互联网反欺诈常见手段解析

目录

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

一、名单库

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。

二、规则引擎

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。

三、专家规则

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。

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。

四、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。

有监督机器学习的反欺诈：

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。

无监督机器学习的反欺诈：

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。

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。