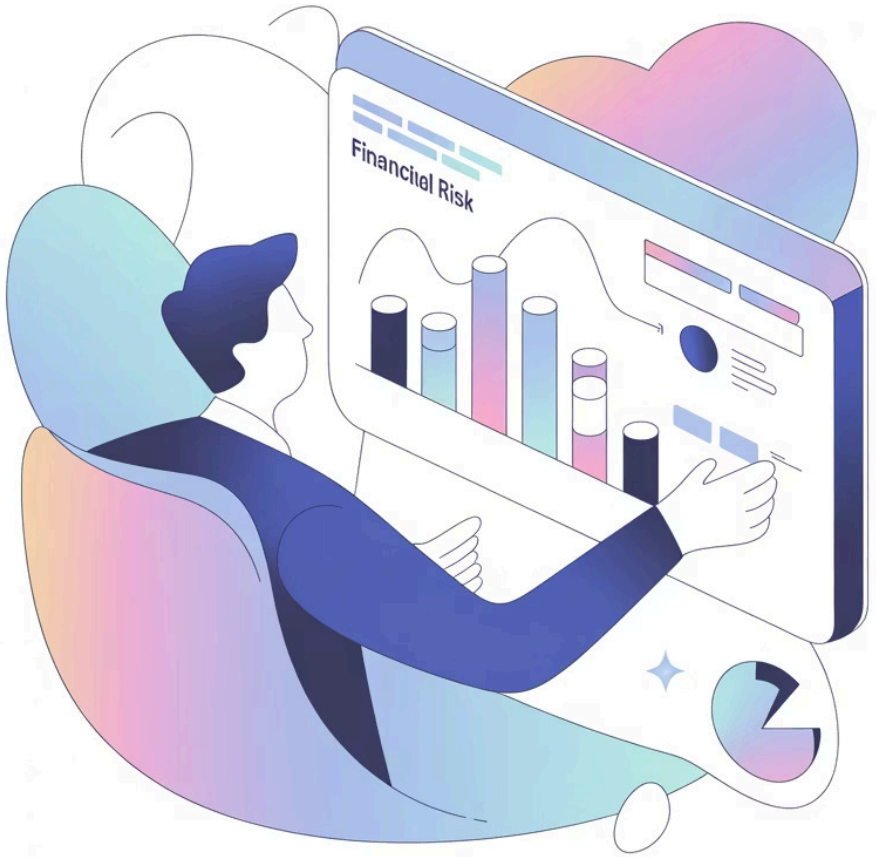
AI-Driven Fraud Detection: Executive Overview

- Developed an AI-based fraud detection model to **identify fraudulent transactions early**
- Achieves **high fraud detection accuracy while minimising false alarms**
- Designed to support **risk management, operations, and compliance teams**
- Delivers **stronger fraud prevention at lower operational cost**



Why Fraud Detection Matters

The Financial Impact

Fraud causes direct financial losses that erode margins and damage brand reputation. But the problem extends beyond stolen funds.

Over-flagging legitimate transactions creates a secondary crisis: frustrated customers abandon purchases, while manual review teams drown in false positives—driving up operational costs.

The Core Challenge

Organizations need to catch fraud without harming the customer experience. This requires walking a tightrope between security and convenience.

The solution demands a data-driven, explainable decision system that can adapt to evolving fraud patterns while maintaining trust with legitimate users.

Proposed AI Solution

01

Risk Scoring

AI model assigns a fraud risk score to each transaction in real-time, leveraging advanced machine learning algorithms trained on historical patterns.

02

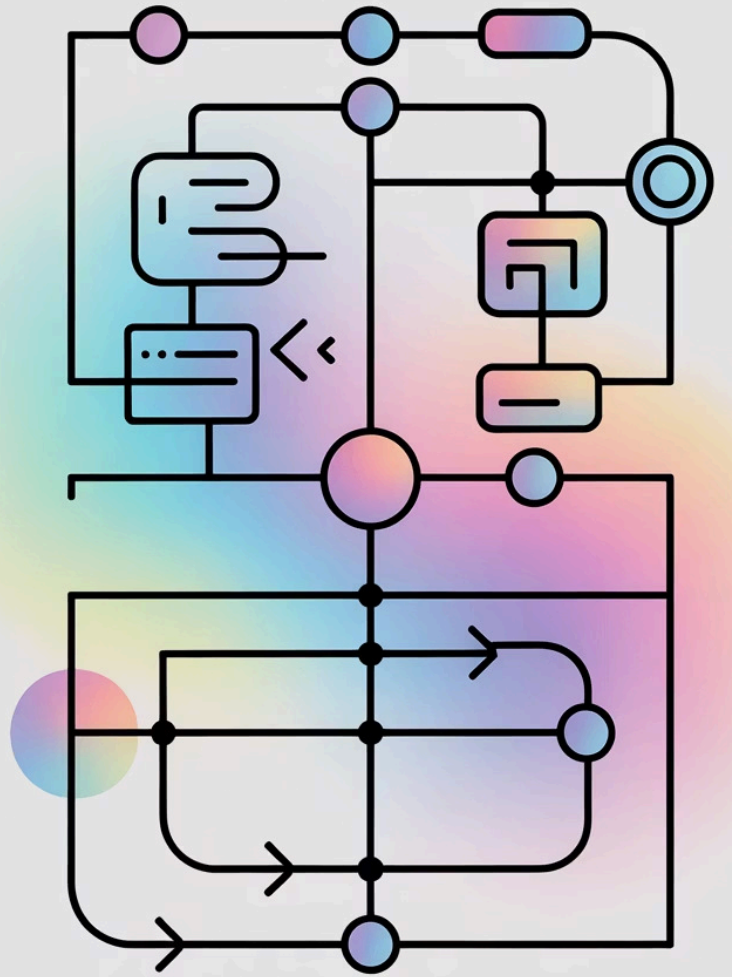
Automated Routing

High-risk transactions are automatically blocked or queued for expert review, while low-risk transactions receive instant approval.

03

Flexible Controls

System is scalable, fully auditable, and adjustable via configurable thresholds that align with your risk appetite.



How Well the Model Performs

84%

Fraud Detection Rate

Successfully catches 84% of all fraud cases, providing robust protection against financial losses.

91%

Precision Score

When the model flags a transaction, there's a 91% probability it's genuinely fraudulent—minimizing wasted effort.

<5%

False Alarm Rate

Extremely low false positives mean very few legitimate customers are inconvenienced by unnecessary blocks.

Validated Performance: These metrics are based on rigorous testing with unseen data, ensuring the model performs reliably in real-world conditions. The model is accurate where it matters and cautious where it should be.

Balancing Fraud Prevention vs Customer Experience

The Threshold Decision

AI outputs probabilities, not binary yes/no decisions. The decision threshold has been carefully tuned to maximize fraud capture while minimizing false positives.

Our selected operating point delivers high fraud protection with low customer friction—but remains flexible.

Current Configuration

Optimized for aggressive fraud detection while maintaining smooth customer experience for legitimate transactions.

Adjustable Anytime

Thresholds can be recalibrated based on evolving risk appetite, seasonal patterns, or regulatory requirements.

Expected Business Value

Reduced Fraud Losses

Early detection prevents fraudulent transactions from completing, directly protecting revenue and reducing chargebacks.

Lower Manual Review Workload

Automation handles the majority of decisions, freeing analysts to focus on complex, high-value cases requiring human judgment.

Fewer Customer Complaints

Precise targeting means fewer false declines, leading to improved customer satisfaction and reduced support tickets.

Efficient Scalability

System scales seamlessly as transaction volume grows, without proportional increases in operational team size.

> "More fraud stopped, fewer customers affected, same operational team size."

Transparency, Risk & Governance

Explainable Decisions

Model decisions are fully explainable—not a black box. Each flagged transaction can be justified with clear reasoning based on specific risk indicators.

This transparency is essential for building trust with stakeholders and maintaining accountability across the organization.

Audit Support

Complete audit trails document every decision, supporting internal reviews and external examinations.

Regulatory Review

Meets requirements for explainability and documentation in regulated industries.

Internal Governance

Aligns with risk management frameworks and corporate governance standards.

Importantly, this system is designed to complement human decision-making, not replace it. Expert judgment remains central to handling edge cases and evolving the fraud strategy.

Bias & Fairness Safeguards

No Personal Attributes

The model excludes sensitive personal attributes such as gender, age, race, or location to prevent discriminatory outcomes.

Proxy Variable Audits

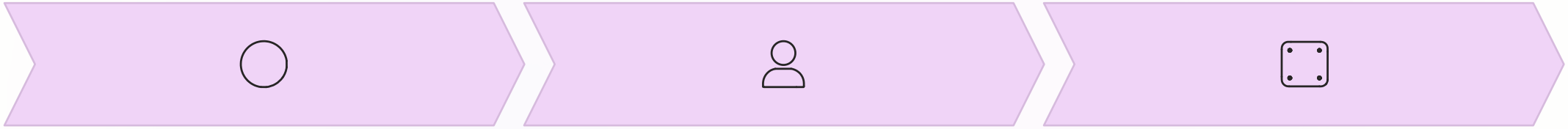
We've conducted thorough audits on proxy variables including transaction size, time of day, and device type to identify hidden biases.

Fair Performance

Analysis confirms no customer group is excessively over-flagged, and error rates remain stable across demographic segments.

Ongoing Commitment: We recommend continuous monitoring post-deployment to ensure fairness metrics remain within acceptable bounds as fraud patterns evolve.

How This Fits Into Operations



Auto-Approve

Low-risk transactions flow through instantly with no friction, maintaining optimal customer experience.

Manual Review

Medium-risk cases are queued for expert analyst review, combining AI efficiency with human expertise.

Auto-Block

High-risk transactions are immediately blocked, preventing fraud before it impacts the business.

Gradual Rollout Strategy

The system integrates seamlessly into existing fraud workflows and supports a phased deployment approach: starting with a controlled pilot, moving to shadow mode for validation, and culminating in full production deployment.

Recommended Actions

01

Deploy with Current Threshold

Launch the AI model using the optimized threshold that balances fraud detection and customer experience.

02

Monitor Key Metrics

Track fraud capture rate, false positive frequency, customer impact scores, and operational efficiency gains.

03

Periodic Recalibration

Regularly review and adjust thresholds based on performance data, seasonal trends, and evolving fraud tactics.

04

Explore Enhancements

Investigate real-time deployment options, incorporate additional contextual data sources, and integrate analyst feedback loops for continuous improvement.

> **This solution strengthens fraud protection while preserving trust and efficiency.**