【助力小微企业发展】电商发展势头迅猛，小微企业针对网络欺诈管理的五招

Visa 金融 Edu Visa 金融 Edu 7 月 2 日

近几个月来，在商业活动加速从线下转向线上的同时，网络欺诈也随之飙升。2020 年第一季度，全球有超过四分之一的交易是以欺诈为目的的（数据来源：securityboulevard.com）。

为了发展业务，服务客户，企业需要受理交易，但同时又要管理好防欺诈风险，在两者之间取得平衡并非易事。全球的小微企业现在已经意识到必须迅速做出调整，转为在线上服务顾客。而转型的关键之一是在保障安全体验的同时采用合适的电商工具。

欺诈分子知道，一些小微企业在销售和欺诈审查团队人力不足时，往往倾向于放宽反欺诈措施。欺诈分子会试图利用这一时机发起攻击，小微企业应当即刻制定全面的反欺诈策略。

在计划和执行策略时，你可以参考以下欺诈管理建议：

积极采用双重认证：

同时开通多个账户，并与同一组用户信息关联的现象激增，这为账户伪造欺诈制造了机会。因为账户休眠一段时间后，看上去会很像合法账户。一旦商家系统视账户为合法的，它便成为了欺诈发生的源头。

请告知你的顾客分享备用电子邮箱地址或手机号码，帮助确认帐户是否处于正常使用和正常消费。另外可以定期检查账户的购买记录。

防范卡片测试：

欺诈分子可以通过卡片测试（欺诈者通过算法不断尝试，获取卡片相关信息，最终牟利）获取被盗的卡片信息，而中微小企业往往会成为卡片测试攻击的目标。

诡计多端的欺诈分子现在使用计算机生成的脚本，一次便可测试成千上万的卡片信息。请确保在结账页面和卡片添加页面（或者任何其他验证卡片的页面）使用检测和防范自动脚本提交交易的技术，其中一些防范技术包括对僵尸网络进行基本探测的防火墙和 CAPTCHA 验证码。CAPTCHA 是用来区分人为和自动化脚本的视觉测试。

监控账户接管：

欺诈分子会利用预存卡号信息的支付模式（快捷支付），“接管”新创建的账户和休眠账户，用于下单实行欺诈。

值得注意的几个特征包括：多次更改最新的收货地址，或者来自旧的休眠账户的订单增加。

检查具体送货信息：

欺诈分子已开始在结账页面上篡改收货地址，或者将商品送至无人居住的房屋或新建筑，这样他们就可以取走留在屋外的包裹。注意收货地址的第二行或第三行的信息，这可能是篡改后的送货路线。

从而要规避只查看收货地址第一行的风险防范策略或交易速度规则。

支持无接触配送：

为了保障快递员和顾客的健康安全，大部分配送合作商现在都支持无接触配送，但这方式也可能导致“未收到商品”的争议。如果你自行送货，请拍下照片作为送达证明，有助于应对声称“未收到商品”的情况。

Visa 已经察觉到线上消费形式的变化，现提供 CyberSource 和 Authorize.Net 解决方案，其中包含众多工具，帮助小微企业转型，并在数字化环境下取得长足的发展。

为了助力完成数字化转型这一富有挑战性的任务，至 2020 年 8 月 1 日，Authorize.Net 为访问 Authorize.Net 网站并注册的新商户免除网关使用月费，商户可以通过网站获得多种数字支付和反欺诈工具。

当前形势下，确保业务安全可靠运行比以往任何时候都更为重要。**欲了解更多信息，请访问：https://www.authorize.net/。**

小贴士

Visa 专门面向小微企业定制的“实用商业技能”培训课程，已经通过国内首个金融教育公益网站“实用理财技巧”（practicalmoneyskills.com.cn）以及金融教育微信公众号——“Visa 金融 Edu”，免费向国内的小微企业主提供通俗易懂的、可靠的在线教育资源，提升小微企业主和企业员工的商业及个人理财技能，提高他们的适应能力和应变能力，帮助他们实现增长。