

Modernizing Fraud Prevention to Outsmart Evolving Threats

Fraud and financial crime has become more sophisticated and faster-paced, challenging institutions to keep up. Fraudsters use advanced tactics that exploit vulnerabilities across payment systems, online channels, and customer accounts. Meanwhile, financial institutions face increasing pressure to deliver seamless customer experiences while safeguarding against these evolving threats.

Traditional fraud models often fail to provide immediate protection, requiring months of training and tuning before they become effective. The lack of proactive, industry trained solutions leaves institutions vulnerable to significant financial losses, regulatory penalties, and reputational damage.

Collective intelligence trained models deliver immediate fraud detection, purpose trained typology coverage, and longterm adaptability to evolving threats.

Accelerate Fraud Prevention with Agile Collective Intelligence Models

Fraud doesn't wait, and neither should your protection. NICE Actimize's **Collective Intelligence Models** are pre-trained fraud detection models designed to deliver immediate protection and tangible value from Day 1. Built on the foundation of cross-industry insights and powered by advanced AI, these models are purposebuilt to combat specific fraud typologies, such as payment fraud by type, scams, and account takeovers.

Unlike traditional models, Collective Intelligence Models are ready to deploy as soon as they are implemented. Leveraging anonymized, aggregated data from financial institutions worldwide, these models detect fraud patterns with unparalleled accuracy. Once live, they continually adapt using your institution's data, ensuring ongoing optimization and superior fraud defense.





Day 1 Readiness

Begin detecting fraud immediately upon deployment



Cross-Industry Power

Harness insights from a global network of financial institutions



Continuous Learning

Models refine themselves in real-time to stay ahead of evolving threats



Tailored Protection

Address specific fraud typologies for maximum accuracy



Secure & Compliant

Maintain data privacy with federated machine learning

NICE Actimize Collective Intelligence in Action

Fraud evolves daily, and your defenses must stay ahead. NICE Actimize's Collective Intelligence Models ensure readiness and adaptability through a systematic, secure approach.

Step 1: Industry Training

The models are trained on aggregated, anonymized data from financial institutions worldwide. By leveraging this collective intelligence, they are equipped to recognize even the most complex fraud patterns across multiple channels and typologies.

Step 2: Day 1 Deployment

Unlike traditional models that require months of training, Collective Intelligence Models are ready to protect your institution from Day 1. This ensures immediate value and eliminates delays in safeguarding your assets.

Step 3: Real-Time Optimization

As fraud patterns evolve, so do the models. By learning from your institution's unique data in real time, they continuously improve their performance, reducing false positives and adapting to emerging threats.

Step 4: Secure Intelligence Sharing

Through federated machine learning, the models utilize shared intelligence without compromising sensitive data. This ensures privacy compliance while allowing institutions to benefit from the collective power of the industry.

- Faster deployment and reduced time-to-value
- Enhanced detection capabilities leveraging global intelligence
- Adaptive models that evolve with your business needs

Secure Today, Adapt for Tomorrow

Fraud doesn't wait, and neither should your defenses. NICE Actimize's Collective Intelligence Models provide immediate protection, real-time adaptability, and unmatched insights to keep your institution ahead of evolving threats. Partner with us to safeguard your assets, enhance operational efficiency, and build trust with your customers. The future of fraud prevention starts today—let's secure it together.