宣传手册

NICE ACTIMIZE

IFM-X

新账户欺诈

更安全的数字化开户

监控、验证和信任

随着数字原住民金融机构颠覆市场，永远改变客户预期，市场形势迅速发生了变化。客户需要数字优先产品带来的即时性与透明度。

遗憾的是，防止犯罪分子利用轻松开户流程并借助合成身份与被盗身份渗透到您的组织机构是一个巨大挑战。

“到 2023 年，预计直接付款授权 (DDA) 申请欺诈金额将接近 10 亿美元。”[1]
— 爱特集团 (Aite Group)

大量数据泄露导致被盗的个人数据随处可见，组织严密、资金充裕的犯罪团伙精心策划新账户欺诈造成的损失加速上升，威胁到数字开户渠道的安全。

身份验证不仅是所有账户开户的核心，也是客户认证与交易过程中持续不可缺少的步骤。简化身份验证与确认并将其与企业欺诈管理联系起来将带来革命性的转变。这将解决数字化开户挑战，促进增长与盈利能力提高。数字化开户流程现代化是实现数字银行业务价值的正确方向。

新账户欺诈是动态的

NICE Actimize 新账户欺诈产品将点解决方案与身份验证 (IDV) 解决方案的功能结合在一起，无需将现有集成或费用高昂的 IT 项目推倒重来，以建立新的集成。新账户欺诈解决方案利用 IFM-X 和 X-Sight 市场平台，专为连接、整合与简化不断发展的点和 IDV 解决方案而设计，同时与组织机构的内部系统无缝集成。该解决方案提供丰富的身份欺诈信号情报以及决策功能。用户利用先进的人工智能与整合数据，全面评估新账户欺诈情况。

新账户欺诈解决方案通过以下方式，多层检测账户发放和新账户阶段的被盗身份或合成身份以及骡子风险：

- 规定并整合身份验证流程，从而对产品与业务线的新客户开户流程予以补充的能力
- 利用身份风险值和身份相关情报并结合行为分析进行早期账户监控，实现高精度的新账户监控和基于风险的动态账户访问
- 运用先进的分析技术，持续监控完整客户生命周期的欺诈风险管理
- 借助强大人工智能提供的大量信息，将申请过程分割成难度与风险相匹配的几部分。

准备好了吗？立即安排演示 >

NICE ACTIMIZE

新账户欺诈解决以下问题：

IFM-X 新账户欺诈：申请欺诈

- 身份欺诈
- 被盗账号
- 骡子账户
- 第一方欺诈

账户欺诈：出于实施犯罪活动之目的开户

- 虚假存款
- 诈骗得手
- 骡子活动
- 身份成熟

通过整个身份验证流程、早期账户监控和持续监控，高精准防范新账户欺诈。

收入增长

难度减小导致放弃率降低，推动新账户采用以及提供更丰富、更快的建议，从而安全提高账户持有人的收入增长。

高效

与单家合作伙伴整合、连接并增强用于 IDV 和欺诈管理的数据与点解决方案生态系统，端到端全面反诈骗。

减少欺诈损失

防止诈骗者渗透以及渗透后在多条产品线实施欺诈计划，以此阻断机构内的欺诈行为。

NICE Actimize IFM-X 新账户欺诈解决方案采用整体全连接的方式，直接解决因被盗身份和合成身份而遭受的直接与间接借记存款账户 (DDA) 欺诈损失。此外，该解决方案还针对出于实施犯罪活动之目的开户行为相关的其他欺诈模式。

新账户欺诈是综合智能欺诈管理的第一步。各组织机构通过将保护措施延伸至申请阶段早期，对新账户进行早期监控，随后无缝移交账户与所有相关数据，持续监控。

1.Fooshée, T. (n.d.).申请欺诈：加速攻击与吸引人的投资机会（2020 年版 11 月卷 Rep.）。Aite Group。

准备好了吗？立即安排演示 >