微三云揭秘：羊毛党的克星！揭秘新零售场景下的账户风险管理之法

产品名称	微三云揭秘：羊毛党的克星！揭秘新零售场景下的账户风险管理之法
公司名称	深圳市微二云信息技术有限公司
价格	12800.00/套
规格参数	SAAS账号:12800元 源码:38000元 源码+定制:面议
公司地址	广东省东莞市东莞生态园瑞和路1号松山湖高新技术创新园B栋2-5层
联系电话	13929266321 13929266321

产品详情

微三云揭秘：羊毛党的克星！揭秘新零售场景下的账户风险管理之法

时下，新零售正在成为一种潮流，“ 大数据 ”反欺诈是新零售中必不可少的一环。

更进一步说，新零售下的“ 大数据 ”反欺诈管理系统，面临着诸多挑战和机遇。一方面，风控变得简单了，在拥有了海量的个人数据之后，对人的分析变得简单了；另一方面，随着新技术的应用普及，黑产份子的各种行为也变得更加隐蔽，他们的各种行为淹没在海量的普通消费者的数据中，导致对黑产的风控异常识别也变得更有挑战了。

综合近些年苏宁
金融在风控管理上的一些经验，我们从垃圾注册防控、养账户群体的识别、盗卡盗账户防控等维度，来探讨新零售下的安全防护问题。

一

垃圾注册防控

垃圾注册防控是在用户进入系统时的第一道安全防控关卡。

互联网平台通常通过各种优惠措施，如注册奖励等手段实现短时间内聚集大量用户注册的目的。对于厂商而言，各种优惠措施如果是给每个真实的消费者，属于一个双赢的局面：用户获得了实际优惠，厂商获取了大批量的真实用户群体。

然而，“ 有人的地方就有江湖 ”，总有黑产分子利用互联网的隐匿性，通过技术手段实现批量的虚假账户注册，进而获取注册账户带来的利益。这样给用户和厂商都造成了损失：一方面，真实用户的注册权益被虚假用户挤占；另外一方面，厂商的营销目的因为海量虚假账户的注册而遭受损失。

垃圾注册的防控怎么做呢？其核心就是寻找其账户群体的规模聚集性。

互联网上的账户注册，都可以追踪到其注册的来源（IP地址），短时间内如果有大批量的账户在同一地址上发生注册行为，我们就能很快的锁定它们，并封堵漏洞。

例如，短时间内设置一个IP地址上的注册账户不能超过xx个。

同样，这也逼迫黑产分子进行垃圾注册技术的升级，即利用代理资源池IP地址列表来动态地变化账户注册的IP地址。

但是，当黑产分子利用软件控制每个IP上注册的账户数量时，以上的控制策略将很容易被攻破。黑产分子通过在每个IP上注册小数量的账户，分散多个IP进行（即代理IP资源池），依然能够实现垃圾注册攻击的成功。由此可见，简单的限制IP上的注册账户数量，无法防范和抵御垃圾注册的攻击。

这个时候，互联网厂商的防范垃圾注册的技术升级包括：

（1）识别IP的属性。通常代理资源池的IP和普通运营商提供给用户上网的IP是不一样的。

（2）寻找更为安全可靠的聚类算法。如时间密度函数算法，实现短时间内批量注册分组的识别。

（3）对注册权益的领取设置更为严格的条件。如需要实名认证来领取，这种措施也大大提升了黑产分子的成本。

二

养账户群体的识别

养账户群体识别是互联网电商的第二道防线。

当批量注册账户、防控漏杀的账户（黑产分子通过限制每个IP上注册的数量，以及拉长注册的时间，进而完成注册的账户群）成功进入电商账户体系后，他们会利用这些打入系统内部的账户进行如下的几种操作：

（1）针对注册新用户的权益进行变现，比如领取新人打折券、代用金等。

（2）通过养账户，择机进行营销薅羊毛。其中“ 养账户 ”表现为通过机器实现定期批量登录、浏览网页（模拟）等，伪装成为正常的用户，等待各种营销活动的出现。

（3）定期维护账户的登录、浏览，利用爬虫技术，获取商家的各种折扣信息。

（4）短时间内的定期维护账户，实现“ 白户 ”转为丰富造假账户，进行欺诈活动。

防范此类账户产生的危害需要聚焦一个核心点：“ 聚集性 ”。通常，此类账户都是黑产人员通过机器进

行批量控制，因此其账户群体明显具有一致性的特征，如批量登录、批量打卡等。电商的反欺诈系统通过大数据的各种技术，识别出聚集性规模账户群。

此类聚集性规模账户群存在的风险，随着不同的业务线，呈现出高低不同的潜在风险因素。例如，在互联网金融领域，养账户群体，通过规律的登录、购买的行为，会被系统认定是普通的账户群，因此借贷时，群体规模风险没有识别出，造成损失；而在传统电商领域，养账户群则可能对各种营销发券进行攻击，导致营销活动的损失。

举例来说，苏宁金融的养账户群体的识别防控用到了两类技术：

（1）大数据环境下的聚集性检测技术——综合不同的事件（各种具体的营销事件）、时间、IP地址、设备ID、手机号码等多维度信息，实现规模账户聚集性的识别；

（2）关系图谱技术——通过手机、收货地址、设备等多维度的信息关联，实现账户群体的发现。

三

盗卡盗账户防控

盗卡盗账户防控是另外一个账户管理的基础核心要素。而盗卡盗账户事件多发生在账户所在平台的安全系统被攻破，或者第三方平台的账户泄露引发的安全风险。对盗卡盗账户的防控主要通过时间、地点、设备、行为几个维度的异常进行判别。

例如，用户在平台的登录通常呈现出规律性的特征，比如地理位置不会发生较大的偏移，比如设备具有稳定性，比如购买的商品类型也符合一定的规律。当以上的维度发生异常时，通常我们的反欺诈系统会首先锁定订单（称之为截单）。

盗卡盗账户的防控，通常还会和风控舆情结合起来，通过风控舆情平台识别出近期出现的“拖库”、“撞库”事件，并进一步探查哪些账户发生了泄露，是否在本平台有一样的邮箱、手机号等信息，进而对该批账户提升风控的警戒水平或者直接短信通知等。

四

账户安全管理的延伸

新零售下的安全场景，实际覆盖三个维度：“人”、“货”、“场”。其中，对“人”的防控是核心根本，对“货”、“场”的防控是在“人”的防控基础上的场景延伸。

例如，针对“货”的安全管控，需要重点关注3C领域，对容易套现出手的电子商品进行严格的控制，特别是对有互联网金融借贷结合的账户群体，更需要严格的风险管控。

又如，针对“场”的安全防控，通常表现在对黄牛、中介的群体识别上，即通过某门店的风险聚集性，识别线下门店潜在的黄牛团伙、中介团伙等。

需要指出的是，新零售下的安全防控不能仅仅是被动的防御，还需要御敌于国门之外。这意味着，新的电商安全防控系统需要主动的探测潜在的黑产动向。通常，我们利用风控舆情监控系统（互联网爬虫技术及时抓取黑产论坛中的各种信息，用于分析最新的黑产动向）提前做好准备。

此外，新零售下的风控，对比传统的风控手段，不仅仅是技术上有了更为广泛的集成和应用，业务策略、规则等也随着大数据分析的介入，有了更为全面和细致的防范布置。

不过，随着业务变更、技术变更的发生，新的技术应用和策略也是一个动态调整的过程。总之，新零售下的风控，以动态变化的技术为驱动力，以实现安全防控的长久稳定为终极目标。

新零售系统源码开发、新零售商城APP小程序开发、拼购类社交电商、会员制社交电商、社区团购、内容电商APP社交电商系统源码、社区团购系统源码、莞云系统源码，云平台系统源码，微三云系统源码、莞云＆云平台加盟代理，免编程电商ＡＰＰ平台制作、社交新零售商城开发、智慧新零售系统开发，找微三云！

东莞市商二信息科技有限公司旗下品牌微三云，创立于２０１４年，是高新技术企业、双软认证企业，经历５年深耕，从４个人发展到如今４００多人，年软件系统销售额超过２个亿，服务企业３０万多家。

公司专业提供微信小程序定制开发、抖音小程序开发、ＡＰＰ定制开发，目前已打造出微信商城分销系统、移动社交分销ＡＰＰ、线下多门店收银系统、城市Ｏ２Ｏ系统、跨境电商系统、社交电商系统、社区团购系统、挂售卖货系统、拼团系统、区／块／链系统、内容付费直播系统等。

公司产品功能应用创新，覆盖新零售解决方案、生鲜电商解决方案、新美业解决方案、同城解决方案、商家联盟解决方案、会员共享跨界盈利解决方案、
百货商超解决方案、农村电商解决方案、智慧养老解决方案、智慧城市解决方案、跨境购物解决方案、服饰鞋帽解决方案、智慧停车解决方案、智慧货柜解决方案、无人零售解决方案、抖音小程序私域流量解决方案，一物一码解决 方案等。

我们的公司地址：广东省东莞市东莞生态园瑞和路１号松山湖高新技术创新园Ｂ栋２－５层

电话：１３９－２９２６－６３２１麦总监（微信同号，加好友了解最新模式解决方案和系统优惠政策）

关注公众号“ 紫弘智慧 ”或搜索微信号（ｚｉｈｏｎｇ３３３）关注，了解更详细资料