

# **AI-Powered Fraud-Prediction Networks Market Forecasts to 2032 – Global Analysis By Component (Fraud Detection Engines, Behavioral Analytics Modules, Identity Verification Systems, Transaction Monitoring Platforms and Risk-Scoring Models), Deployment, Application, End User, and By Geography.**

<https://marketpublishers.com/r/AE719111FCC4EN.html>

Date: November 2025

Pages: 200

Price: US\$ 4,150.00 (Single User License)

ID: AE719111FCC4EN

## **Abstracts**

According to Statistics MRC, the Global AI-Powered Fraud-Prediction Networks Market is accounted for \$10.8 billion in 2025 and is expected to reach \$38.6 billion by 2032 growing at a CAGR of 20% during the forecast period. AI-powered fraud-prediction networks utilize machine learning and artificial intelligence to analyze vast transactional datasets, detect patterns, and identify anomalies indicative of fraudulent activity in real time. These adaptive systems continuously learn new fraud strategies, minimize false positives, and automate alerts, bolstering protective measures for sectors such as banking, e-commerce, identity verification, and insurance—reducing economic losses and enhancing trust.

According to the Bank for International Settlements, consortium-based AI models that analyze transaction patterns across multiple banks are significantly more effective at detecting sophisticated, cross-institutional payment fraud.

### **Market Dynamics:**

Driver:

Escalation of real-time transaction fraud

Escalation of real-time transaction fraud is intensifying enterprise demand for adaptive, AI-native prediction networks capable of detecting micro-anomalies at millisecond latency. Fueled by surging digital payments, cross-border e-commerce, and instant-settlement rails, financial institutions are prioritizing proactive fraud interdiction over reactive post-event investigations. Rising attack sophistication, especially across mobile wallets and embedded finance platforms, is accelerating platform modernization. Consequently, vendors are scaling graph-based inference engines to augment contextual decisioning and reduce false positives across continuously evolving threat landscapes.

Restraint:

High model drift in rapidly changing fraud signatures

High model drift in rapidly changing fraud signatures remains a critical barrier, as adversaries continuously alter behavioral patterns to evade detection. Spurred by volatile transaction streams and region-specific fraud vectors, supervised models often degrade without frequent re-training, imposing heavy operational overheads. This drift necessitates constant feature engineering, quality labeling, and pipeline recalibration, inflating cost structures for banks and fintechs. As a result, many organizations struggle to sustain reliable predictive performance, especially when fraud volumes spike unpredictably.

Opportunity:

Fusion of behavioral biometrics

Fusion of behavioral biometrics presents a compelling expansion pathway, enabling fraud-prediction networks to assess intent-driven micro-interactions beyond static credentials. Motivated by rising identity-theft cases and synthetic-ID fraud, institutions are integrating keystroke dynamics, gait patterns, touchscreen pressure, and navigation rhythms into multimodal fraud scoring engines. This convergence strengthens continuous authentication and enhances risk segmentation across high-velocity digital channels. Consequently, next-generation AI-risk platforms can deliver richer anomaly detection, reduce customer friction, and differentiate between legitimate users and orchestrated fraud attempts with higher precision.

Threat:

## Adversarial AI undermining predictive accuracy

Adversarial AI undermining predictive accuracy poses a substantial threat, as malicious actors deploy generative models to craft attack patterns that mimic legitimate user behavior. Driven by the proliferation of automated fraud-as-a-service ecosystems, these adversarial agents manipulate model blind spots, degrade classifier reliability, and inflate false-negative rates. Additionally, targeted poisoning of training datasets can destabilize fraud-prevention pipelines. This escalating arms race forces vendors to embed robust model-hardening, constant adversarial testing, and resilient ensemble architectures to maintain defensive efficacy.

## Covid-19 Impact:

Covid-19 accelerated the digitalization of payments, inadvertently triggering an unprecedented surge in phishing, account-takeover, and stimulus-fraud incidents. As remote onboarding and contactless transactions became mainstream, financial institutions adopted AI-fraud prediction tools to offset rising operational exposure. Heightened consumer vulnerability and reduced in-person verification fueled demand for automated risk-scoring engines and behavioral monitoring modules. Post-pandemic, fraud-prediction networks remain integral to safeguarding digital channels, with sustained investments in scalable cloud-native analytics and continuous identity assurance frameworks.

The fraud detection engines segment is expected to be the largest during the forecast period

The fraud detection engines segment is expected to account for the largest market share during the forecast period, resulting from their central role in orchestrating real-time anomaly scoring across high-velocity payment environments. Propelled by surging demand for deep-learning-based pattern recognition, these engines aggregate transactional, device, and behavioral telemetry to generate risk signals at scale. Their versatility across banking, insurance, and e-commerce ecosystems further solidifies dominance. Additionally, rapid enhancements in graph analytics and adaptive rule orchestration reinforce their market leadership.

The cloud-based systems segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the cloud-based systems segment is predicted to witness the highest growth rate, propelled by enterprises shifting from legacy on-premise risk engines to elastic, API-driven fraud intelligence platforms. Accelerated by real-time transaction volumes and global payment flows, cloud architectures provide rapid model deployment, continuous updates, and cross-regional threat telemetry sharing. Their pay-as-you-scale economics and seamless integration with digital banking stacks further amplify adoption. This flexibility is especially valuable for fintechs and neo-banks requiring instant fraud-response capabilities.

Region with largest share:

During the forecast period, the Asia Pacific region is expected to hold the largest market share, attributed to explosive growth in digital wallets, QR-based payments, and super-app ecosystems. Fueled by dense mobile penetration and rising cross-border remittance flows, the region faces elevated fraud exposure, prompting heavy investments in AI-centric risk-scoring frameworks. Additionally, regulatory bodies across India, Singapore, and Australia are mandating stronger authentication and fraud-monitoring controls. These dynamics position APAC as the most expansive deployment hub for real-time fraud-prediction networks.

Region with highest CAGR:

Over the forecast period, the North America region is anticipated to exhibit the highest CAGR, associated with rapid adoption of advanced fraud-intelligence platforms by banks, card networks, and digital-first lenders. Heightened cybercrime sophistication, coupled with aggressive regulatory scrutiny around consumer protection, is accelerating system upgrades. Furthermore, the region hosts leading AI-risk analytics vendors, enabling faster innovation cycles in adversarial detection, behavioral biometrics, and federated learning. Expanding fintech ecosystems and instant-payment rails further amplify demand for scalable, cloud-native fraud-prediction networks.

Key players in the market

Some of the key players in AI-Powered Fraud-Prediction Networks Market include FICO, Experian, NICE Actimize, SAS, LexisNexis Risk Solutions, Featurespace, Forter, Sift, Kount, Darktrace, DataVisor, Mastercard, Visa, PayPal, Feedzai, and ACI Worldwide.

### **Key Developments:**

In September 2025, NICE Actimize introduced its Generative AI Suspicion Analyzer, a tool that uses advanced large language models to automatically analyze the context of suspicious activity reports (SARs) and customer interactions, dramatically reducing false positives and improving the accuracy of financial crime alerts.

In August 2025, Featurespace unveiled the ARIC™ Risk Hub for Real-Time Payments, a specialized AI model designed to analyze the unique risk patterns of instant payment rails like FedNow and RTP, preventing fraudulent transactions within the sub-second decision window.

In July 2025, Mastercard launched its 'Consumer Fraud Risk' scoring service, an open-banking enabled AI network that allows merchants and issuers to share anonymized risk signals, providing a holistic view of a user's digital footprint to stop account takeover and friendly fraud.

#### Components Covered:

Fraud Detection Engines

Behavioral Analytics Modules

Identity Verification Systems

Transaction Monitoring Platforms

Risk-Scoring Models

#### Deployments Covered:

Cloud-Based Systems

On-Premise Platforms

Hybrid Infrastructure

Edge-AI Fraud Detection Nodes

## Distributed Fraud Intelligence Networks

### Applications Covered:

BFSI Fraud Management

E-Commerce Transaction Security

Identity & Access Fraud

Payment Gateway Monitoring

Digital Wallet Security

### End Users Covered:

Municipal Water Utilities

Industrial Facilities

Marine

Environmental Agencies

### Regions Covered:

North America

US

Canada

Mexico

Europe

Germany

UK

Italy

France

Spain

Rest of Europe

Asia Pacific

Japan

China

India

Australia

New Zealand

South Korea

Rest of Asia Pacific

South America

Argentina

Brazil

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & Africa

**What our report offers:**

- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2024, 2025, 2026, 2028, and 2032
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

**Free Customization Offerings:**

All the customers of this report will be entitled to receive one of the following free customization options:

**Company Profiling**

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

**Regional Segmentation**

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

## Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

## Contents

### **1 EXECUTIVE SUMMARY**

### **2 PREFACE**

- 2.1 Abstract
- 2.2 Stake Holders
- 2.3 Research Scope
- 2.4 Research Methodology
  - 2.4.1 Data Mining
  - 2.4.2 Data Analysis
  - 2.4.3 Data Validation
  - 2.4.4 Research Approach
- 2.5 Research Sources
  - 2.5.1 Primary Research Sources
  - 2.5.2 Secondary Research Sources
  - 2.5.3 Assumptions

### **3 MARKET TREND ANALYSIS**

- 3.1 Introduction
- 3.2 Drivers
- 3.3 Restraints
- 3.4 Opportunities
- 3.5 Threats
- 3.6 Application Analysis
- 3.7 End User Analysis
- 3.8 Emerging Markets
- 3.9 Impact of Covid-19

### **4 PORTERS FIVE FORCE ANALYSIS**

- 4.1 Bargaining power of suppliers
- 4.2 Bargaining power of buyers
- 4.3 Threat of substitutes
- 4.4 Threat of new entrants
- 4.5 Competitive rivalry

## **5 GLOBAL AI-POWERED FRAUD-PREDICTION NETWORKS MARKET, BY COMPONENT**

- 5.1 Introduction
- 5.2 Fraud Detection Engines
- 5.3 Behavioral Analytics Modules
- 5.4 Identity Verification Systems
- 5.5 Transaction Monitoring Platforms
- 5.6 Risk-Scoring Models

## **6 GLOBAL AI-POWERED FRAUD-PREDICTION NETWORKS MARKET, BY DEPLOYMENT**

- 6.1 Introduction
- 6.2 Cloud-Based Systems
- 6.3 On-Premise Platforms
- 6.4 Hybrid Infrastructure
- 6.5 Edge-AI Fraud Detection Nodes
- 6.6 Distributed Fraud Intelligence Networks

## **7 GLOBAL AI-POWERED FRAUD-PREDICTION NETWORKS MARKET, BY APPLICATION**

- 7.1 Introduction
- 7.2 BFSI Fraud Management
- 7.3 E-Commerce Transaction Security
- 7.4 Identity & Access Fraud
- 7.5 Payment Gateway Monitoring
- 7.6 Digital Wallet Security

## **8 GLOBAL AI-POWERED FRAUD-PREDICTION NETWORKS MARKET, BY END USER**

- 8.1 Introduction
- 8.2 Banks & NBFCs
- 8.3 E-Commerce Companies
- 8.4 Fintech Firms
- 8.5 Telecom Operators
- 8.6 Insurance Providers

## **9 GLOBAL AI-POWERED FRAUD-PREDICTION NETWORKS MARKET, BY GEOGRAPHY**

### 9.1 Introduction

### 9.2 North America

#### 9.2.1 US

#### 9.2.2 Canada

#### 9.2.3 Mexico

### 9.3 Europe

#### 9.3.1 Germany

#### 9.3.2 UK

#### 9.3.3 Italy

#### 9.3.4 France

#### 9.3.5 Spain

#### 9.3.6 Rest of Europe

### 9.4 Asia Pacific

#### 9.4.1 Japan

#### 9.4.2 China

#### 9.4.3 India

#### 9.4.4 Australia

#### 9.4.5 New Zealand

#### 9.4.6 South Korea

#### 9.4.7 Rest of Asia Pacific

### 9.5 South America

#### 9.5.1 Argentina

#### 9.5.2 Brazil

#### 9.5.3 Chile

#### 9.5.4 Rest of South America

### 9.6 Middle East & Africa

#### 9.6.1 Saudi Arabia

#### 9.6.2 UAE

#### 9.6.3 Qatar

#### 9.6.4 South Africa

#### 9.6.5 Rest of Middle East & Africa

## **10 KEY DEVELOPMENTS**

### 10.1 Agreements, Partnerships, Collaborations and Joint Ventures

- 10.2 Acquisitions & Mergers
- 10.3 New Product Launch
- 10.4 Expansions
- 10.5 Other Key Strategies

## **11 COMPANY PROFILING**

- 11.1 FICO
- 11.2 Experian
- 11.3 NICE Actimize
- 11.4 SAS
- 11.5 LexisNexis Risk Solutions
- 11.6 Featurespace
- 11.7 Forter
- 11.8 Sift
- 11.9 Kount
- 11.10 Darktrace
- 11.11 DataVisor
- 11.12 Mastercard
- 11.13 Visa
- 11.14 PayPal
- 11.15 Feedzai
- 11.16 ACI Worldwide

## List Of Tables

### LIST OF TABLES

Table 1 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Region (2024-2032) (\$MN)

Table 2 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Component (2024-2032) (\$MN)

Table 3 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Fraud Detection Engines (2024-2032) (\$MN)

Table 4 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Behavioral Analytics Modules (2024-2032) (\$MN)

Table 5 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Identity Verification Systems (2024-2032) (\$MN)

Table 6 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Transaction Monitoring Platforms (2024-2032) (\$MN)

Table 7 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Risk-Scoring Models (2024-2032) (\$MN)

Table 8 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Deployment (2024-2032) (\$MN)

Table 9 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Cloud-Based Systems (2024-2032) (\$MN)

Table 10 Global AI-Powered Fraud-Prediction Networks Market Outlook, By On-Premise Platforms (2024-2032) (\$MN)

Table 11 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Hybrid Infrastructure (2024-2032) (\$MN)

Table 12 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Edge-AI Fraud Detection Nodes (2024-2032) (\$MN)

Table 13 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Distributed Fraud Intelligence Networks (2024-2032) (\$MN)

Table 14 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Application (2024-2032) (\$MN)

Table 15 Global AI-Powered Fraud-Prediction Networks Market Outlook, By BFSI Fraud Management (2024-2032) (\$MN)

Table 16 Global AI-Powered Fraud-Prediction Networks Market Outlook, By E-Commerce Transaction Security (2024-2032) (\$MN)

Table 17 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Identity & Access Fraud (2024-2032) (\$MN)

Table 18 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Payment

Gateway Monitoring (2024-2032) (\$MN)

Table 19 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Digital Wallet Security (2024-2032) (\$MN)

Table 20 Global AI-Powered Fraud-Prediction Networks Market Outlook, By End User (2024-2032) (\$MN)

Table 21 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Banks & NBFCs (2024-2032) (\$MN)

Table 22 Global AI-Powered Fraud-Prediction Networks Market Outlook, By E-Commerce Companies (2024-2032) (\$MN)

Table 23 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Fintech Firms (2024-2032) (\$MN)

Table 24 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Telecom Operators (2024-2032) (\$MN)

Table 25 Global AI-Powered Fraud-Prediction Networks Market Outlook, By Insurance Providers (2024-2032) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

## I would like to order

Product name: AI-Powered Fraud-Prediction Networks Market Forecasts to 2032 – Global Analysis By Component (Fraud Detection Engines, Behavioral Analytics Modules, Identity Verification Systems, Transaction Monitoring Platforms and Risk-Scoring Models), Deployment, Application, End User, and By Geography.

Product link: <https://marketpublishers.com/r/AE719111FCC4EN.html>

Price: US\$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

[info@marketpublishers.com](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/AE719111FCC4EN.html>