NICE Actimize

Insights Article

Fighting Financial Crime with Generative AI

Generative AI has the power to disrupt the financial crime and compliance field, but firms face a double-edged sword when considering implementing generative AI solutions. Generative AI can provide substantial economic and productivity benefits, easing workloads, adding labor efficiencies and reducing manual touchpoints. Conversely, bad actors are using the technology to increase the sophistication of their malicious attacks. Opportunities and challenges abound, setting high expectations for cutting-edge generative AI solutions.

As the leader in financial crime solutions, NICE Actimize has long been at the forefront in delivering solutions that optimize AI for fraud detection, anti-money laundering and trading surveillance. Our experience and knowledge give us insight into the opportunities and challenges of using emerging technologies.

When incorporating Generative AI in financial crime solutions, financial institutions (FIs) must carefully consider the opportunities and challenges the technology can provide, such as:

Identify the Problem, Not the Technology. Business challenges should be analyzed to identify the optimal solution. The disruptive power of generative AI has the capability to transform financial crime program efficiencies, however, it's not the solution to every challenge.

Privacy is Paramount. Cloud-based AI offerings raise privacy and data security concerns given the extensive data large language models (LLM) require for training—and the use of generative AI can magnify those risks by unintentionally recreating or sharing personal client details. When building a solution that involves a large language model, a multilayered security protocol should be established, one where all data and PII is encrypted to ensure protection.

Don’t Underestimate Diversity. The information used to train a LLM will substantially impact the model’s performance. A lack of diverse data can produce incomplete and possibly biased outcomes. Metrics can only be gauged with proper testing. A comprehensive generative AI solution should include testing across geographies and jurisdictions to protect against biased and unintended outcomes.

Lack of Contextual Understanding. The speed and tone of responses from generative AI models can be wrongly mistaken for accuracy. But as evidenced by many high-profile “generative AI gone wrong” cases around the world, well-intentioned applications can produce unintended results. The potential for financial and reputational damage can pose a real threat to an enterprise, and model limitations need to be assessed to ensure accuracy.

Keeping a “Human in the Loop.” By blending the traditional approaches of AI-behavior analysis, pattern detection with cognitive capabilities, generative AI can provide enhanced intelligence and insights to the investigation process. But human oversight is still essential in critical decision-making processes to provide direction and outcomes. A thoughtful generative AI solution will incorporate meaningful human interaction, providing an investigator with suggestions and recommendations. It should streamline their workload, make them more efficient, and prioritize their time in a risk-based manner.

A Continuous Effort to Monitor and Improve. Generative AI models learn patterns based on prompts, data and past interactions, which can all lead to changes in the performance of the model. The evolutionary nature of these models requires a need to assess and retest, establishing before and after metrics, necessary for internal governance and external regulatory reporting. Only through analysis of the AI outputs can we effectively understand how well the solution is performing.

NICE Actimize is A Trusted Partner

Generative AI solutions have the capacity to transform the financial crime and compliance landscape. But the earliest creators don't always have the best outcomes. Without the proper training, design and testing, these solutions can provide biased, incomplete, or inaccurate outcomes. As with any emerging technology, a thoughtful and responsible approach with a trusted partner who has a deep understanding of AI and experience developing financial crime solutions is necessary.

Given the potential for economic and reputational damage, the stakes of getting generative AI wrong are high. FIs should choose partners that can help mitigate risks.

As the industry leader in financial compliance solutions and a pioneer in the use of Artificial Intelligence and Machine Learning, NICE Actimize helps firms optimize solutions that balance innovation with risk, empowering clients to comply with confidence. We have the largest footprint in the industry, and our solutions are designed with careful implementation, providing clients with the best value proposition. Schedule a demo of our latest Generative AI Solutions.

→ Request a demo

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