Oceanpayment
Global Digital Payment Solution Provider

【风控-欺诈攻击】

批量地址欺诈攻击分享

2025/10/15

【风控-欺诈攻击】批量地址欺诈攻击分享

Oceanpayment 自 2025 年 6 月份起，出现一类欺诈攻击，统计 2025 年 6 月至 2025 年 10 月 13 号，共计攻击笔数 52994 笔，涉及金额 389046USD 左右，没有成功订单。

1. 本次欺诈攻击涉及商户数量共计 249 个，主要攻击以网站的低客单价产品链接为攻击产品

2. 欺诈风险特征分布

- 相近/相同地址出现多邮箱多卡
- 攻击的订单间隔时间很短
- 地址集中：77 greatwood lane、11n lane avenue south、123 main （实际和账单地址回传 new york 为同一批）
- 接近 80%的订单集中在 10USD 以下

单笔金额分段	笔数	占比
10USD 及以上	11097	20.94%
10USD 以下	41897	79.06%
总计	52994	100.00%

- 邮箱后缀相对集中

邮箱后缀	笔数	占比
@gmail.com	31044	58.58%
@outlook.com	10897	20.56%
@yahoo.com	10742	20.27%
@outkook.com	311	0.59%
总计	52994	100.00%

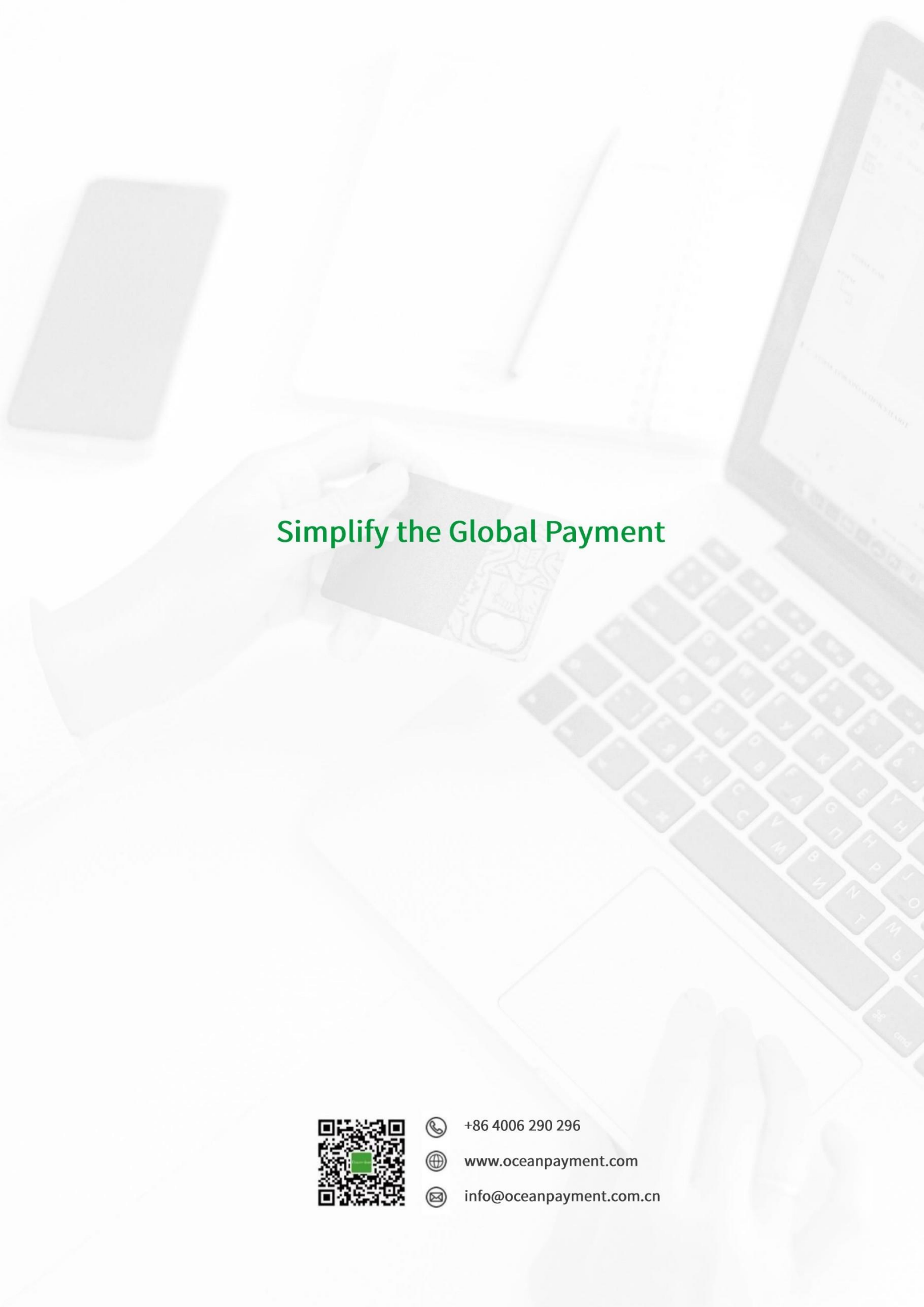
- 发卡国家分布看，主要集中在美国、日本、英国和东南亚主流国家，且77%以上是存在 IP-发卡跨国

卡所属国家	笔数	占比
US	19843	37.44%
MY	6667	12.58%
PH	2644	4.99%
SG	2355	4.44%
TH	2124	4.01%
GB	1602	3.02%
AU	1457	2.75%
JP	1234	2.33%
CA	1117	2.11%

3. 受攻击的网站全部为 shopify 的建站。通过调研发现 https://community.shopify.com/t/game-over-77-greatwood-lane-villa-rica-ga-30180/563744 反馈关于本次地址欺诈运用的相关论坛。

4. 总结：

- 近期欺诈特征，通过运用指定的地址，批量生成相关交易信息，主要盗用 US 和 MY 及其他东南亚国家的部分发卡行的信息，通过商户网站上的低金额产品进行高频率的 Card Testing Attack 测试卡号的有效性。这些订单在 Oceanpayment 已全部被风控识别并拦截。
- 相关的订单已全部纳入黑名单情报库，且实时风控已完成加强调整和更新。



Simplify the Global Payment

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