Infosys topaz

WHITE PAPER

LEVERAGING AI TO COMBAT FINANCIAL CRIME

Infosys®
Navigate your next

Executive summary

From money laundering to terrorist financing, fraud to cybercrime, financial criminals constantly develop new techniques and typologies to commit offences. This threat has multiplied with the emergence of technologies that act as double-edged swords.

This paper outlines real-world AI use cases for preventing anti-money laundering, fraud management, and surveillance, including scenarios where criminals can leverage AI for deepfakes, automated attacks, and enhanced social engineering. It also explores how leading-edge AI platforms allow banks to proactively prevent financial crimes while addressing the growing challenge of AI-enabled criminal activities. By applying machine learning, natural language processing, and predictive modeling to vast datasets, banks can uncover hidden patterns and create robust countermeasures like advanced authentication, AI-powered defensive systems, and enhanced due diligence.spanning from the initial use of Gantt Charts through the introduction of the Agile Manifesto in recent years, technology has been an important medium in implementing changing approaches to managing projects.

Rising impact of financial crime on banks

Financial crime causes billions in annual losses through direct theft, reputation damage, regulatory fines, and eroded customer trust. As financial institutions deploy AI defenses, criminals weaponize the same technologies, creating an evolving technological arms race across multiple fronts.

Identity manipulation is a primary threat, with criminals leveraging deepfake technology to create synthetic faces, voices, and documents. These sophisticated tools generate false credentials at scale and enable the manipulation of digital evidence, fundamentally compromising traditional verification methods.

Automated attack systems have grown increasingly sophisticated, with adaptive botnets that evade detection while systematically testing stolen credentials. These systems employ machine learning to optimize the success rates of cyber attacks, while AI models analyze public data to identify and target the vulnerable with precision.

AI has also revolutionized social engineering, enabling criminals to craft highly persuasive phishing campaigns using natural language processing. Automated chatbots now conduct fraudulent conversations at scale, while advanced analytics of social media profiles enable attacks tailored to each victim's circumstances and vulnerabilities.

The promise of AI-driven solutions

Financial institutions are increasingly fighting AI with AI in their defensive strategies. Specialized defensive AI systems are being trained to detect AI-generated content, from fraudulent documents to synthetic video and audio. Adversarial machine learning techniques are employed to identify and counteract malicious AI models, while real-time adaptation capabilities allow defensive systems to recognize and respond to emerging AI-powered attack patterns as they evolve.

Enhanced due diligence has become essential in the age of AI-enabled crime. The adoption of zero-trust architecture principles ensures that authentication is not a one-time event but a continuous process, with AI systems constantly verifying the legitimacy of user actions. Financial institutions are also deploying AI-powered background check systems that can verify customer authenticity with thoroughness. Advanced network analysis techniques are used to uncover rings of synthetic identities that might otherwise appear unrelated. Continuous monitoring systems, powered by AI, can detect sudden changes in customer behavior indicating account takeover or other forms of fraud.

Institutions are also implementing multimodal biometric verification systems specifically designed to resist deepfake attacks. These systems are complemented by advanced behavioral analytics that continuously monitor user actions to detect anomalous patterns indicating an AI-powered attack.

A deep dive into AI use cases for preventing financial crime

Leading AI platforms leverage techniques like machine learning and natural language processing to analyze massive volumes of customer, transactional, and communications data. This helps in identifying subtle anomalies, predictive patterns, and hidden relationships indicative of criminal activity. Banks can proactively uncover this critical intelligence and intervene before major losses occur. Rather than just reacting to crimes already committed, AI enables institutions to get ahead of financial criminals and prevent their activities from succeeding in the first place.

Anti-money laundering

AI techniques revolutionize AML prevention through comprehensive analyses of transactional datasets, customer information, and communications. Advanced machine learning models uncover sophisticated money laundering patterns by detecting suspicious transactions, unusual fund placements, and complex layering strategies. Natural language processing examines customer communications to identify anomalies indicative of laundering risks, while relationship mapping algorithms trace fund flows through seemingly unrelated third parties. These AI-powered solutions, incorporating pre-built AML accelerators and customizable models, significantly outperform traditional rules-based approaches in accuracy and efficiency.

Fraud detection

AI platforms enable sophisticated fraud prevention by analyzing multiple data streams simultaneously. During customer onboarding, predictive analytics identifies high-risk indicators of application fraud. Continuous transaction monitoring employs anomaly detection to flag potential credit card and check fraud, and account takeovers in real-time. As criminals evolve their techniques, these

systems adapt to recognize new fraudulent behaviors while monitoring internal transactions to detect potential insider threats. This comprehensive approach delivers superior detection rates with fewer false positives than legacy systems.

Trade surveillance

AI enhances market oversight through real-time monitoring of trading activities across diverse markets, asset classes, and geographical regions. Advanced algorithms detect potential market manipulation and abusive trading strategies by analyzing complex patterns across multiple dimensions. These systems integrate news and social media analysis to identify potential insider trading activities before major market announcements. This holistic approach enables financial institutions to maintain comprehensive trading surveillance while adapting to rapidly changing market conditions and emerging manipulation techniques.

There are a myriad of other use cases emerging as AI capabilities mature, like improving cybersecurity through recognizing attack patterns, automating customer risk scoring for Know Your Customer checks, analyzing third-party risks in correspondent banking, uncovering hidden beneficial ownership in networks, and more. Cutting-edge techniques like graph and voice analytics will further expand the horizons of AI in financial crime prevention.

Guardrails for responsible AI implementation

Data privacy and explainable AI

Financial institutions must navigate strict regulatory frameworks like GDPR and the EU AI Act when implementing AI solutions, particularly regarding customer data usage limitations. To address these constraints while maintaining effectiveness, technology providers incorporate explainable AI capabilities that make algorithmic decision-making transparent. This transparency enables bank experts to validate the reasoning behind AI alerts and understand prediction context, transforming AI from an opaque 'black box' into an accountable tool that builds trust while remaining actionable.

Monitoring for unfair bias

Preventing algorithmic bias requires rigorous testing before deployment and continuous monitoring during operation. Financial institutions must proactively identify and address any model fairness issues or skewed outcomes through comprehensive pre-deployment testing protocols. Post-deployment monitoring ensures rapid detection and correction of emerging bias, with model enhancement procedures ready to implement necessary fixes. This ongoing vigilance maintains the integrity and fairness of AI systems throughout their operational lifecycle.

Change management considerations

Successful AI adoption demands strong executive sponsorship paired with comprehensive employee training across organizational levels. From fraud teams to front-line staff, employees need foundational AI knowledge to understand the capabilities and limitations of these systems. Cross-functional collaboration ensures AI solutions address practical operational needs while breaking down traditional organizational silos. This holistic approach to change management creates an innovation-friendly culture that supports effective technology adoption and utilization.

Best practices of AI development

Quick wins and high-value focus areas first

Institutions should pursue targeted deployment focused on high-impact AI use cases first based on their risk priorities and pain points. Whether for AML, fraud, or surveillance, the roadmap should deliver quick wins in domains with the clearest business case and ROI. Starting with proofs of concept and pilots focused on the highest payoff areas minimizes risk while demonstrating benefits for further buy-in.

Integration with core banking systems

Successful AI implementation requires seamless integration with existing payment infrastructure, customer databases, and data warehouses to access the substantial data volumes needed for accurate algorithmic processing. Modernization can solve integration challenges present in legacy systems, while cloud migration can enhance agility and scalability for AI applications. A robust data ingestion and API infrastructure provides the foundation for long-term flexibility when use cases expand beyond initial implementations.

Transitioning from rules-based systems

Financial institutions can manage the transition from legacy systems through an incremental approach, beginning with retraining existing models using advanced AI techniques. Modern AI solutions can be introduced for specific processes initially, allowing for measured evaluation and optimization. As benefits are demonstrated and enhanced through continuous feedback loops, institutions can confidently proceed with the broader replacement of legacy systems, minimizing operational risks during the transition.

Expanding over time

As AI capabilities mature, the deployment scope can progressively expand across the enterprise. This growth is supported by continuous model enhancement, strategic partnerships for additional data access, and the adoption of emerging technologies like graph databases and quantum computing. This measured expansion approach ensures each phase of AI implementation builds upon previous successes while incorporating new innovations, achieving comprehensive coverage across all aspects of financial crime prevention.

Measuring success in the world of AI

Key risk KPIs to track

Institutions must track progress through relevant risk Key Performance Indicators. Reduced false positives, faster alerts, higher detection rates, and lower losses are key metrics to quantify AI impact. Customer satisfaction scores also indicate

where AI customer service applications like chatbots increase value. Ongoing model iterations further optimize these metrics over time.

Business value impact

The measurement strategy should tie back to overall business value. Institutions need to track direct cost reductions such as fraud losses avoided, fines prevented, and operational efficiencies achieved. Maintaining customer trust and loyalty through AI is also a key success factor. The ROI should be demonstrated through concrete bottom-line impact.

Course correcting based on results

Ongoing monitoring of model performance and user feedback is needed to course-correct and enhance the solutions. Any incorrect predictions, ineffective models, or integration issues discovered after deployment can be promptly addressed through rapid iteration. Weekly model evaluation cycles and user input into enhancement backlogs will facilitate continuous improvement.

AI focus areas for maximum impact

Regulatory considerations

The rise of AI-enabled financial crime has necessitated the evolution of regulatory frameworks to address new challenges. Regulators are increasingly requiring financial institutions to conduct AI-specific risk assessments that consider the defensive and potential offensive uses of AI technologies. New guidelines for the detection and reporting of AI-enabled fraud will require institutions to adapt compliance processes accordingly. There is also a growing emphasis on standards for AI model transparency and auditability, ensuring that both defensive and potentially harmful AI applications can be examined and understood by regulatory authorities.

Collaborative defence

The fight against AI-enabled financial crime cannot be won by individual institutions acting alone. Information-sharing networks are crucial, allowing banks to rapidly disseminate threat intelligence about new AI-powered attack methods. Joint AI research initiatives between banks and security firms are accelerating the development of more effective countermeasures. Emerging public-private partnerships enable coordinated responses to AI threats that leverage the resources and capabilities of both sectors.

Proactive approach to implementation

Financial institutions must fundamentally redesign their AI implementation strategies to address emerging threats. This begins with comprehensive threat modeling that anticipates AI-enabled criminal activities, ensuring defensive systems are architected with these sophisticated attacks in mind.

Adversarial resilience must be embedded as a core principle in AI system design, with defensive mechanisms specifically engineered to identify and counter attempts at manipulation or deception. These systems require regular retraining cycles to maintain effectiveness against evolving AI-powered schemes.

Critical to this approach is the implementation of robust ethical constraints throughout the AI architecture. These safeguards ensure that defensive systems, while powerful, cannot be repurposed for harmful activities. This balanced approach enables financial institutions to aggressively combat crime while maintaining strict control over their AI capabilities, preventing the inadvertent creation of new vulnerabilities through defensive systems themselves.

Unlocking AI's transformative potential is a step into the future

Leading AI solutions provide tremendous opportunities for banks to tackle the persistent threat of financial crime with greater sophistication. These technologies have the potential to be truly transformative in reducing the massive global cost of financial crime over the next decade. AI represents a paradigm shift in financial crime prevention. However, to fully realize benefits, institutions need to ensure privacy, ethics, and organizational change considerations are addressed upfront. This includes oversight protocols, transparency mechanisms, training programs, and more. With prudent implementation, AI can be a game changer for managing evolving financial crime risk.

Suki Barn, Data & Analytics, Industry Principal, UK & EMEA

Author

Sukhdeep Singh Barn, Infosys

Infosys Topaz is an AI-first set of services, solutions and platforms using generative AI technologies. It amplifies the potential of humans, enterprises and communities to create value. With 12,000+ AI use cases, 150+ pre-trained AI models, 10+ AI platforms steered by AI-first specialists and data strategists, and a 'responsible by design' approach, Infosys Topaz helps enterprises accelerate growth, unlock efficiencies at scale and build connected ecosystems.

For more information, contact askus@infosys.com

Infosys® Navigate your next