互联网金融反欺诈入门解析

一、业务现状

二、常见欺诈形式

三、常见反欺诈手段

四、信用风险与欺诈风险比较

五、常见反欺诈策略

六、如何搭建全流程反欺诈体系

七、反欺诈工作流程

八、线上解决方案（案例）

九、反欺诈岗位从业建议

一、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。

二、常见欺诈形式

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。

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）

3、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

4、欺诈分类（作案人数）

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。

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。

5、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）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。

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。团伙成员的北京往往不同，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

3）内外勾结

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。

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。

以下仅针对于一些黑产常见手段解析

a 生物识别模拟

生物识别如指纹、人脸识别其目的就是为了验证是用户本人操作。而黑产想要通过验证，就必须想方设法模拟用户的生物特征。历史上像缺少细节的指纹模型、低分辨率的人脸视频等方法已经无法通过验证。目前黑产已经很少会费时费力去挑战这道反欺诈策略了。

b 数据获取

俗称“拖库”，指的是黑客通过破解服务提供商的服务器，获取大量敏感数据，如账号密码等，导致大量用户数据信息泄露。建议加强业务代码的安全性，及时为操作系统打补丁(修复安全漏洞)，

并且对用户敏感数据进行加密存储。

c 薅羊毛

通常在注册阶段，较为常见。指的是新平台或者新业务为了营销，经常会开展优惠或者返现等活动，黑产进行大量注册新用户领取活动奖励。

建议后续通过手机验证码实时监控其手机号码是否处于正常状态。

d 廉价实体卡

指的是黑产从卡商那里购买即将废弃但仍然可以接收短信的手机卡或者廉价的物联网卡，以这针对于短信验证环节。

建议强化登录验证，比如随机图片验证码和拼图验证。

e 养号

指的是黑产利用实体手机和手机卡，用猫池长期供养大量的手机卡并且定期产生通讯，让手机号码模拟正常使用状态，以此为了绕开了风控规则。

建议配合手机卡号黑灰名单库。

5）交易欺诈

与前面介绍的欺诈类型不同，交易欺诈往往发生在贷后，并且属于第三方欺诈，即所发生的交易非本人意愿的交易。交易欺诈通常在银行更为常见，信用卡或虚拟信用卡产品上。

在银行这个岗位比信审、催收苦逼的一点是，真的是 7*24 上班。因为很多时候都是深夜+境外+大额消费。

通过是不法分子利用各种渠道窃取卡信息或者账户信息后进行作案。

以下几点是交易欺诈常见类型

a 交易地点异常：例如境外消费

b 交易金额异常：例如大额消费

c 交易时间异常：例如深夜消费

d 交易商品异常：例如易变现商品

e 交易频次异常：例如沉默账户突然集中消费

三、常见反欺诈手段

目前针对于欺诈类型所针对于的反欺诈手段不同。以下仅针对于常见反欺诈手段分享~即名单库筛选（黑白名单）、生物识别、规则引擎、机器学习和专家策略。

一、名单库筛选（黑白名单）

名单库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，但是可以作为反欺诈的第一道过滤。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。

二、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。

1、人脸识别

2、声音识别

3、虹膜识别

三、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

四、机器学习

1、有监督学习

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、无监督学习

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。

五、专家策略

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。

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。

四、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。

五、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。

六、如何搭建全流程反欺诈体系

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

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。

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、 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。

那么如何建设反欺诈体系呢?

1、收集数据

这里说的数据指的是底层数据，包括内部数据、外部数据等。现在大环境监管国家对于数据安全隐私的监管越来越严格，外部数据获取越发的困难，所以更多的就要依靠公司内部的业务数据，即日常业务场景下数据的沉淀。

2、 制定规则

这里说的规则也就是规则引擎，这些模型规则是渗透在风控每个环节中。比如说贷前准入、OCR 认证等。当然说这些反欺诈规则并不是一成不变的，都是需要实时更新的。

3、 构建系统

或者说是这是实现手段，有了数据，有了规则，最后通过系统落地实现。这个系统起码要有四个模块，即配置系统、查询系统、分析系统

预警系统。具体系统建设，

七、反欺诈调查流程

1、风险识别

这个环节主要是通过多渠道收集风险点

1）外部分反馈，如客服、信审、催收、事业部等

2）数据反馈，如贷后逾期数据等

3）其他渠道，如投诉，市场动向等

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

1）信息收集

2）涉案信息链补全

3）案件分析调查

4）案件定性

3、案件处理

1）最大化减少损失

2）最小化减少影响

3）处理措施有效

4、案件反馈

1）客观评价

2）合理建议

5、评估优化

1）反欺诈案件库

2）定期风险复盘

3）风险相关政策、标准、流程优化

八、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。

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”？

1）四要素认证

2）学历、信用情况

3）运营商通讯

2、信贷表现数据

1）多头负债

2）多头申请

3）信贷逾期名单

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取。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。

1） 欺诈客户信息

2） 长期拖欠信息

3） 中介信息

4、司法失信信息

1）企业失信信息

2）个人失信名单

3）公安通缉名单

5、社交数据

1）虚假号码

2）通讯小号库

3）欺诈骚扰库

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。

1）设备指纹

2）设备安装应用

3）设备网络环境

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。

1、手机号码

2、座机号码

3、单位名称/地址

九、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