

IFM-X

新帳戶詐騙

更安全的數位開戶



監控、驗證、信任

數位原生金融機構的橫空出世，讓市場動態急遽改觀，永遠改變了客戶的預期。客戶要的是數位優先產品帶來的即時性與透明度。

可是，防範歹徒伺機對流暢的開戶過程上下其手，利用偽造和竊取的身分滲透到您的機構，是一項浩大的工程。

「2023 年直接付款授權 (DDA) 申請案件的詐騙金額預估上看 10 億美元。」¹
— 艾特集團 (Aite Group)

實力雄厚的犯罪集團，利用從大規模資料外洩事件得手的個人資料，對數位開戶管道的安全性下手，造成的新帳戶詐騙損失日益增加。

身分驗證不僅是所有開戶作業的核心，也是客戶驗證與交易作業過程中不能間斷的需求。精簡身分驗證與確證，並與企業詐騙管理連結，需要進行一場變革，著手因應數位開戶挑戰，而且將會帶來成長與獲利能力。現代化的數位開戶流程，是實現數位銀行價值的指北針。

新帳戶詐騙具動態功能

NICE Actimize「新帳戶詐騙」結合資料點解決方案與身分驗證 (IDV) 的功能，而且不需要重新建構現有的整合，或為新的整合進行昂貴的 IT 專案。「新帳戶詐騙」解決方案利用 IFM-X 和 X-Sight 平台，可連結、協調及簡化日新月異的資料點與 IDV 解決方案，同時流暢地整合組織的內部系統。「新帳戶詐騙」解決方案提供豐富的身分詐騙訊號情報，以及作成決定的功能。使用者運用進階的人工智慧與合作團體資料，獲得對新帳戶詐騙的整體評估。

「新帳戶詐騙」提供一套多層式方法，具備以下在帳戶開立過程與新帳戶階段，偵測身分失竊/偽造與車手風險的能力：

- 定義及協調身分驗證流程，完善跨產品與業務線的新客戶開戶手續
- 使用身分風險分數與身分相關情報，並結合行為分析進行早期開戶監控，實現高準確度的新帳戶監控與動態的風險為本帳戶存取
- 運用進階分析，對完整客戶生命週期的詐騙風險管理，持續進行監控
- 運用大量的資訊，搭配功能強大的人工智慧，為申請案進行風險與鬆緊程度相符的區分。

準備好開始了嗎？立即安排一場示範



「新帳戶詐騙」解決：

IFM-X 新帳戶詐騙：在申請時行騙

- 身份盜竊
- 身分失竊
- 車手帳戶
- 第一方詐騙

帳戶詐騙：為犯罪活動而開戶

- 假存款
- 破產詐欺
- 車手活動
- 身分成熟

藉由身分識別驗證流程、早期帳戶監控及進行中的監控，全程高度精確防範新帳戶詐騙。

收益成長

減少摩擦力，進而降低放棄率，促進新帳戶獲得，並提供更快速、更豐富的提議，穩當地增加帳戶持有人收益成長。

效率與效果兼顧

借助單一合作夥伴，協調、連結及加強您的 IDV 及詐騙管理所用的資料與資料點解決方案生態系，實現整體端對端詐騙預防。

降低詐騙損失

避免詐騙份子滲透，在多個產品線設下騙局，阻止整個機構內的欺詐。

NICE Actimize IFM-X 的「新帳戶詐騙」解決方案，採用綜合且完全連接的方法，直接處理身分失竊與假造身分等形式的直接和間接簽帳存款帳戶 (DDA) 詐騙損失，同時涵蓋與開戶從事犯罪活動有關的其他詐騙手法。

「新帳戶詐騙」是智慧型整合詐騙管理的第一步。組織將防護往前延伸到申請階段，即可對新帳戶實施早期監控，然後在對所有有關資料執行進行中監控的情況下順利交付帳戶。

1. Fooshée, T. (n.d.). 申請詐騙：增長的攻擊與所帶來的投資良機 (2020 ed., Vol. November, Rep.). Aite Group.

準備好開始了嗎？立即安排一場示範

