NICE · ACTIMIZE

Your Guide to Advanced Fraud Prevention

Fraud has never been faster, more sophisticated, or relentless. Financial services organizations (FSOs) are facing complex challenges and new vulnerabilities as they adapt to an evolving threat landscape and changing customer behaviors.

eBook

NICE · ACTIMIZE

Shifting Behaviors Create New Opportunities for Fraud

Finance is a data-rich industry, making it an ideal domain for the strategic application of AI and machine learning (ML) in fraud prevention.

As the financial services industry experiences accelerated digitalization, acute disruption and an intensifying threat landscape, FSOs are positioned to deploy AI and machine learning to capitalize on the potential benefits of autonomous intelligence and strengthen fraud prevention strategies.

Evidence indicates that consumers will continuously shift to digital.[1]

Fraudsters are looking to profit from this escalating online activity and weaknesses in existing fraud prevention systems. FSOs must emulate this mindset and act now to improve their technologies and digital services, and continuously address diversifying, complex, well-orchestrated fraud schemes.

Physical bank branches are being rapidly replaced by digital banking channels, and 85 percent of consumers who have used digital platforms for financial services will continue to favor this form of interaction post-pandemic.[1]

Radical Transformation for Fraud

NICE · ACTIMIZE

The fraud culture, which encompasses a surge in fraud losses related to peer-to-peer (P2P) payments, digital wallets, phishing, authorized push payment (APP) fraud, friendly-fraud, and the gamut of identity fraud scams, has created surmounting vulnerability for FSOs.

Executing an effective fraud strategy that coincides with diverse business and digital transformation agendas while maintaining high quality, seamless digital experiences is a multifaceted challenge:

- Robust fraud prevention must not come at the expense of the customer experience (CX).
- Lack of real-time data insights makes it difficult to quickly detect and respond to fraud.
- Historical views toward fraud slow down time-to-insights and resolution and ultimately lead to more substantial fraud losses.
- Relying solely on human analysts can result in increased false positive rates, an excess of false declines, and frustrating CXs.

Identity fraud scams comprised **$43 billion** of the **$65 billion** total combined fraud losses in 2020.[2]

Challenges with Implementing AI Solutions

- Employees may have to adapt to evolving ways of working, and collaborating with new technologies.
- Developing and implementing AI solutions can be a substantial financial investment.
- Data collection, processing and storage architectures must have the agility and capacity to support fluctuating computing requirements and large amounts of diverse data sources and types.
- Poor quality data can impact compliance and lead to skewed, biased or untrustworthy AI outcomes.
- AI systems need to scale alongside data growth and intricacy, and seamlessly integrate and validate new data sources and types.

NICE · ACTIMIZE

Only 53%

of organizations have transitioned their AI POCs into production over the past two years.[6]

The Value of AI in Fraud Prevention

FSOs are accelerating adoption of AI-powered systems, with over $217 billion spent on AI applications for use cases such as fraud prevention. [3]

- Augmenting human-centric investigations with advanced AI-powered autonomous intelligence to boost efficiency, accuracy and shift human focus to more specialized, value-driven tasks and knowledge work.
- Addressing weak points in their fraud prevention efforts and strategies, and orchestrate a multi-dimensional, multi-layered approach to fraud management.
- Coordinating advanced, non-intrusive, omni-channel authentication methods in every channel with a unified approach to fraud and authentication management that provides improved fraud detection rates and cross-channel attack identification.

NICE · ACTIMIZE

80%

of fraud prevention specialists attribute AI to lowering payments fraud

63.3%

of FSOs credit AI with being a valuable tool in stopping fraud [6]

Advanced AI and ML in Fraud Prevention

NICE · ACTIMIZE

FSOs must eschew rules-based fraud detection and predictive models in favor of next-generation AI and ML built upon highly-developed crime indicators, fraud behaviors and holistic data repositories.

Unsupervised learning: Capable of detecting anomalies in behavior, even with limited transaction data. Unsupervised learning can analyze new data and self-update by identifying patterns to conclude if they represent legitimate or fraudulent transactions.

Supervised learning: Relies on labeled data sets of transactions appropriately tagged as either fraud or non-fraud. Pertinent, quality, voluminous training data contributes to both model accuracy and learning patterns that correlate to legitimate transaction behaviors.

Federated learning: Distributed ML process that addresses decentralized data across siloed applications, cloud environments and data centers. Combined with cross-entity data, it helps FSOs address emerging fraud trends and threats, and gain a single, holistic view of customer intelligence.

NICE · ACTIMIZE

IFM-X

AI and ML technologies streamline the approach to fraud management and resolve the limitations of traditional, rules-based fraud prevention systems and manual-intensive processes.

NICE Actimize's integrated fraud management platform, IFM-X, is an agile, autonomous, end-to-end fraud prevention solution that helps FSOs deploy holistic approaches to fighting fraud in a dynamic fraud environment:

- Enable accurate identity evaluations, detect abnormal transaction behaviors and administer continuous fraud prevention across every stage of customer lifecycle fraud management.
- Reduce false positives, accelerate investigation time and enhance decision-making via AI-powered scoring and authentication.
- Make smarter, accurate, faster decisions with entity-driven investigations and visual analytics.
- Deploy AI capabilities that incorporate changing behaviors, emerging trends and anomalies to generate actionable insights regarding customer risk.
- Leverage automated decisioning for real-time transaction approval or rejection to facilitate proactive approaches to fraud prevention.
- Mitigate fraud loss by preventing fraudsters from penetrating the organization and perpetrating fraud across numerous lines of products.

The Always on AI Approach to Fraud Prevention

IFM-X is powered by Always on AI, which uses industry and behavioral intelligence to continuously learn, discover and adapt to rapidly detect divergent activity and prevent fraud attacks.

NICE · ACTIMIZE

NICE Actimize monitors and protects like no other organization.

Monitors
4+ billion
transactions per day

Trusted by
750+
global organizations

Protects
~$6 trillion
each day

Always on AI can support:

- Optimize data acquisition, processing and operationalization with **X-Sight DataIQ, X-Sight Marketplace** and **X-Sight Connect**.
- Leverage consortium intelligence to catch more fraud with **Fraud Insights** and **Cross-FI Entity Risk Score API**.
- Safeguard any payment type via an omni-channel approach to monitoring the entire payment cycle with **Payment Fraud**.
- Deploy intelligence curated from infrastructures used by fraudsters with **Dark Web Intelligence**.
- Orchestrate omni-channel authentication for real-time risk decisioning with **Authentication Management**.
- Find fraudulent employee activity across multiple enterprise lines with **Employee Fraud**.
- Detect fraud from stolen and synthetic IDs and mule risks via **New Account Fraud**.

Realize the Full Potential of Fraud Prevention

In the future, AI and ML are likely to become increasingly dominant in finance alongside the growth of cryptocurrencies, pervasive automation and digital transformation. AI advancement helps FSOs use autonomous intelligence to eliminate fragmented approaches to fraud prevention and transform their fraud operations to efficiently, holistically and proactively mitigate fraud.

Learn more here

NICE ACTIMIZE

1 McCaffrey, O. (2020, June 7) People Aren't Visiting Branches. Banks Are Wondering How Many They Actually Need. The Wall Street Journal https://www.wsj.com/articles/people-arent-visiting-branches-banks-are-wondering-how-many-they-actually-need-11591531200

2 Hershman, E. (2021, March 23) Total Identity Fraud Losses Soar to $56 Billion in 2020. Businesswire. https://www.businesswire.com/news/home/20210323005370/en/Total-Identity-Fraud-Losses-Soar-to-56-Billion-in-2020

3 Digalaki, E. (2021, January 13) The impact of artificial intelligence in the banking sector & how AI is being used in 2021. Business Insider. https://www.businessinsider.com/ai-in-banking-report

4 (2021, June) AI In Focus: The Bank Technology Roadmap. PYMNTS.com. https://www.pymnts.com/artificial-intelligence-study/

5 McCormick, J. (2020, August 7) AI Project Failure Rates Near 50%, But It Doesn't Have to Be That Way, Say Experts. The Wall Street Journal. https://www.wsj.com/articles/ai-project-failure-rates-near-50-but-it-doesnt-have-to-be-that-way-say-experts-11596810601

6 Shilling, M. Celner, A. (2020, December 3) 2021 banking and capital markets outlook. Deloitte. https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-outlooks/banking-industry-outlook.html

About NICE Actimize

NICE Actimize is the largest and broadest provider of financial crime, risk and compliance solutions for regional and global financial institutions, as well as government regulators. Consistently ranked as number one in the space, NICE Actimize experts apply innovative technology to protect institutions and safeguard consumers and investors assets by identifying financial crime, preventing fraud and providing regulatory compliance. The company provides real-time, cross-channel fraud prevention, anti-money laundering detection, and trading surveillance solutions that address such concerns as payment fraud, cybercrime, sanctions monitoring, market abuse, customer due diligence and insider trading.

www.niceactimize.com