## 薅羊毛

不讲黑产，不讲平台刷单，不讲水军。这些跟薅羊毛有相似的地方。

薅羊毛是要按照商户的流程获取收益，黑产是按照黑产的流程获取收益。

按照规定的流程走，获取规则给出的收益。

黑产是无视商户的限制，获取非法违规收益。

# 第一部分：基础设施

## 猫池

猫池就是个通信硬件，实现了手机卡的通信协议。

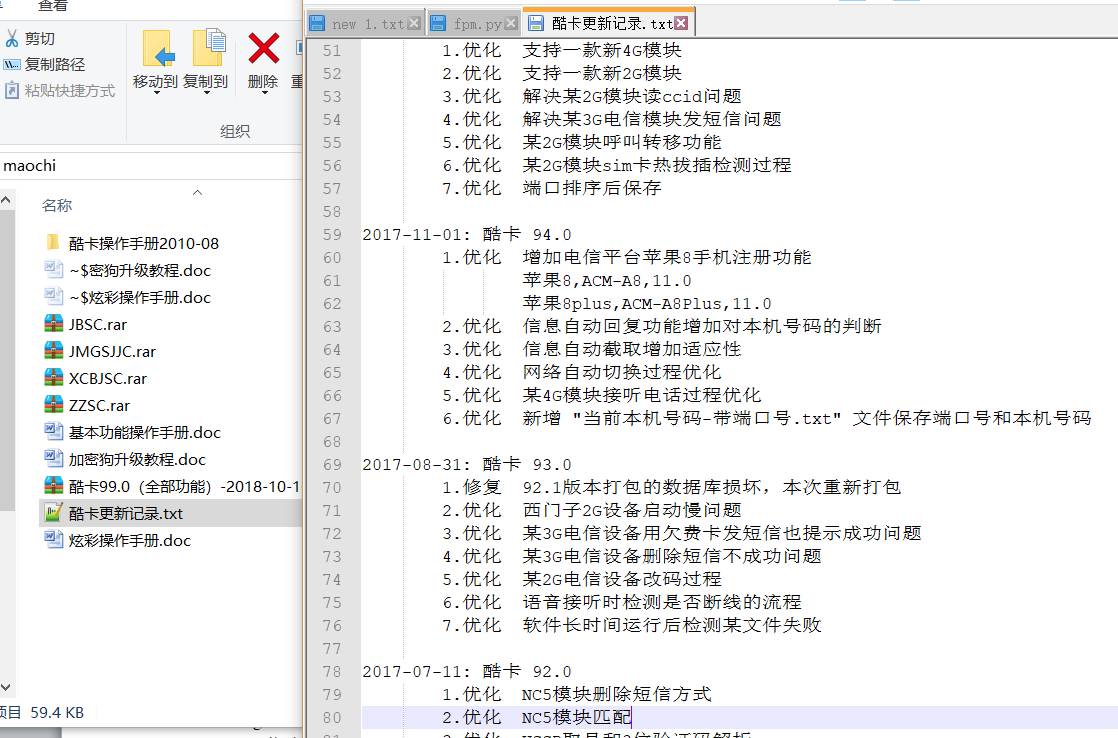


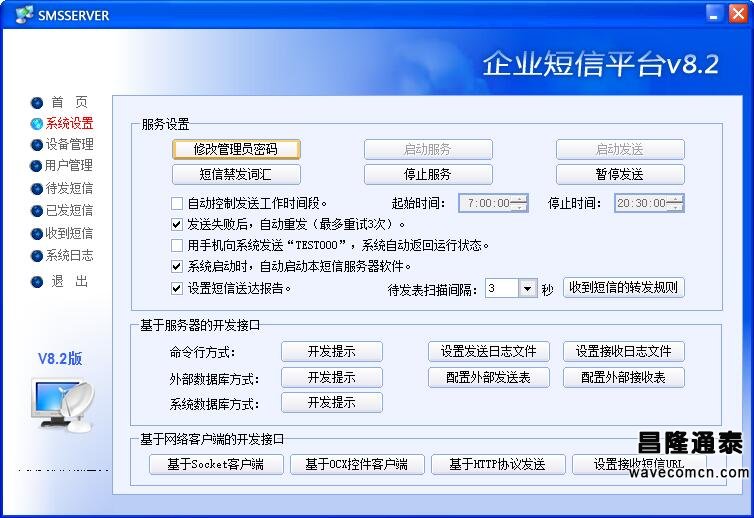


## 猫池操作软件

<http://www.smscp.com/>







软件实现了在电脑上操作猫池功能，软件实现了设备的调用协议。

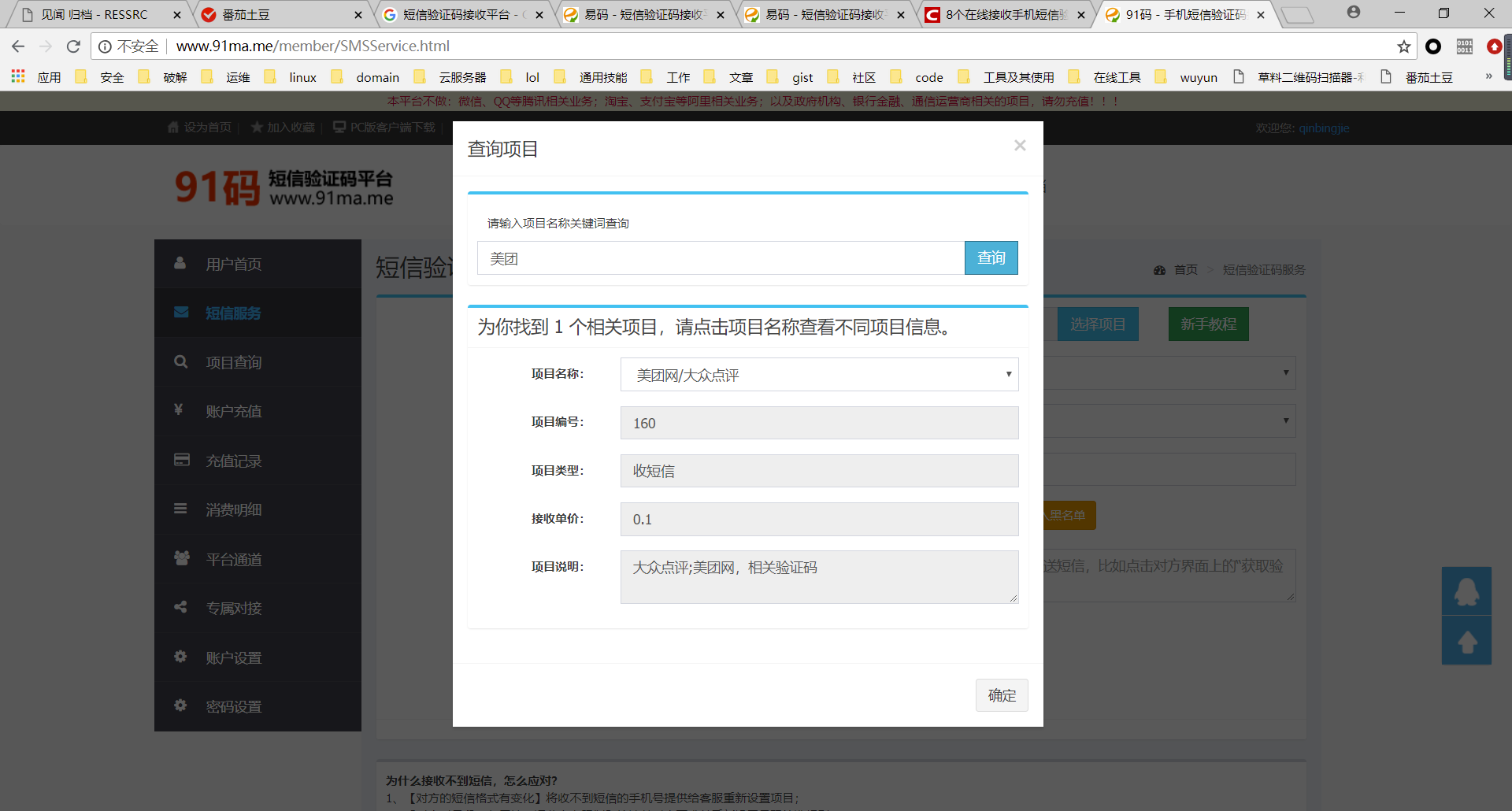
## 验证码平台

以网页端为例，来介绍一下。

使用流程：充值，选择短信模板，分配手机号，使用手机号，获取短信，扣钱。

下图中的项目就是模板。









此类平台，都可以批量获取手机号码，可以使用API自动化操作。

## 实名认证四要素

四要素是指：身份证照（正反面）、证主手持身份证照片、实名制手机SIM卡，以及相对应的银行卡号U盾信息。

四要素资料是有专门的团队 从 “三和”大神、网络边缘人群、偏僻乡村 等地组织当地人群制作购买的。其成本已经从原来的500～1500元降低到100元。

这些资料都可以一份多用，一分多卖，利润也很高。

# 第二部分：产业结构

## 基础设施部分

先从基础设施部分说起，基础设施部分有 **卡商，猫池，接码平台。**

卡商可以说是互联网江湖供应链条的最初供应链。他们手上有大批运营商资源可以超低价拿到手机卡。

猫池是卡商用来接验证码的设备，一般猫池在几千到几万元不等。一个猫池一般可以插16-128张卡不止。猫池的硬件商也是暴利行业。

接码平台其实原理也比较简单，就是一个对接猫池的协议，一个对接云端的数据库，和客户端的PC。一个手机号，能够给互联网上万个平台接码。这就是它的价值所在。

## 工作分工部分

羊毛党 就是羊毛党，有职业羊毛党，以薅羊毛为生的人。有兼职羊毛党，就是普通人。一般提羊毛党就是指职业羊毛党，群主/版主 一般叫做羊头。这些人也能做职业水军，羊头就叫水头了。羊头水头都要求有强大的信息渠道，有商户活动的第一手信息。以此为需求，就衍生出了很多的羊毛群，羊毛论坛。





软件作者 就是 写软件的人，这里主力是学易语言/按键精灵的脚本作者，只有少部分是程序员。

资料商，主要作用是提供账号资料等个人身份信息。各种资料都卖，可能一手可能二手。

收货商，就是收赃并销赃的商家，一般有强大的渠道，变现速度越快，越受欢迎。这里可以是正常商户，有多种进货渠道而已。

交易平台，为上诉交易活动提供平台，收商家提成。

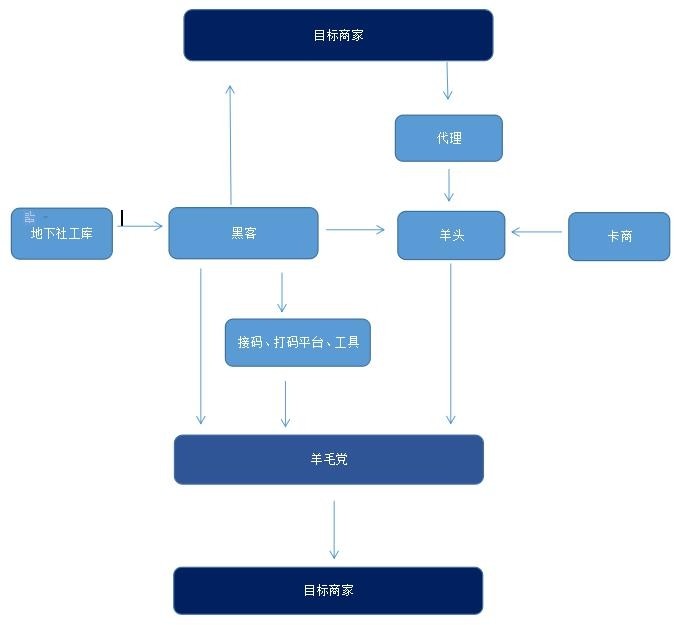
骗子，可能冒充上诉身份中的任意一种，要求先货后款或先款后货。或者以次充好，编篡数据等方式进行诈骗。

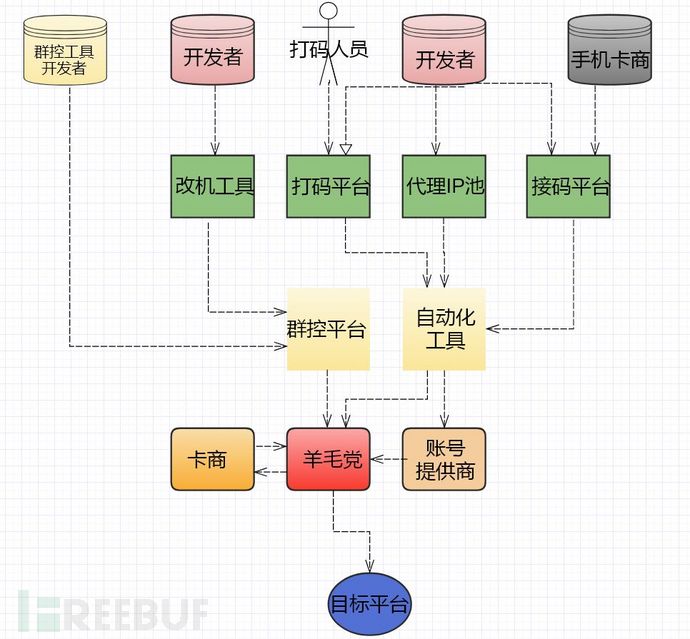
终端消费者：就是有正常需求的普通人，从淘宝，咸鱼，白菜群，拼多多等低价渠道购买赃物。

## 分工如下

羊毛党搜集信息，寻找平台规则漏洞；卡商提供账号，建立猫池养卡；脚本作者编写软件，销售软件挂靠平台提成；收货商收赃并销赃，每个环节，各司其职，默契配合，提供自己的最大价值，迅速集结成一条密不透风的产业链。核心就是这些，可以接入其他正常衍生行业如代理池，打码平台，二手物品交易，虚拟物品交易平台，批发商等。然后将物品卖给有需求的正常消费者。

## 结构图





# 第三部分：存在条件

第一条件呢，就是上边讲的基础设施部分，按理说手机号实名制制度落实之后，应该会解决很大一部分问题。

其他条件按相关性排序如下：

活动漏洞：活动规则不严谨，有漏洞。或者是意外事件，如拼多多的测试卷自动上线。

信息壁垒：编程人员，测试人员不知道这方面的知识，以为自己的逻辑或策略没问题。

监控及控制：没有相关的监控及控制程序与流程，没有报警条件提醒

公司风控数据垄断：各公司积累的风控数据都是自己的核心机密，当然是垄断处理。有的提供对外的查询服务，如蚂蚁信用。但是不会给你详细的判断资料。

# 第四部分：介绍与对抗

## 起源

现在以80、90后为代表的新兴都市族们对银行等金融机构及各类商家开展的一些优惠活动产生了浓厚兴趣，并专门出现了这样一批人，搜集各个银行等金融机构及各类商家的优惠信息，在网络和朋友圈子中广为传播，这种行为被称作**薅**（hāo）**羊毛**。

薅羊毛 羊毛党利用接码平台、打码平台、代理 IP 等黑灰产服务，整合成自动化注册软件，针对目标网站进行批量注册，囤积大量账号。之后利用所囤积的账号，参与到各种营销活动中，针对各网站的营销规则制定相应薅羊毛的方案，刷取网站给到真实用户的奖励，并将其变现，转化为真实获利。

电商类网站在“双十一”之类的各种特殊节日，会推出大量的游戏送抵用券，送红包、送流量、送优惠券等等活动。如某送流量活动，输入手机号，鼠标点击鼓达某个阈值送多少流量，攻击者可直接修改js或者写js自动模拟点击刷活动。再比如，商家为了冲销量，经常举办前几百名免单活动，攻击者通过自动化脚本秒杀商品，大量薅这羊毛。这直接导致商家销售产品存在大量恶意退货、退款，对于正常用户而言，认为自己被耍猴；对于商家投资成本带来的回报与预期有较大出入。

## 特点

分类：省钱与套利

根据薅羊毛目的划分可以分为两类。

一类是利用规则给自己省钱，追求性价比。特点是单人，自用，真实转化率，与厂商互利。

一类是以套利为目的，追求套利。特点是批量，产业化，危害厂商。

关键词，自动化

对目标物进行分级

第一等：现金类的，如红包，无门槛卷。

第二等：可变现商品。如手机，化妆品等硬通货。

第三等：可日用的消耗类东西，吃喝玩乐。

重点：渠道

风险：黑吃黑。利用信息不对称，进行坑蒙拐骗。

羊毛宗旨：蚊子腿再小也是肉。关键词：大批量。

## 发展及案例

从互联网之前，就有各种的灰色产业者，俗称捞偏门。伴随着互联网发展，其产业发展到互联网领域，日趋完善，日趋庞大。

### 刷卡爆卡---电话卡

刷卡，指的是将手机话费套现，然后通过运营商结算。一般出现的是，做自消费，移动金曲，移动彩铃，游戏 这些，把话费通过下载消耗掉， 换取现金。

刷卡 只属于消耗话费，通过低价买卡， 话费套现 赚取中间的利润。需要改码设备， 群发软件。

爆卡就是，把手机卡里的话费套现完毕之后。在还没停机的情况下，用最快的速度充到大额欠费。透支之后直接废掉了。

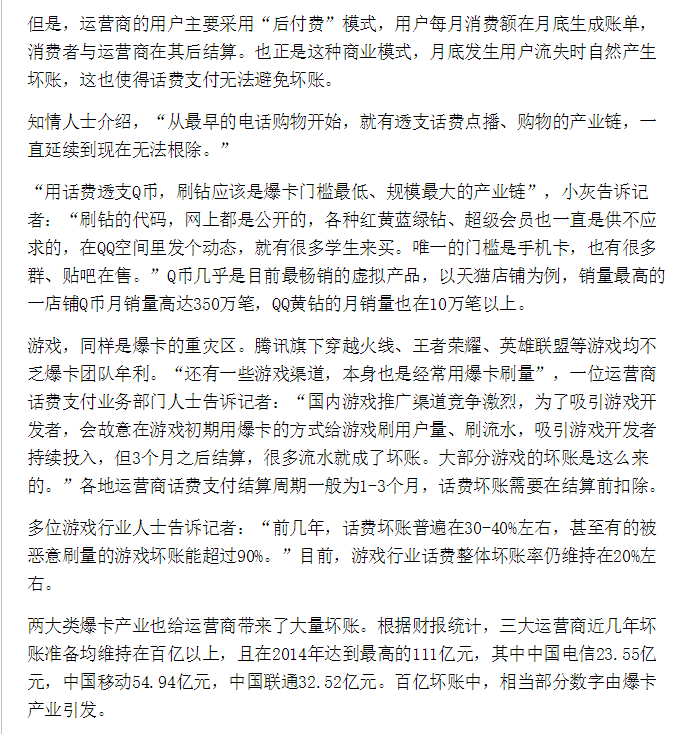
受害者为运营商。

### 游戏点卡短信操作：



当时就有简单产业结构了。

受害者是运营商，羊毛党是爆卡的人，商家为运营商接入的各种游戏，彩铃等商家，可以与羊毛党打配合，也可以自做广告坑害消费者。终端消费者是普通人。



类似的新闻报道如下





### 电话卡风控

对这方面的风控不熟悉，网上也没有搜到。就不讲了。

### 套现及刷积分---信用卡

刷卡消费有积分，还可以参与银行的活动，获得相应的礼品等等。

信用卡积分，可以兑换吃的（如必胜客）、喝的（如星巴克）、玩的（如电影票）、住的（如星级酒店）、飞机（里程数）等，还有各种折扣，例如汽车加油、免费洗车、洗牙、体检。

信用卡账单日与还款日一般相隔为20天，等于最长无偿拥有一笔钱50天左右；



为了薅这样的羊毛，有些持卡人就会进行套现，制作“消费”记录来达到银行的要求，从而获得积分或者礼品。

现在就有对信用卡活动整理的公众号。





还有一些人刷POS机套现是为了形成一定的刷卡记录，有助于提额养卡。



自己办POS机刷卡套积分显然并没有发生真实的交易，而且在套取积分的同时也是在套现。交通银行信用卡中心总经理王卫东谈道，本来一个POS机对应一个商户，现在一个POS机对应一万个商户（号称万户侯），可以轻易的模拟出20倍甚至100倍的虚假交易场所。

### 信用卡风控

不是本文重点内容，有兴趣的朋友移步

https://zhuanlan.zhihu.com/p/33565863

### 互联网行业羊毛党

互联网时代之后，商户为了销量，知名度等的考量，推出的网络促销活动，衍生出来了互联网行业的羊毛党，也是当前羊毛党这个词的默认归属。

### 风控规则发展

以新用户为例介绍认证过程

任意注册：早期的邮箱，QQ号等都是随意注册申请的。一个人可以有N多的账号。可以用脚本批量注册。

图形验证码：为防止脚本批量注册，出现了图形验证码。然后出现了打码平台与智能识别。现在简单清晰的图形验证码智能识别有很高的成功率了。所以又出了拼图验证码，互相对抗的路上越走越远。

邮箱：早期互联网，手机不普及的时候，注册都是要求邮箱的。然后有多个邮箱的人还是可以批量注册账号。

手机验证码：这个就将门槛提高了很多了，虽然有猫池这种软件，但是需要有这方面的见知。而普通大众并没有这方面的信息，所以可以杜绝全民薅羊毛。

手机特征码：手机有一个出厂的唯一特征码，就跟电脑的MAC地址是一样的东西。结合手机型号等信息也可以作为一个新用户认证标识。

姓名+身份证号:要求实名的网站，有此要求。但是现在有很多的社工库，此规则也形同虚设。

银行四件套：姓名+身份证号+银行卡号+银行预留手机号。四件套认证基本可以保证真人概率，但是由于买卖四件套交易存在，还是会被薅羊毛。

不同的端风控不一样。一个产品可能有：PC页面、安卓APP、IOSAPP、H5页面、M5页面小程序等，黑灰产可以从中选取一个风控简单的入口。

# 第五部分：案例分析

### 拼多多分析

以下内容来自知乎

2019年1月20日凌晨1点至上午10点，9个小时，拼多多出现了重大BUG，平台上可以无限制领取100元无门槛全场通用优惠券，大量羊毛党开始刷券，并且通知了大量无知群众，所有人都参与到这场盛宴中。

被薅最多的是1元钱买100话费以及Q币，而最终损失是一个天文数字。

作为天天与羊毛党相爱相杀的风控从业者，昨夜我顶着酒劲，折腾了一夜没睡。别问我干了啥，不懂薅羊毛策略的风控，在我看来全都是没有实战经验的弱鸡。

先讲下这次事件暴露了哪些问题，再讲追责。

1.在电商行业，对于无门槛券是非常非常重视的，因为不同于有门槛券（满多少减多少，创造GMV和毛利抵扣），某种程度上，无门槛券等同于送现金，所以针对无门槛券，必须有一系列的核身策略，保证这张券不能被相同的人所领取。

核身策略中最常见的就是不同账号出现了同一收货手机号，同一收货地址，同一历史行为，同一IP，同一设备ID，同一支付ID，LBS，资料血缘，关系网络等等等一系列策略，这些可以防范住最大批量的LOW比羊毛党和低端机刷党，是电商最常见基础防范手段。

2.由于无门槛券几乎等同于现金，所以除了核身策略，往往还有其他匹配的风控体系，例如单人领取金额上限（1个月内领券不得超过XXX元），例如券额限制（无门槛券不得高于单张10元），例如消费领域限制（不得用于购买Q币，话费，游戏充值等虚拟物品）等等等等，这一系列的策略的目的就是拦截灰产的变现体系以及追溯灰产身份，例如无门槛只能买实物，那么就必然要留收获地址，那么这个地址就可以做很多事情，即使是假地址。

而且实物发货的话，拼多多是来得及拦截发货和半路撤回的，我经历过这种大面积撤回包裹。

但昨夜，这一系列限制统统都没有，羊毛党的变现最看重的就是高流通性和赢通性的产品，例如Q币，话费，这些东西很容易就能洗干净变成现金，很多羊毛党都有专门的洗白通道，现在这个节点，速度快的羊毛党已经全部变现了。

3.即使1和2都没有，也应该有一整套监控体系，对于优惠券的流向以及流量监控，并且设置报警阈值，失效机制，熔断机制，这些风控和大数据都应该早就准备好的。

就算我上面说的实现起来需要时间，那么就基础电商平台该有的商品销售TOP10，品类TOP10这样的可视化数字大盘也该有吧？肯定第一时间就发现就TM这些Q币话费卖的好，GMV出现同比环比的各种异常。

根据123，透露出来的问题是，优惠券设置逻辑没有过大脑，高风险业务无风险意识，风控交易与反欺诈策略缺失，数据监控体系及熔断机制缺失，要么是拼多多的风控没脑子，要么就是业务驱动，逼的风控不敢多讲话，这不奇怪，电商公司都是业务驱动，GMV是爹妈，风控这种挡GMV的角色往往被业务踩在脚下摩擦。

4.说完风控，再看看其他部门。

这张券是凌晨1点上线的，无门槛，大面额，全品类通用，假使这张券真的应该存在，那么，这种券的上线难道没有经过多级审批么？测试没有测出来吗？上线后没有至少120分钟的持续观察效果吗？

整个系统上线流程都有问题，运行监控也是缺失。

相关的研发到测试到运维，都有很大的责任。

5.问了下内部的朋友，说是这张券是某人配置失误，系统自动上线。

那问题又来了，整个优惠券系统里面，对于券的条件限制（金额，门槛，适用范围）是缺失的，并且在券发布的时候，没有中间隔一层预发环境来做缓冲，也没有做流量测试，就能直接上生产环境？上了也没有持续监控？

即使是配置的运营犯傻逼，但涉及到现金的业务如此草率，这部分研发是拼多多上买来的吗？

结合4和5，透露出的问题是，整个系统上线机制不合理，业务系统配置中没有加入风险校验环节，预发环境形同虚设，业务上线后的持续人工监控缺失。

考虑到拼多多拿来吹的高并发支持，我只能理解这条壮汉外功已经登峰造极，但内力大概是肾虚的小学生水平，这不意外，因为内功修炼是很难拿出去吹KPI的，所以大神程序员都不愿意做，都是能用就行的态度，这是血的教训。

6.我们来谈谈如何止损。

6.1已充出去的Q币和话费，如果还没有被羊毛党变现，那么也许还能追会一部分，QQ可以直接回收账号，三大运营商也能锁号扣费，但是这里面涉及到了很麻烦的一个问题。

那就是他们凭什么配合拼多多？因为这些交易都是拼多多认可后才让他们执行的，他们没有道理由着拼多多人性，腾讯爸爸可能会帮一把亲儿子，但是三大运营商可未必会配合。

另外不知道拼多多和他们是怎么结算的，是像iphone代理一样实时结算，还是类支付宝的先资金池再按时结算。

如果是前者，那基本很难追回了，如果是后者，那就是一场惊天撕逼大战。

6.2拼多多肯定不会善罢甘休的，羊毛党深知这一点，所以才在薅够了之后公开这个BUG，期望把水搅混，法不责众。

这个BUG是夜里5点左右公布出来的，然后就是全民狂欢，这些狂欢的人，我们一般称之为肉机，就是真人，真机，真身份，真行为。

现在的情况是，假使拼多多报警，能否抓到这些羊毛党头子，作为攻防的老手，我想说的是可以抓，但前提是拼多多有足够多的人力物力往里面投，并且数据保留要足够精准。

如果拼多多的数据部门和运维部门傻逼到定时清缓存，或者设置了某个系统BUG直接重启的话，那就不用抓了，没数据你怎么追溯。

另外就是这些被刷的都是虚拟物品，就看拼多多能不能抓住他们变现的节点来追溯身份了，祝他们好运。

6.3这批羊毛党一定有法律风险，但是只是那批最low的会被逮住，最大的几个早就变现隐匿了，人家用的东西都是没法追溯的。

真正的反追溯不是隐藏自己，而是创造更多虚假的自己，这才是高手所为。

6.4不用担心拼多多破产，最终的实发金额，亏损金额，未追回金额等等一系列的数字没有那么夸张的，不过买了拼多多股票的各位，下一个交易日见，对于电商而言，这么初级的错误很有可能会导致投资者信心丧失。

总结一下这个案子，拼多多是狂奔的超级独角兽不假，但在业务猛增的时候，内功没有修炼好，导致被一剑封喉。

原本就不该出现这种券，就算出现了也不该上线，就算上线了也应该被监控到，就算没有监控到也不该被同一批人领走，就算被同一批人领走也不该能应用于虚拟物品，就算能被应用于虚拟物品也不该9小时后才被制止，这其实不是一个问题，而是一系列问题。

这一系列不应该的阴差阳错，导致了这个巨额亏损，那么问题来了，这一系列问题下，拼多多的交易数字还可靠吗？之后美股怎么看这件事？这也是一场好戏。

内功一塌糊涂。

至于为啥不修内功嘛，一来修内功外人看不到，对外不方便吹逼讲故事，对内不利于个人晋升答辩（毕竟风控这种东西，除了金融领域，都很难量化成果），这种事情聪明人最不爱做了，可惜这只是小聪明。

二来嘛，很多电商为了讲故事，拉高估值，GMV可着劲儿注水，高层睁一只眼闭一只眼，很多运营恨不得管羊毛党叫爸爸，跪求他们来薅，反正羊毛薅完，GMV是特别好看，亏损是公司的，绩效奖金和升职加薪是自己的，所以何苦来哉？

对风控而言，最大的敌人，永远在内部。

这是风控的宿命。