群黑白名单规则是不同。我们采用的第三方黑名单不排除被污染，其准确度，需要测试评估后使用

3）信审核查

主要是授信审批环节，主要是信用模型和授信规则。

4）贷后管理

贷后一般是两块一个是催收风险预警监控，一个是催收策略制定实施。

3、实施

1）前期准备

客群产品定位

产品设计（客群分析，数据采购维度）

2）风控部署

风控方案设计

风控流程制定（数据使用，反欺诈规则、反欺诈模型）

3）后期调优

风控方案调整

业务监控调整（流程调整与优化，规则与模型调优）

4）业务优化

反欺诈工作是一个不断循环优化过程，需要根据实际业务情况，数据指标，场景不断进行调整更迭。

4、跟踪监控

1）实时监控

进件渠道中的识别到风险客户需要进行渠道核查。

审批流程时遇到风险客户建议进行人工电话交叉核实。

同时一些高危地区、单位，需要根据数据实时监控。同时一些同行竞对或者黑中介也应注意。

2）离线监控

定期抽测已经放款案件以及拒绝案件，进行电话回访、数据核实。

定期对合作机构渠道进行调查，严控人员操作风险。

定期拉取贷后表现，针对于疑似或者欺诈客户，进行行为画像分析，降低审核环节降低误杀。

七、反欺诈方案调整解析

之前说过欺诈和反欺诈工作一直都是此消彼长的持久战，所以我们具体的风控反欺诈方案也是需要不断调整完善的。

实时监控

调整完善肯定不是拍脑袋的，在日常风控工作中就要实时进行监控

1、业务运营监控

这里主要指的是数据报表，来自于贷前、贷中、贷后的数据监控指标。

2、策略模型监控

业务上线后，不断的试探我们的反欺诈策略，需要实时监控自身的策略模型是否有漏洞，或者具体某一条策略被欺诈团伙技巧性避开绕过。专门有这么一群人，可能比我们的反欺诈人员都要熟悉各大机构的欺诈策略模型，根据不断试探寻找风控漏洞，并形成详细的教学文档视

频，通过社交平台（短时间/QQ 群组等）拜师学徒或者付费学习传授骗贷的行为。目前在行业内已经有形成相当成熟的产业链。

3、异常情况监控

这个是属于临时突发性时间，比如业务刚刚上线时间批量申请，或者是某个集中时段平台出现黑产攻击。

实施依据

在说具体实施的依据之前，有个指导方针要先说明下：风控过严就要松松，风控过松就要紧紧。毕竟都是业务导向，考虑到获客成本，产品赢利，公司战略等诸多方面。

1）数据指标

2）风险表现

3）监控发现的问题

4）策略性调整

5）目标客户偏移