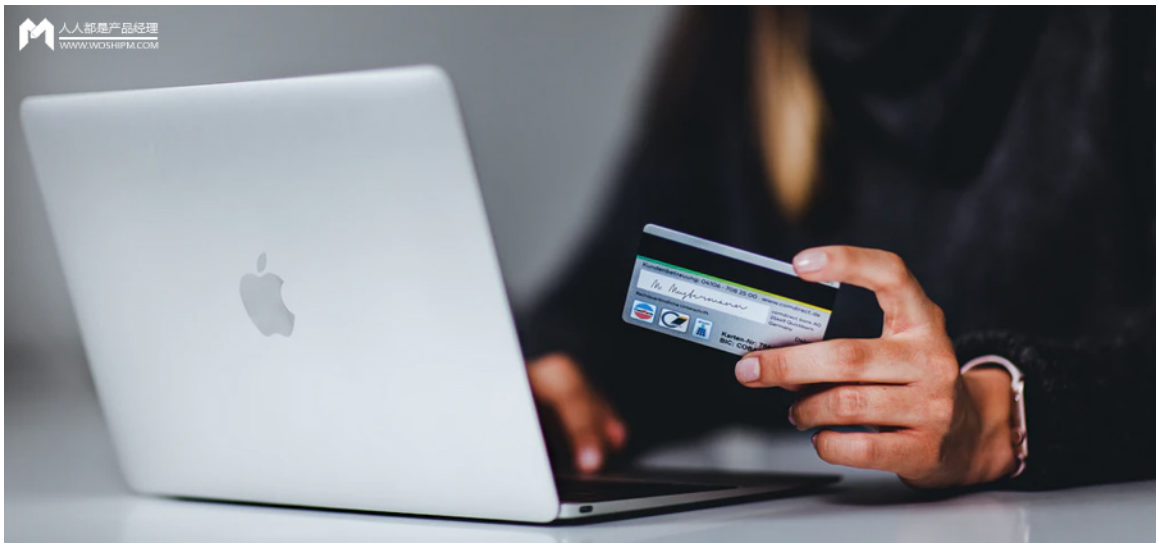
编辑导语：线上交易现在已经成为人们普遍使用的交易方式，这就要求第三方支付系统做好各方面的风险防控，而第三方支付风控系统的设计与其他金融机构风控系统设计有所不同。本篇文章里，作者从交易的各个流程阶段分析了第三方支付风控系统的有关设计，一起来看一下。



前言：由于涉及机密，在本文中，只分析大概方向。只要你往这个方向去思考，基本没错。

第三方支付风控系统不同于其他金融机构的风控业务系统，第三方支付风控系统除了要关注自身的业务风险之外还要时刻关心央妈的合规风险，以便更好地把握全面风险控制。

一般对于第三方支付风控系统而言，事前风控处理主要依托外部联防系统，主要依靠银联、清算协会等国家机构。

一、事前风控处理（进件行为）

事前风控处理

1）小微商户管理

根据商户进件查询商户个人/法人信息是否虚假，可联防银联风控系统查询是否有个人欺诈风险（虚假申请人员，经济犯罪人员，失信人员名单等）、个人合规风险（疑似赌客标签，营销套利标签，账户风险标签节点，II/III 类账户风险标签等）、黑名单等。

2）企业商户管理

根据商户进件查询商户信息，可联防银联风控系统查询是否禁止发展商户、收单机构报送的风险商户、银联高风险商户、疑似涉赌商户、高法失信企业、工商经营异常名录、工商严重违法失信企业、商户频繁变更信息节点等。

二、事中风控处理（交易行为）

事中风控主要体现在交易行为，为此我们可以建立一套交易规则匹配，当发生交易时，会通过规则引擎来过滤掉命中的交易记录。

1）实时刷卡交易/扫码规则

当日单笔、累积上限、频繁交易、多失败、黑名单异常、交易金额/时间异常（交易金额位数 88,66,99 等，时间常发生在凌晨或其它异常时间）等。

2：银行卡支付/互联网支付监控规则

当日多笔交易相同金额（规律尾数 00-99 或 68/69/89/98/998 或含 999）等），某个时间段内交易金额大于设定的金额，客户收款人年龄，黑名单，频繁交易等。

3）反洗钱规则

特殊金额尾数、交易 IP 与装机 IP 不一致、定位异常、新商户交易频率高、单笔整数、大额交易频繁等。

4）实时交易定位匹配规则

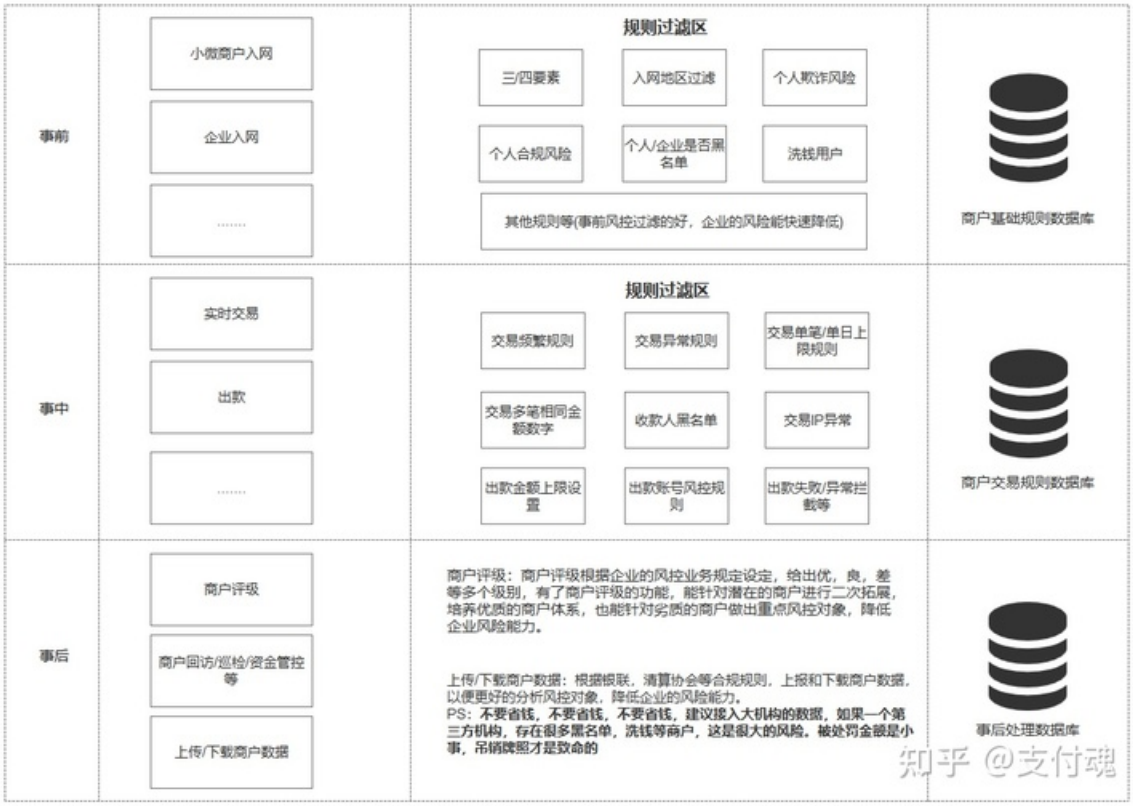
特定不允许交易地区、短时间内交易地址不一致、虚拟 IP 地址等

5）风险阻断/资金拦截

三、事后风控处理

接入联防银联风控系统，清算协会风控系统等，同步商户数据； 针对高异常的商户资金延迟结算； 商户回检/回访； 建立商户风险评分/等级，资金管控等。

PS：建议风控的数据分开储存，例如像联防机制的这种数据，A 用户入网，如果在本地黑名单没查到，那么再去查联防接口（银联水晶球/清算协会系统接口等等。）



风控系统草图

题图来自 Unsplash，基于 CC0 协议。