NICE Actimize

Case Study

Top 40 European FI reduces fraud losses from scams by €5.5 million in one year

The Customer

A top 40 European regional financial institution (FI) with a retail and commercial banking focus.

The Outcome

With this end-to-end fraud prevention strategy fueled by machine learning and AI, the FI's fraud operations teams could react in real time. This new approach created immediate business value:

200%

Increased the value detection rate (VDR) by 200% versus their outdated legacy models.

€5.5m

Reduced fraud loss by €5.5 million over the course of one year.

The Challenge

This FI experienced a significant increase in fraud from social engineering scams brought on by an increase in digital activity, the shifting payments landscape, and criminal sophistication.

Social engineering is one of today's most complex fraud typologies as it often involves a combination of coordinated attacks that are difficult to identify. In parallel, fraudsters exploit faster or instant payments, as they provide quick cash transfers to anyone, anywhere. To thwart controls used to reclaim illicitly obtained funds, fraudsters often leverage mule accounts to further shield themselves.

The sheer prevalence and scale of these scams have drawn regulatory attention at the highest levels. As regulators look to incentivize risk control investments to prevent them, liability laws are trending towards pushing responsibility on FIs.

In this case, social engineering scam tactics evolved so quickly that it strained the FI's ability to fight back. Even with cutting-edge point solutions for fraud, the firm endured significant operational pressures and increased workloads.

The Solution

NICE Actimize provided a layered approach to fraud prevention that gave the FI a comprehensive view of customer risk. By leveraging a powerful combination of data intelligence, machine learning, and artificial intelligence, the bank was able to:

- Identify customers who might be more vulnerable to scams and activate early intervention strategies with proactive customer risk profiling.
- Leverage targeted machine learning models that were trained and optimised to pinpoint specific social engineering scams.
- Reduce false positive rates with transaction-focused modeling including behavioural analytics and mobile device and web intelligence.
- Get earlier identification to address the rise in money mules who open accounts and give access to fraudsters.
- Create purpose-built machine learning models to cover a broad spectrum of fraud typologies.

Contact us today to learn more about how to combat social engineering scams.

Get started now

NICE Actimize