Oceanpayment

欺诈交易防控

风控部　　2022年02月04日

Oceanpayment

01

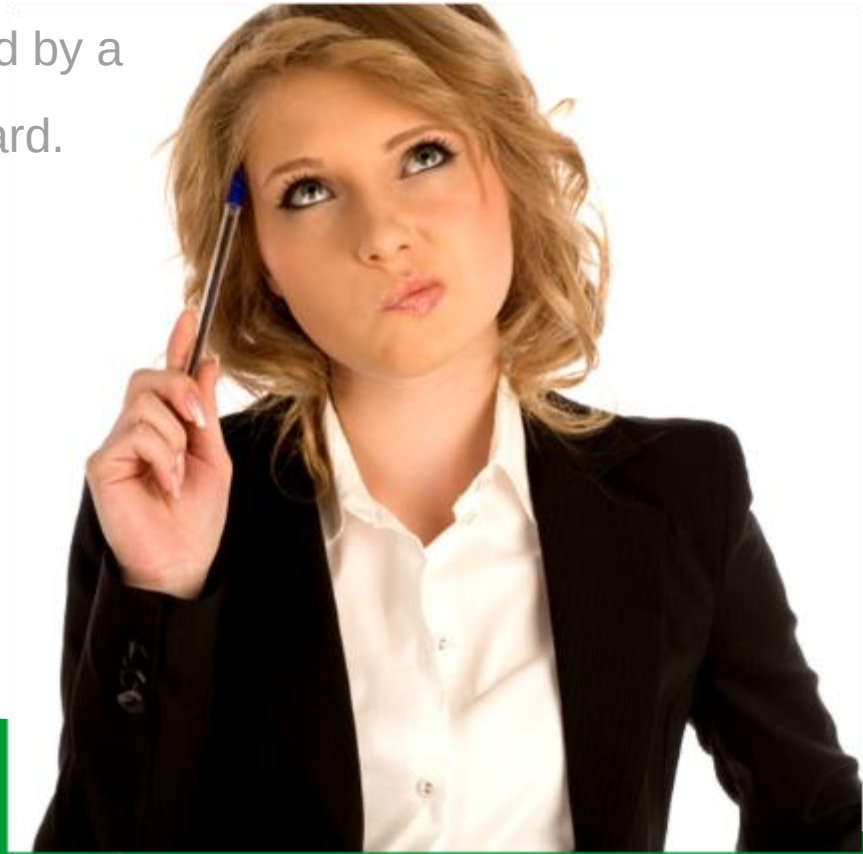
为什么要防范欺诈交易

什么是拒付Chargeback

信用卡拒付

任何反馈到收单行将资金退回持卡人账户的有争议的信用卡交易。

A chargeback is the reversal of financial transaction,typically initiated by a customer(the cardholder),who disputes a sale on his or her credit card.



拒付时间期限

一般为交易后180天内，某些行业（如航空行业）和某些发卡行可以接受更长时间期限的拒付申请。

Visa拒付考核标准

Visa拒付控制标准（VDMP）

Visa Global Chargeback Monitoring Program（VDMP）

级别	VDMP
Level 1（Early Warning ）	0.65% and 75 chargebacks
Level 2（Standard Program ）	0.9% and 100 chargebacks
Level 3（Excessive Program ）	1.8% and 1000 chargebacks

Visa拒付率计算方式：

MasterCard拒付考核标准

Excessive Chargeback Program（ECP）

Excessive Chargeback Merchant (ECM) and High Excessive Chargeback Merchant (HECM).

级别	新考核标准
ECM	1.5% and 100 chargebacks
HECM	3% and 300 chargebacks

Mastercard拒付率计算方式：

如果商户进入ECM程序时，且收单机构延期向Mastercard提交该商户的ECM整改报告，则Mastercard在过期的15天内，向收单机构收取评估费500USD天，后续1000USD/天，直至收单行最终提交ECM整改报告。

欺诈交易严重影响卖家的发展和消费者的体验

- 跨境支付欺诈是很多跨境电商都遭遇过的问题，也给卖家带来了不小的损失。
- 而且很多卖家因为没有判断风险的能力，拒绝掉正常的客户的比例也非常高，这些都严重影响了企业的发展和客户的体验。

中小卖家由于缺少人力物力，较难建立起一套完善的风控体系，因此比较容易成为欺诈交易者攻击的对象。那么是否有策略可以减少这种风险呢？

Oceanpayment

02
减少欺诈风险的策略

确保使用的建站软件是最新版本

许多中小卖家会使用第三方的建站软件或平台搭建商城，建站服务商本身也会十分重视防范欺诈交易者，因此会经常对建站软件进行升级，防止建站软件出现漏洞被黑客利用。

卖家需要做的就是保持软件的同步更新

要求消费者设置复杂的账户密码

Oceanpayment

设置复杂账户密码

为了避免因消费者账户被盗而产生欺诈，在消费者创建网站账户时，卖家可以让消费者设置复杂的密码减少被盗的风险，比如，要求消费者运用大小写字母、符合、数字的组合设置密码。

密码保护

此外，在注册时最好让消费者填写一些用于安全保护的信息，如询问他们的幼儿园学校名称或出生地点等，当消费者遗忘密码或账户被盗时，可以通过验证问题找回账户。

充分了解你的消费者特征

- 卖家销售的产品不一样，或推广的地区不一样，面对的消费群体也不一样，每个群体都会呈现出独特的消费特征，可以根据这些特征捕捉异常情况从而识别欺诈者。

- 欺诈订单往往以批量购买产品的形式出现，且对尺寸、颜色、设计、型号等没有任何喜好，卖家应该谨慎接受这类订单。

关注高频订单

- 通常情况下，欺诈性订单会热衷于易于变现的产品，相同的产品更方便欺诈者变现。所以相同消费者短时间对相同的产品购买多个订单，建议卖家谨慎接受此类订单。

- 欺诈者一般会通过在网上多次尝试支付，来验证信用卡信息的可靠性，这个过程通常会因为风控或银行信息不匹配等原因而失败。在成功交易之前，一两次的失败比较正常，但如果在成功交易之前出现批量的失败，卖家就应该警惕了。

- 卖家可以设置一个重复下单的次数限制，一旦达到这个限额，消费者账户将会被锁定且无法使用购物车，然后要求消费者联系客服核实身份后再完成购买。

针对高价商品采用3D验证

- 通常情况下，欺诈性订单会集中在高金额的产品，因为高金额的产品可以给欺诈者带来更多的利益。当同一消费者的交易金额过高，或频繁购买高金额的不同产品，建议卖家谨慎接受此类订单。

- 此外，对于单价较高的商品，卖家还可以通过设置信用卡的3D验证来防范消费者的欺诈拒付。

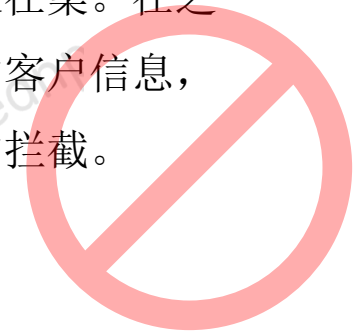
电话确认异常交易

- 需要注意的是，并不是所有的异常交易信号都能马上判断为欺诈行为，在不确定的情况下，卖家可以通过消费者留下的电话联系对方，与消费者进行沟通，核实消费者的相关订单信息。

- 很多时候，欺诈者都不会留下真实的联系电话，因此这种方式可以很好的查验消费者的身份。

建立欺诈黑名单

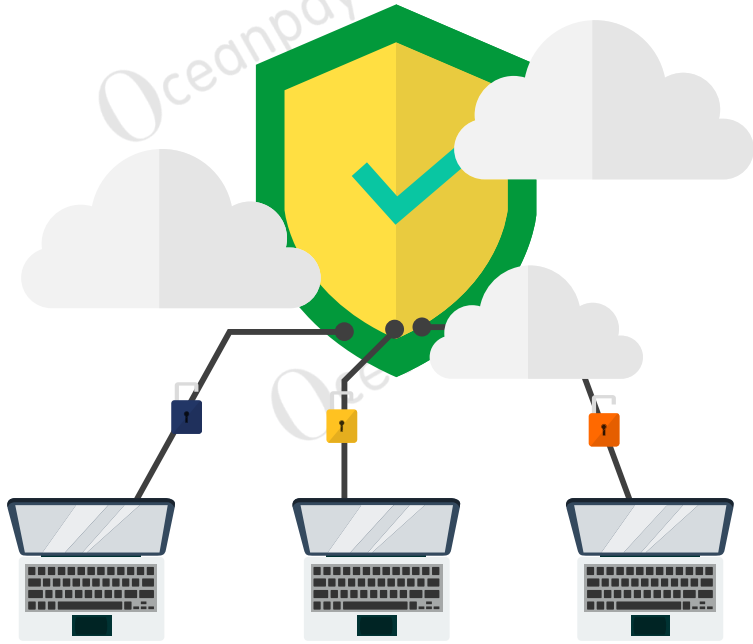
- 如果欺诈性订单已经被确认，那么所有与这个订单相关的信息，都应该记录在案。在之后的交易中，一旦出现了相同的客户信息，卖家需要对这类交易进行相应的拦截。



选择专业的跨境支付服务供应商

- 事实上，识别欺诈交易者是一项十分复杂且专业的工作，**对于卖家而言，最好的策略是找一家值得信赖的跨境支付服务供应商帮助把控交易风险；**

- Oceanpayment的智能风控系统能够根据不同交易风险特征，通过多维度分析和大数据匹配精准识别出异常交易，及时发现欺诈者，保障卖家的交易安全。



THANK YOU

扫一扫，
让全球支付更简单

info@oceanpayment.com.cn
HK@oceanpayment.com
www.oceanpayment.com
+86 4006 290 296