唯品会 | 唯品会安全应急响应中心

因唯安全 所以信赖

2017唯品会第二届电商安全峰会

——深度揭秘唯品会信息安全建设实践

苏州
中国·苏州

业务与安全的冲突和平衡

唯品会高级安全产品经理　刘新永

议题简介

- 风控与业务、安全与体验似乎一直处于冲突和对抗之中。
- 在最重视体验的电商企业和业务驱动的组织生态，如何破解业务和安全的冲突怪圈，确立业务和安全的平衡目标？
- 让我们一起从产品设计的视角来探索业务和安全的取舍之道。

冲突分析——两种常见冲突

1. 体验之争

- 安全风控措施影响了谁的体验 ？

2. 转化率之争

- 是转化了用户还是便宜了黑产？

根据统计，如果任何安全风控措施保障的情况下，一般线上的拉新（转化新客）优惠活动，马甲用户率达90%以上（羊毛党、黄牛党流量）

冲突分析——正确地理解体验

正确地理解体验 ：

- 安全为体验提供基础保障
- 体验是便捷性、严谨性、安全性的综合统一

冲突分析——重新认识转化率

正常用户流量 = 全部流量 — 黑产流量

$$转化率 = \frac{进入下一流程的正常用户流量}{上一流程正常用户流量}$$

冲突分析——原因总结

冲突原因：

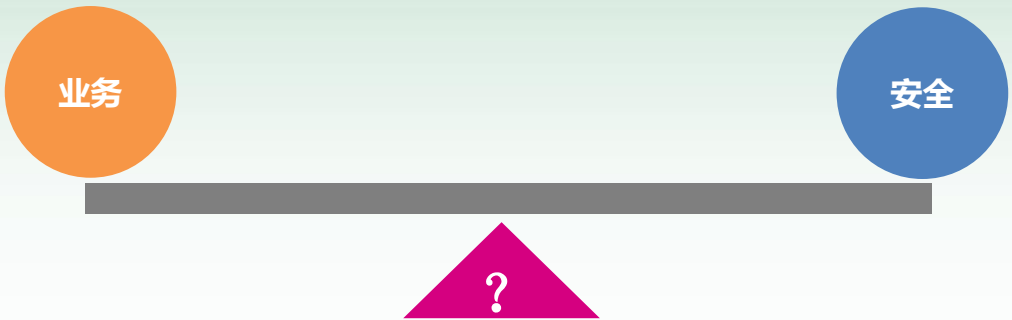
- 把黑产和用户混为一谈（主观）

  搞不清真正的目标用户是谁、业务的真正目的是什么

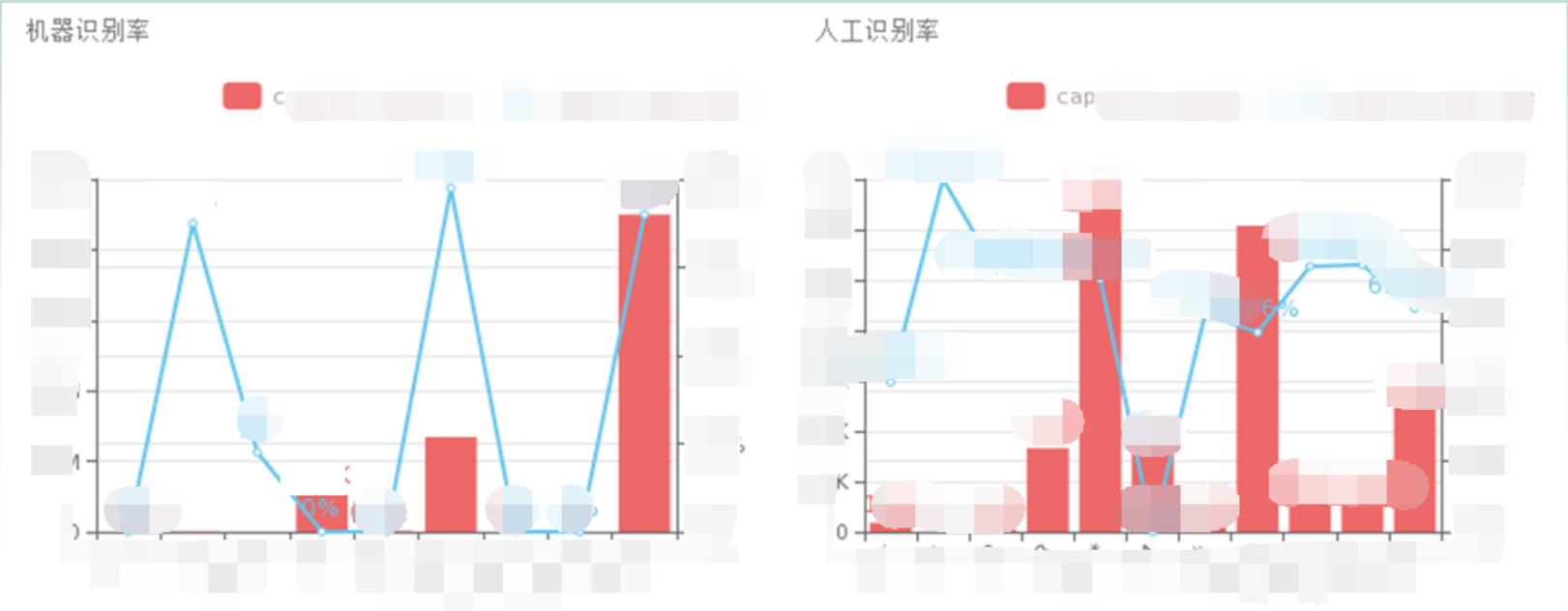
- 技术局限性和标准不统一（客观）

  无法完全泾渭分明地界定黑白

如何化解冲突



三大法宝之“Use data to talk”



三大法宝之“按需配置”

可配置化设计  安全风险控制
业务灵活运营

三大法宝之“以业务目标为基线”

新客ROI  “薅羊毛”

典型案例分析——“一元夺宝”

- 用户支付1元，获得一个抽奖码，每份宝物每用户一次参与机会
- 一台iphone售价6,000份抽奖码（相当于售价6,000元，等于或略高于市场价）
- 没有中奖退回100唯品币
- 100唯品币在唯品会相当于1元购买力，不可转让，不可提现，有效期一年，过期作废

黑产投入产出分析（收益在于没中奖的补偿）

业务场景	收益	说明
购买100%抽奖码	599,900唯品币（5,999元）	1，每账户唯品100币（1元），分散于5,999个账户，较难形成购买力变现 2，销售手机成本（渠销售道？折旧？） 3，政策风险，中奖率也不好保障
购买50%抽奖码（购买2份）	599,900唯品币（5,999元）	
未中奖	现金变成等额唯品币	亏钱

典型案例分析——“一元夺宝”

- 用户支付1元，获得一个抽奖码，每份宝物每用户一次参与机会
- 一台iphone售价6,000份抽奖码（相当于售价6,000元，等于或略高于市场价）
- 没有中奖退回100唯品币 **● 没有中奖退回1元现金**
- 100唯品币在唯品会相当于1元购买力，不可转让，不可提现，有效期一年，过期作废

黑产投入产出分析（收益在于没中奖的补偿）

业务场景	收益	说明
购买100%抽奖码	599,9元（现金）	1，无论原路退回还是退回账户钱包 2，销售手机成本肯定不会高于5999元 3，政策风险不好利用（恶意投诉压力大增）
购买50%抽奖码（购买2份）	599,9元（现金）	
未中奖	0元	可零成本刷羊毛

典型案例分析——“一元夺宝”

- 用户支付1元，获得一个抽奖码，每份宝物每用户一次参与机会
- 一台iphone售价6,000份抽奖码（相当于售价6,000元，等于或略高于市场价）
- 没有中奖退回100唯品币 **● 没有中奖退回1元现金**
- 100唯品币在唯品会相当于1元购买力，不可转让，不可提现，有效期一年，过期作废

用户体验对比分析

没有中奖退回100唯品币	没有中奖退回1元现金
没中奖，退回的100唯品币，有绑架嫌疑，用户心理可能会有一定沮丧感	没中奖，没损失，愉快体验
带来一定的用户购买粘性	无后续用户购买粘性

不中奖退回100唯品币 

- 遵循便捷性、严谨性、安全性的原则，业务与安全达到理想平衡状态
- 不需要额外的安全风控措施保障，确保了整体用户的优秀体验

不中奖退回1元现金 

- 为了照顾小众用户体验，需要暴露一个风险极高的接口
- 需要增加安全风控措施控制风险，整体上降低了用户体验

最高安全防御境界：“不战而屈人之兵”

Q & A

谢谢您的倾听！

唯品会 | 唯品会安全应急响应中心

VIP Security Response Center

唯品会安全应急响应中心

专业

我们致力于保护用户信息安全

我们积极营造更加安全的

线上电商购物平台

微信号：VIP_SRC

官方网站：http://sec.vip.com

微信公众号：唯品会安全应急响应中心

漏洞接收邮箱：sec@vipshop.com