



## STOPPING FRAUD BEFORE IT HAPPENS: AI'S ROLE IN BANKING RISK MANAGEMENT

### Abstract

NYC, 3 am. While most of the city sleeps, agentic AI 'soldiers' of the city's banks are prowling the financial networks, monitoring transactions flowing in and out of the system. A sharp spike in a customer's credit card charges from Venezuela is handled within seconds: the customer had made an ATM withdrawal in NYC just hours ago, so the agent decides based on its rules engine, that the customer could not be making high-value charges in South America and declines them. The agent freezes the customer's card immediately and notifies her to contact the bank in the morning to verify, or validate the rejection of, the charges.

Every business today is a digital business. Armed with digital identity cards, credit cards, and payment systems, every person is also a digital entity unto themselves. It goes without saying that the financial institutions that support business and people — namely, banks — have now acquired an almost completely digital DNA.

Risk management is a distinct focus in the banking industry: from credit card risk to

market risk, operational risk and more, banking leaders must maintain a constant state of vigilance to monitor, assess, and mitigate risks of all shapes and sizes.

Risk can threaten the financial stability, reputation or compliances for banks, any of which can be catastrophic.

Risk management in banking has been evolving by the day due to the sharp rise in digital transactions globally. More and more complex forms of fraud are hitting

the ecosystem daily, such as threats built using advanced technologies like Artificial Intelligence (AI). Whether with ecommerce fraud solutions, web and social media analytics services, financial data and analytics protection, or fraud solutions in the Business Process Outsourcing (BPO) industry, **fraud management** in banking is now as complex and technology-oriented a subject as is possible in the banking industry.

## Fighting fire with fire

Banking industry technologists have deployed a number of AI-driven solutions for risk management.

When it comes to **advanced fraud detection**, AI systems routinely analyze transaction data and user behavior — by studying behavioural analytics and

biometrics such as login patterns or mobile device usage — to spot anomalies and to identify fraudulent activities far faster and more accurately than manual audits. This can often happen even before the fraud occurs, and fail-safes ensure the fraudster is stopped instantly. Bankers

rely on real-time and big data analytics here: AI platforms consume and analyze large datasets instantly for anomalies and emerging risks. This also supports continuous, proactive monitoring for ripples across the system.



**Automation of compliance** is another key area that banking CTOs have focused on. AI RegTech tools regularly scan communications and documents moving through the system for regulatory breaches, compliance checks or inconsistencies. The automated scanning frees up human audit teams to focus on higher-risk areas and sample checking. As

Banks now use **enhanced risk profiling** for all new applications. Here, machine learning (ML) models are trained on large

global standards are frequently updated, AI tools are better at this kind of checking. For instance, Oleg, a banker in Budapest has to evaluate the week's 58 new loan applications. He uses the bank's AI-driven risk profiling system to prioritize the applications and derive a risk score based on the bank's criteria. He notices that one application — a small business loan to

datasets to predict the creditworthiness of customers and to flag systemic risks. This leads to better risk segmentation

start a new kindergarten — is flagged 'high risk' as the applicant has been without a job for four months. But he digs into the AI system's conversation interface to understand more about the applicant: a Master's Degree holder in Psychology and Child Development. He overrides the system recommendation and approves the application.

and reduced default rates on loans, while giving enough information for human teams to make data-driven decisions.

AI has also been put in place to speed up processes such as loan application reviews, claims validation, and vendor checks, **improving operational efficiency** numbers in manifold ways. This enables

bank personnel to make quicker, data-driven decisions while still improving risk controls for the overall organization. Of note is the use of a mature technology such as Robotic Process Automation (RPA)

to automate repetitive but critical tasks like data entry, audit trails, and regulatory filings. All of these reduce the risk of human errors creeping into the workflows.



With the increasing reliance on AI, there's a heightened focus on building transparent, auditable, and explainable AI models for the industry. Banks are working actively to ensure that models can be regularly audited and they meet all the regulatory expectations for bias and fairness. AI ethics and explainability are turning out to be core concepts for banking risk managers.

## At the bleeding edge of evolving risk

The risks are evolving too: Research firm Gartner highlights that globally, banks are changing their audit frameworks and increasingly relying on AI-powered sample testing and validation, as **AI-driven synthetic data** makes traditional documentary evidence less trustworthy.



Here are some ways the industry is leveraging bleeding-edge AI technology:

### Agentic AI and autonomous agents

Banks have started to leverage specialized agentic AI-based solutions for risk assessment, fraud detection, compliance monitoring, predictive and **descriptive analytics**, and incident response. These autonomous software entities automate risk evaluation, proactively spotting threats, and orchestrating immediate responses to anomalies by making independent decisions.

### Machine learning (ML) for predictive risk modeling

Banks are using ML and deep learning to forecast risks, analyze transactional and behavioral data, and to predict defaults or market shifts in real time. This nuanced approach allows for a more granular, personalized assessment of creditworthiness and risk segmentation.

### Natural Language Processing (NLP) and Intelligent Document Processing (IDP)

NLP and IDP technologies help banks process vast amounts of unstructured data from regulatory texts, contracts, and communications, and to automatically detect compliance issues; or to match the text against evolving regulatory requirements. Such technologies can be invaluable in compliance matters, helping human teams speedily wade through many documents and make necessary decisions.

## Here's another case study



It's been a long day at the office for Senior Risk Manager Natasha in the Philippines. She's about to log off when she notices a flag from the AI risk manager — an email that has been sent to all the bank's employees. It's a phishing mail, as evidenced by multiple 'tells' in the body, with suspicious links. The system has quarantined the email and recommends deletion. Natasha sends the email across to the cybersecurity team and deletes it from the incoming message queue. She shuts her laptop and heads home. Risk management for the day, done right!

Banks are staying on their toes as they transform. Leading consultants and industry analysts universally point towards a trend of leveraging AI in fraud analytics, process automation, regulatory surveillance, and adaptive risk management as central themes.

## How Infosys can help

Infosys BPM offers a comprehensive range of [solutions and services for fraud management](#) to the financial services industry. These include fraud alerting models, fraud loss assessment tools, unknown pattern identification, case visualization, and data platform integration. Infosys BPM brings in deep domain, data science, data, and visualisation skills to develop and deploy analytics solutions tailored to drive better business outcomes for banking and financial services organizations.

For more information, contact [infosysbpm@infosys.com](mailto:infosysbpm@infosys.com)

**Infosys**<sup>®</sup>  
Navigate your next

© 2025 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.