



## SAS® 欺诈网络分析

超越交易和账户视野,在网络维度分析所有活动和关系

### 挑战

- **不断演变的欺诈趋势。** 日益狡猾的犯罪策略和替代银行业务渠道的增多给欺诈检测和防止其变得更加具有挑战性带来了困难。
- **不断增加的复杂性。** 不断加剧的全球化 and 通过合并和收购来实现增长使得有效地监测多个产品系列和业务线更加困难。
- **系统限制。** 目前的系统不支持健壮的分析建模,且没有直观的界面来检视客户关系。
- **数据管理问题。** 各自为政的业务单元和分散在各地的客户使得以正确格式存取正确的信息并对之进行清洗而不危害那些可能被证明为“金块”的重要异常情况造成困难。
- **对风险概况(risk profile)的影响。** 人们经常混淆第一方欺诈与信用损失,这常常导致不准确的信用损失报告和对实际欺诈损失的错误解释。

### 概述

有组织欺诈正在成为银行面临的一个日益棘手的问题。其部分原因在于欺诈者的行为与合法客户非常相像。替代银行业务渠道和日益狡猾的欺诈技巧也加剧了这个问题。

为了检测欺诈活动,许多银行都使用了监测系统,监测系统对个人实时、销售终端欺诈非常有效。但监测跨越多个账户和系统的客户行为需要一种不同的方案,以便识别那些可能看似正常,然而却在“雷达区外”的行为——例如休眠账户突然出现资金抽逃(bust out),造成巨大损失。

遗憾的是,很少有银行对跨越多个账户和渠道的客户行为有很好的理解。这经常是由于没有用于分析客户数据,以发现趋势和可疑行为的分析工具。

目前的经济气候也迫使银行减少支出和靠更少的资源过活。目前用于检测欺诈活动的手动流程效率低下,并浪费了宝贵的时间和资源——这是银行在目前的经济情况下无法承受的。使用SAS欺诈网络分析解决方案(SAS Fraud Network Analysis)可改变这种局面。

### SAS® 解决方案

SAS欺诈网络分析解决方案(SAS Fraud Network Analysis) 可帮助银行和其他金融机构通过超越交易和账户视野,在网络维度分析所有相关活动和关系来检测和预防第一方欺诈。该解决方案:

- 使调查员能够使用可让他们准确查看网络连接的独特网络可视化界面揭示先前未知的关系和开展更高效的调查。
- 能够获取现有风险分数或危险信号(red flag),并在网络层面提供一个总分,以识别可能表明存在账户资金抽逃或共谋的细微或隐蔽关系。
- 生成独立或综合分数,以便在客户、产品和网络基础上评估整体风险,然后生成可自动发送至相应人员的警报。
- 让调查员使用一个可存取所有客户详细信息和访问所有相关各方及网络的直观界面生成围绕一个案件的完整网络卷宗。

### 选择 SAS® 解决方案的理由

SAS 为银行业提供了一个完整的企业级金融犯罪管理框架,帮助您预防、检测和管理涉及所有业务线的金融犯罪。该框架将检测、警报管理和案件管理功能与类别专属的工作流、内容管理和先进分析技术结合在一起。该解决方案的完全集成组件提供使隐蔽和高危网络可视化的自上而下和自下而上的功能,提供了增强的欺诈检测、更好的案件管理和更高的运营效率,同时降低总拥有成本。此外:

- 先进、大规模网络分析跨越内部和外部数据源,根据共同属性或微妙的行为模式将客户和账户联系起来。
- 网络可视化界面真实显示网络连接,所以调查员能够揭示隐蔽的关系和开展更高效和有效的调查。
- 先进的剖析引擎根据规则、欺诈分数以及对已知骗子或诈骗网络的联系对个人、账户、产品和网络进行评分。
- 来自多个系统的警报被综合为关于诈骗的真正企业级视野。
- 该解决方案可按照需要定制(例如,您能开发您的机构独有的欺诈模型)

### 好处

SAS 欺诈网络分析解决方案使金融机构能够实现无可比拟的检测率、更准确地识别合规风险和减少欺诈损失。

#### 获得关于欺诈的整体视野

该 SAS 解决方案超越传统的客户视野,提供了关于欺诈活动(包括相关犯罪者)的整体视野,以及对客户行为的非常清晰的了解。这个灵活的解决方案:

- 利用来自多个产品线的所有相关数据源(包括第三方)的数据。
- 解析数据并创建所有实体及其关键关联属性的完整数据模型。
- 能够获取现有的风险分数或危险信号(red flag),并在网络层面提供一个总分。



以一个可疑网络为例,此图显示了SAS欺诈网络分析解决方案可视化界面的下钻功能。

在元数据配置的驱动下,所有记录根据数据内属性的组合完全联系在一起。然后,使用统计学技术,共同实体被识别和压缩,从而产生网络内实体的单一视野。同时还生成数据内的许多离散有界网络,代表统计学上相关的活动和关系组。这个解决方案还:

- 克服与不完美匹配和存在紧密联系的实体有关的数据质量差的问题。
- 能够在数十亿个记录上运行并完全可扩展(实时或批量)。
- 支持网络增量更新(在有新数据增加时)。
- 接受员工数据和审计记录,使检测内鬼或共谋欺诈更容易。

#### 减少假警报的同时识别更多欺诈

银行收到的假警报比例经常高达1%。但SAS解决方案极大地降低了假警报率,这会提高您的整体捕获率和减少解决方案的总成本。为实现这个目标,先进的评分引擎在三个核心范式上使用独立和综合分数:

- 基于评分卡驱动模型和文本分析的申请评分。
- 单个客户及其完整历史的评分。
- 相关网络的评分,包括行为数据(交易模式、网络增长率、活动层面)和其他所提供的数据(当前/以前的地址、联系电话、雇主)。

现有客户账户和实时申请评分的批处理可让您检测和调查现有欺诈及预防新欺诈。一旦网络已被评分并按照严重程度进行了分等,调查员即可开展深入调查和按需要关闭或中止现有信用额度、账户或合约。

#### 使调查员的工作效率提高到原来的两位或三位

SAS 解决方案可显著减少通常与调查有组织欺诈和第一方欺诈有关的工作量,每个转介案件只花费通常调查所需的三分之一到一半时间。

一旦网络被评分和优先化,其即被自动进行警报标记并发送至特侦组。然后调查员即可快速而高效地自动深入检视所生成的网络示意图,以确定是否有账户或交易涉嫌欺诈。

独特的网络可视化、数据下钻功能和其他工具可让调查员:

- 通过点击按钮目睹单个客户、其产品、交易和网络的完整画面。
- 在数分钟而非数小时内探索整个身份、账户和申请网络。
- 进一步下钻至底层数据,以获得完整客户详细信息,包括其他相关客户和网络。

完全基于 Web 的环境可让您:

- 管理潜在欺诈性申请的发送和处理以及特侦组内的主动调查。
- 测量生产力和获得其他信息,以帮助高效和有效地管理特侦组。

#### 预防未来的欺诈

SAS 解决方案帮助您更好地理解新出现的威胁,所以您能采取行动来防止造成重大损失。例如,该解决方案:

- 可自动捕获调查结果并在未来的评分中重复使用这些结果。

- 可对已知的欺诈网络使用自动化的风险评估,以防犯罪分子掩饰其原来的身份和反复开立账户。
- 可自动生成网络示意图,使战略家能够目睹模式和征兆,以便实施控制改进和新监测技术。

#### SAS® 解决方案的独特之处

其他解决方案在针对第一方欺诈的检测、自动化、易用性和投资回报率方面均无法达到 SAS 解决方案的水平,包括以下能力:

- 以高度直观的方式可视化社交网络和揭示先前隐藏的联系和关系。
- 使用先进的数据网络构建和分析技术实现无可比拟的检测率。
- 使用真正的大规模网络分析提供更多可据以采取行动的警报,以保持极低的假警报率。
- 从参数驱动型、基于规则的系统演进到与金额无关的网络及建模方案。
- 执行有监督和无监督的评分,使用预测性分析来发现数据中的异常。
- 通过将多个系统集中进一个环境获得关于欺诈的真正企业级视野。
- 充分利用外部数据源(如欺诈银联数据库)。
- 按需要对解决方案进行定制(如开发您的机构独有的欺诈模型)。
- 通过减少假警报、优先调查得分值高的网络以及提高调查的准确性和效率使调查员平均投资回报率增加 10 倍。