LexisNexis®
RISK SOLUTIONS

案例研究

LexisNexis® Risk Solutions 帮助大型电信公司检测并阻止欺诈，同时为优质客户减少摩擦

ThreatMetrix 数字身份情报能帮助近实时区分欺诈者与可信客户

概览

公司

电信和传媒公司

要求

- 近实时地阻止在申请过程中检测到的高风险行为。
- 减少优质客户摩擦。
- 减少与欺诈和大量人手审核相关的成本。

解决方案

借助 LexisNexis® Digital Identity Network®提供的全球共享情报，该电信公司能够部署端对端的动态身份验证和认证，更好地刻画注册新手机合约的交易用户的合法性。

结果

- 近实时地阻止在申请过程中检测到的高风险行为。
- 减少优质客户摩擦。
- 减少与欺诈和大量人手审核相关的成本。

总览

该电信公司是欧洲市场的一家巨头公司。公司开始将其服务组合延伸到消费者和企业，推出了一项新的手机服务，通过电话销售和在线方式提供合约机及仅售手机记忆卡的套餐。

业务问题

随着消费者持续要求即时通信及连通性、优先采用移动端服务，电信提供商们的负担越来越重，因为欺诈者寻求利用日渐增多的手机分布。

投放新手机服务过程中，该电信公司意识到自身很容易被欺诈者列为目标，通过派送的高端手机或者拖欠大额电话费来获取收益。公司需要能够近实时准确区分合法客户及欺诈客户的解决方案，同时促进优质老客户的无摩擦体验。

电信公司需要能够检测并阻止使用被盗身份注册新账户的欺诈者，以及阻止尝试盗用优质用户账号以订购新手机或者手机记忆卡的网络犯罪分子。公司还需要一款能够帮助检测欺诈性支付并识别想要将被盗信用卡凭证兑现的欺诈者的解决方案。随着消费者行为的日益复杂，而欺诈者越来越擅长模仿这种行为，公司迫切需要真正理解其入网用户的数字身份并区分优质用户与不良用户。

利用 LexisNexis® Risk Solutions 建立可信行为

LexisNexis® ThreatMetrix®提供的数字身份情报使运营商能够更准确地检测并阻止欺诈性的新手机申请。LexisNexis Risk Solutions 集成到申请过程的关键点中，这个过程从客户首次入网，一直到信用协议及手机和/或合约的支付。借助数字身份情报，电信公司能够在新账户注册时准确识别高风险行为与异常行为。根据 LexisNexis® Digital Identity Network®提供的动态行为历史数据，通信公司能够通过分析位置、设备和行为异常现象等属性，了解入网用户的可信度。电信公司还在申请过程的第二阶段部署了数字身份情报，用基于风险的评分补充额外的信用验证检验。检测新账户注册及信用协议阶段潜在欺诈性行为的整体分析让电信公司在签发新合约之前就能够检测并阻止潜在欺诈行为。

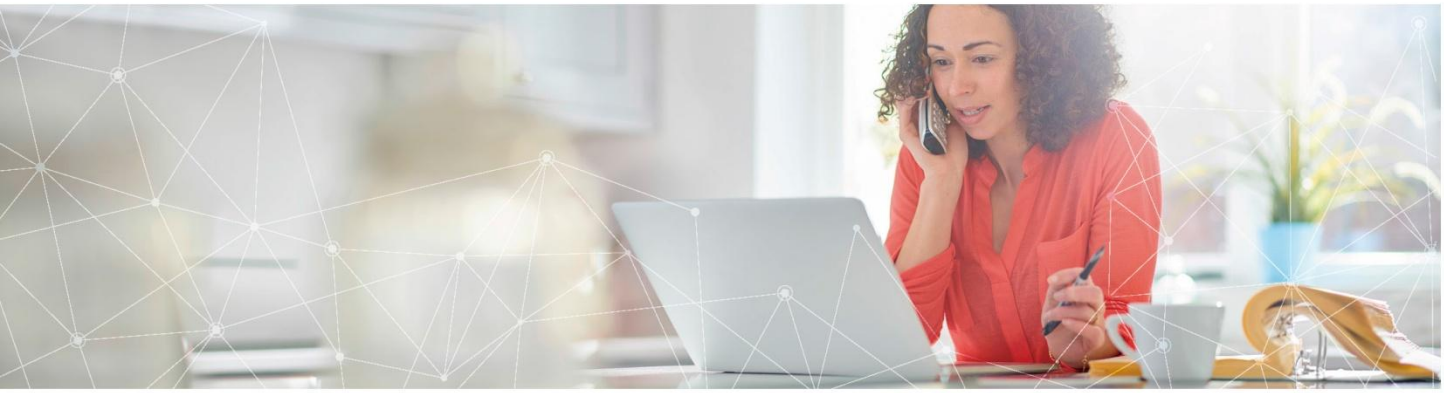
电信公司同时还利用 LexisNexis Risk Solutions 准确找出使用被盗信用凭证的欺诈者，并阻止欺诈性支付。也是因为有了 LexisNexis Digital Identity Network 提供的众包情报，该电信公司能够识别并阻止与先前欺诈活动相关的支付方法，其中一次阻止了一个在一台设备使用多个信用卡凭证的潜在欺诈者。

LexisNexis ThreatMetrix 让我们能够绘制出每名用户的准确图像，捕捉人们进行线上交易的独特属性。这种情报让我们能够显著减少欺诈并在三个月内实现 ROI。

案例研究

另外，ThreatMetrix 解决方案还被集成到电信公司所有用户账户的登录页面。如此，优质用户可以评为可信；这样做不仅减少了登录过程中的摩擦、预防账户盗用攻击，同时还能够简化未来手机合约的申请流程。运营商从与 LexisNexis® Risk Solutions 的合作中受益，同时反馈欺诈数据，可立即用于改善交易评分及风险评估。通过合作，欺诈驳回率大大改善，转诊及误报也得以降低。此外，电信公司还能够利用从交易中收集到的历史数据预测趋势；它们发现，创建超过 60 天的新账户 ID 欺诈率较低，而首次支付的预付费卡欺诈率较高。这些趋势被用于优化规则、进一步强化交易的评分及评估。

有了 LexisNexis Risk Solutions，我们可以利用历史数据及我们收集的欺诈数据即刻优化和加强评分。这意味着我们识别与检测欺诈的能力会随着每笔交易的完成而越来越强大。



案例研究

LexisNexis® Risk Solutions/电信公司合作伙伴的关键特征

- **受信标记**是指让企业能够确定、分类、标记和区分优质用户与不良用户、设备、位置或者人物的数字标签。信任可以与设备、电子邮箱、卡号等在线属性或者交易接受、驳回或审查等相关的任何其他属性的任何组合动态关联。

- **人物 ID** 能够帮助企业近实时将当前交易与相关交易相匹配。基于规则的机制通过与访问者、设备和链接相关的属性矩阵连接交易。它可以通过相关历史活动的关联，近实时地揭示异常行为。

- **深层关系分析技术**能够更清楚地看出可疑事件。尝试从异常或者高风险位置开立新账户的欺诈者可能会尝试隐藏在位置和身份隐匿服务（如隐藏代理、VPN 和 TOR 浏览器）后。利用代理穿透技术，LexisNexis® ThreatMetrix®可以对 TCP/IP 数据包报头信息进行审查，找出代理 IP 地址和真实的 IP 地址。

LexisNexis® RISK SOLUTIONS

更多信息，请拨打 852.39054010 或登录网站：
risk.lexisnexis.com/FIM-ZH