LexisNexis®
RISK SOLUTIONS

案例研究

大型金融机构在使用 LexisNexis® Risk Solutions 的第一年检测到的钱骡账户数量增长 50%

LexisNexis Risk Solutions 帮助银行为钱骡账户受害者退还了 965,000 美元

概览

公司

大型金融机构

要求

- 精确识别并阻止钱骡账户。
- 阻止欺诈者资金通过钱骡流动。
- 将由于钱骡造成的欺诈损失降至最低。
- 为优质客户优先提供无摩擦且成功的用户体验。

解决方案

有了 LexisNexis Risk Solutions 提供的数字身份情报，该大型金融机构就能够准确地识别并阻止钱骡账户，同时更大范围地检测钱骡网络，优先为合法客户提供无摩擦的体验。

结果

- 识别的钱骡数量提高 50%。
- 阻止了 965,000 美元资金进入钱骡账户并将其退还给受害者。
- 将优质现有客户的摩擦降至最低。

总览

该大型金融机构可以提供广泛的服务，包括个人和企业银行业务、私人银行业务、保险和企业理财。客户是银行企业文化的核心：信任是银行获取客户尊重与重视的重要内容。

业务问题

钱骡已经成为许多影响整个行业客户与银行的第三方欺诈和其他欺诈的主要推动因素。受到巨额财务收益的驱使并在各种数据泄露中盗取的凭证的帮助下，网络犯罪分子越来越擅长盗用真实的网上银行账户。但是，一旦欺诈者用盗用凭证侵入账户、或者针对真正的客户部署社会工程战略，则钱必须转入欺诈者持有并且可以将非法所得洗白的账户中。

钱骡是其银行账户用于通过金融系统洗白犯罪所得的人，通常有意或无意地被牵扯或招募进行洗钱活动。资金通过在多个金融机构开立的、看似互不关联的钱骡账户组成的大型网络快速流动，很难跟踪。

该大型金融机构曾面临识别其网上银行环境中的钱骡活动的难题，需要有一款不但能够检测此类活动，同时还能帮助阻止资金流动，并最终退回到犯罪受害人账户的解决方案。

“我们现在具备与钱骡一战的能力，LexisNexis® Risk Solutions 让我们能够采取更主动的方法检测钱骡。如果不是这种方法上的改变，我们根本不能将这么一大笔钱退还给这些骗局的受害者。”

利用 LexID® Digital 建立受信行为

自 LexisNexis® Risk Solutions 首次投入使用以来，银行已经识别出 50%以上的钱骡账户，并已经将 965,000 美元的欺诈所得资金退回到钱骡受害者账户中。这一成功离不开 LexisNexis® Digital Identity Network®的功劳。LexisNexis® Digital Identity Network®能够通过分析位置、设备和行为异常等属性，揭露代表钱骡活动的异常行为。

有了全球数字身份情报，银行能够清楚地看到钱骡活动产生的关联账户蜘蛛网。因此可以在登录时将已知的钱骡设备与新账户相关联，发送电子邮件警报，使其快速屏蔽这些新的钱骡账户。利用设备和 IP 情报联系设备，识别增加的钱骡和网络，在某个案例中，银行揭露了一个涉及 140 个钱骡账户的欺诈团伙。利用 LexisNexis Risk Solutions 提供的情报，银行还能够查明钱骡账户活动的位置，协助逮捕招募钱骡的欺诈者。

银行还根据行为模式部署了一个针对未知钱骡的钱骡模型。这样就可以从颗粒级别分析行为和模式，从而更准确地区分新钱骡与合法的行为变化。该钱骡模型允许可信用户行为发生变化，帮助减少合法客户的摩擦。

依据从数千笔全球交易中产生的数百万日常客户交易众包情报（包括登录、支付和新账户应用程序），LexisNexis Digital Identity Network 可以利用匿名的全球共享情报，更好地区别客户与欺诈者。

LexisNexis Risk Solutions / 银行合伙人的主要特征

- **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。

- **Smart ID** 能够识别清除上网痕迹、使用无痕浏览、以及通过更改其他参数以绕过传统设备指纹工具的老用户。此项功能可以帮助检测老用户，降低误报。根据对多个浏览器、插件和 TCP/IP 连接属性的分析，Smart ID 生成一个置信度得分，检测同一台设备发起的多次欺诈性账户注册。

- **真实 IP** 能够准确地检测位置和身份隐匿服务（比如隐藏代理和 VPN）的使用，让银行可以查看每笔交易的真实 IP 地址、地理位置和其他属性。
它还可以检测行为模式中的变化，比如异常交易量、交易速度或者频率变化。此项动态数据能够帮助识别欺诈性的行为，让银行能够获得更精确的背景信息，以决定是否接受、驳回或者审查任何交易。

- **深层关系分析技术**能够对可疑事件有更清晰的认识。欺诈者通常试图通过位置和身份隐匿服务（例如隐藏代理、VPN 和 TOR 浏览器等）隐藏自己。利用代理穿透技术，LexisNexis® Risk Solutions 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

关于LexisNexis Risk Solutions

LexisNexis Risk Solutions 充分利用数据和先进分析法的力量，助力企业和政府实体降低风险并改善决策，使全球人口受益。我们为各行业（包括保险、金融服务、医疗保健和政府机构）提供数据和技术解决方案。LexisNexis Risk Solutions 隶属于RELX 集团（LSE：REL/NYSE：RELX），该集团是一家全球信息和分析技术提供商，为各行业的专业及企业客户提供服务，总部位于乔治亚州亚特兰大市，办事处遍及全球各地。RELX 是富时100指数公司，位于伦敦。更多信息请登录 www.risk.lexisnexis.com 和www.relx.com。

关于ThreatMetrix

ThreatMetrix® 是一家LexisNexis® Risk Solutions 公司，它增强了全球经济实现盈利和安全增长的能力而不损害其安全性。凭借其对14亿个标记化数字身份的深入了解，LexID® Digital 提供了1.1亿个日常身份验证和信任决策相关的情报，以实时区分合法客户和诈骗者。

更多信息请登录：risk.lexisnexis.com/FIM-ZH。NXR14087-00-0919-ZH-GL