OPUS

Whitepaper

Harnessing AI for Payment Fraud Detection

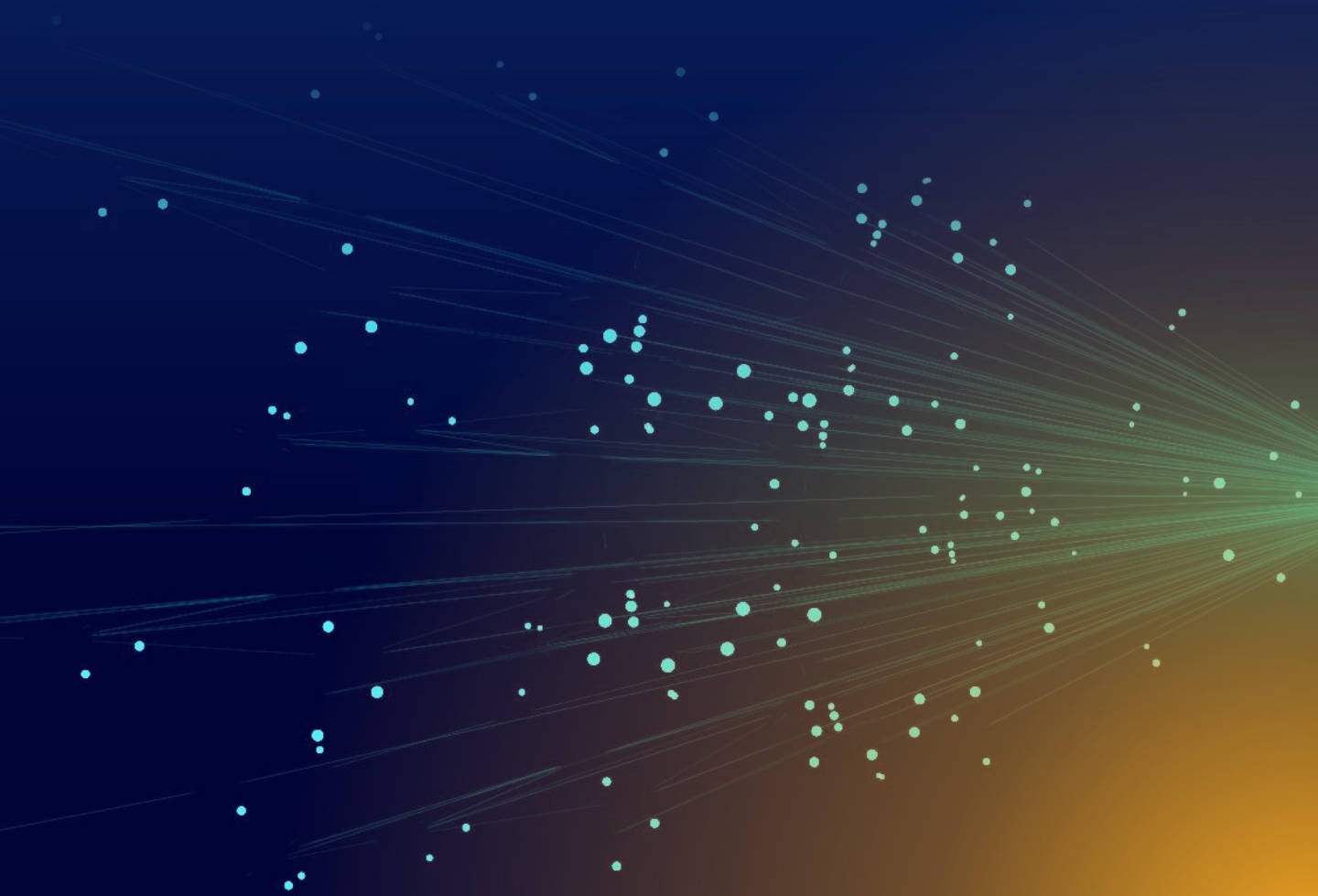


Table of Contents

	Page
Executive Summary	03
The Invisible Risk in Modern Commerce	04
The Modern Fraud Landscape: Scale, Velocity, and Key Statistics	05
Reassessing Financial Liability and Operational Costs	08
Current Fraud Defenses: Strengths and Limitations	09
Generative AI as the Catalyst for Security Resilience	10
Strategic Business Value of AI-Powered Fraud Detection	13
Building the Data Foundation for Intelligent Fraud Management	14
Analyzing AI-Powered Fraud Detection Tools and their Key Features	16
Strategic Outlook Directives for Future Security	18
Establishing AI Intelligence as the Foundation for Future Payments Resilience	19

© 2026, Opus Technologies

Executive Summary

Payment fraud is evolving exponentially in both scale and sophistication, presenting a systemic risk to financial institutions, processors, and merchants. The imperative is clear: transactions must be safeguarded while maintaining uninterrupted commerce and customer experience.

Traditional, rule-based security systems are fundamentally reactive. They struggle to adapt to emerging threats, creating critical vulnerabilities that fuel the proliferation of fraud across expanding digital channels. The convergence of high-volume digital commerce and evolving threat actor tactics necessitate intelligent, adaptive, and real-time defense architecture.

This paper outlines how Artificial Intelligence (AI) facilitates effective combat against payment fraud. By leveraging advanced machine learning, behavioral analytics, and precise anomaly detection, AI enables organizations to:

- Identify fraudulent patterns proactively
- Minimize operational friction caused by false positives
- Accelerate defense and response times

We present the strategic roadmap for strengthening defenses, illustrating practical use cases and deployment strategies. AI-driven intelligence is the critical investment required to reduce financial losses, ensure operational resilience, and establish enduring customer trust in the digital economy.

© 2026, Opus Technologies

The Invisible Risk in Modern Commerce

Digital payments are the fundamental engine powering the growing global economy. While facilitating unprecedented transaction velocity and convenience, this reliance on speed introduces a significant, often hidden cost: systemic risk driven by fraud, operational disruption, and critical regulatory exposure.

This reality poses a pivotal question for every commerce platform and financial institution: What happens when the very systems built for seamless digital payments become direct conduits for financial crime?

Consider the Cost: A retailer processes a sudden surge of high-value, seemingly legitimate orders. Transactions are approved instantly. Hours later, the inevitable chargebacks roll in. The merchant discovers that automated bots have exploited system blind spots using dozens of stolen credit card numbers. The consequence is immediate: thousands of dollars in chargebacks, valuable operational time consumed by manual investigations, and a severe erosion of customer and partner trust.

Modern payment fraud is fast, adaptive, and increasingly automated. As the global payments infrastructure becomes more connected, threat actors proliferate and quickly exploit subtle system vulnerabilities. Relying on traditional, reactive fraud detection systems is no longer a viable option; these legacy models detect damage only after the financial loss has occurred. In an economy where frictionless, millisecond transactions define success, the defense strategy must pivot from reactive triage to proactive anticipation.

AI-powered intelligence transforms how organizations preempt, tackle, and neutralize payment fraud. Fraud often occurs in plain sight, undetected by static rules, a failure point that AI-driven systems are specifically engineered to avoid. These models analyze patterns across billions of data points in real-time, instantly identifying subtle anomalies and predicting emerging threats with minimal human intervention.



© 2026, Opus Technologies

The Modern Fraud Landscape: Scale, Velocity, and Key Statistics

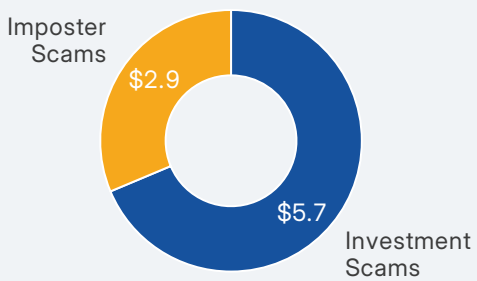
Consumer fraud risk is accelerating year over year, driven by higher loss severity per victim rather than increased incident volume, signaling more targeted, high-impact attacks. The table below highlights a sharp escalation in fraud impact, with losses rising 25% year-over-year, a growing share of victims losing money, and attack patterns shifting toward more targeted, high-value fraud.

Exhibit 1: Annual Fraud Loss and Severity Trends

Metric	2023	2024	YoY Change
Total Fraud Losses	~$10.0B	$12.5B	▲ 25%
Victims Losing Money	27%	38%	▲ 11 pts
Attack Pattern	Broad	Targeted, High-Value	↑ Severity

The chart indicates that investment scams contribute the largest share of reported fraud losses in 2024, significantly exceeding losses from imposter scams. This reflects a shift toward more sophisticated, high-value fraud schemes that exploit trust and long-term engagement. The trend highlights the increasing severity and financial impact of investment-related fraud.

The threat landscape is rapidly crystallizing around financially destructive schemes. Furthermore, operational risk is concentrated in transaction channels, with credit card fraud particularly card-not-present transactions, driving most incidents, chargebacks, and merchant P&L impact.



© 2026, Opus Technologies

Key Pressure Points: Benchmarking the US Payments Vulnerability

The speed of digital commerce amplifies high-frequency fraud vectors, creating critical pressure points in the U.S. payments infrastructure and highlighting where defenses are most urgently needed.

Fraud Vectors and Statistics for 2024

- **New Account (Application) Fraud:** Criminals utilize stolen or synthetic identities to open new accounts or acquire new cards. With 406,110 reported cases, this vector accounts for a dominating 90% of all credit card-related fraud incidents.
- **Existing Account Fraud:** Any unauthorized use of a valid card/account. This type represents with approximately 52,400 reported cases, accounting for about 10% of total cases.
- **Card-Not-Present (CNP) Fraud:** Fraud conducted via online or mobile transactions where physical card presentation is absent. Losses from CNP transactions reached an estimated $10 billion, accounting for approximately 71% of all card-related fraud losses.
- **Synthetic Identity Fraud:** Fraudsters create fictitious identities by combining real and fabricated personal data to establish accounts that appear legitimate. This is the fastest-growing form of fraud, demonstrating a massive 153% rise.
- **Account Takeover (ATO) Fraud:** Cybercriminals gain unauthorized access to a customer's digital wallet or bank account, often through credential stuffing, malware, or phishing. ATO fraud rose 28% and constitutes a significant portion of digital fraud cases.
- **Phishing and Social Engineering:** Fraudsters trick individuals into revealing sensitive information via emails, calls, or websites, accounting for about 15% of global payment fraud attempts.
- **E-Skimming:** Incidents of e-skimming (digital skimming) have surged by 350% across e-commerce platforms, costing U.S. banks and consumers an estimated $1 billion every year.
- **Friendly Fraud (Chargeback Fraud):** Customers dispute valid charges to receive refunds. This loss serves as a cost multiplier; for every $1 lost to chargeback fraud, merchants typically lose between $2.40 and $4.61 after factoring in labor, fees, and operational costs.



© 2026, Opus Technologies

Quantifying the Rising Cost of Fraud

The table highlights that fraud losses continue to rise sharply in the United States and are projected to grow steadily worldwide. Card-not-present fraud remains the dominant driver of losses across digital channels. For merchants, the true impact of fraud extends well beyond direct losses, with significant additional costs incurred per incident.

Exhibit 2: US vs Global Fraud Economic Impact

	United States (2024)	Global (Projection)
Reported fraud losses	$12.5 billion	$32+ billion annually by 2025
Year-over-year increase	25%	Rising steadily worldwide
CNP Fraud	~70% of card fraud losses	Similar trend across digital channels
Cost multiplier per $1 lost (merchants)	$3- $4	Comparable across regions
AI/ML fraud detection adoption	~80% of financial institutions	Rapidly increasing, but uneven
Impact of AI adoption	20 - 30% fewer false positives	Early adopters report similar gains

Exhibit 3: Fraud losses in the US for 2023 and 2024

Fraud losses are climbing in the US.

US consumers lost 25% more to fraud in 2024 than the year prior.



Source: Federal Trade Commission (FTC)

For most organizations, the real challenge now lies in strengthening fraud detection without letting technology costs spiral.

Root-Cause Factors Behind Fraud Acceleration

The rise in fraud stems not just from external threats but from system and market vulnerabilities. Fast, complex digital payment chains create multiple weak points like misconfigured APIs or outdated authentication, allowing attackers to exploit transactions before detection.

The key systemic drivers accelerating payment fraud risk include:

- Proliferation of Non-Cash Transactions
- Mobile Proliferation and Fragmented Ecosystems
- Globalization and Cross-Border Payments
- Usage of AI-Enabled tools by threat actors

© 2026, Opus Technologies

Reassessing Financial Liability and Operational Costs

Payment fraud affects the entire financial ecosystem, causing financial and reputational damage. Its ripple effects force costly recovery and operational disruption across key stakeholders:

Consumers: Face financial loss and lengthy account recovery, eroding trust in digital payments and merchants.

Merchants: Incur chargebacks, inventory losses, operational disruptions, reputational damage, and costly security upgrades, squeezing profit margins.

Financial Institutions: Face reimbursement liabilities, resource-intensive dispute management, costly fraud investigations, system upgrades, and regulatory compliance burdens.

Regulators and Policy Makers: They must continually update anti-fraud frameworks, security standards, and cross-border rules to maintain market stability.



© 2026, Opus Technologies

Current Fraud Defenses: Strengths and Limitations

While a growing number of organizations today are adopting advanced fraud detection techniques like predictive analytics and anomaly detection to prevent payment fraud, below traditional approaches remain mainstream in several organizations:

Rule-Based Monitoring: Uses predefined rules and thresholds to flag unusual activity, such as high-value transactions, rapid transfers, or repeated login failures.

Manual Transaction Monitoring and Analytics: It involves analysts reviewing alerts using customer profiles, transaction history, and context to assess authenticity.

Blacklists and Historical Pattern Matching: Institutions use blacklists and historical patterns to block or flag transactions linked to known fraud accounts, IP addresses, or cards.

Static Authentication Methods: Traditional security relies on static methods like passwords and PINs, which are easily compromised by phishing and social engineering.

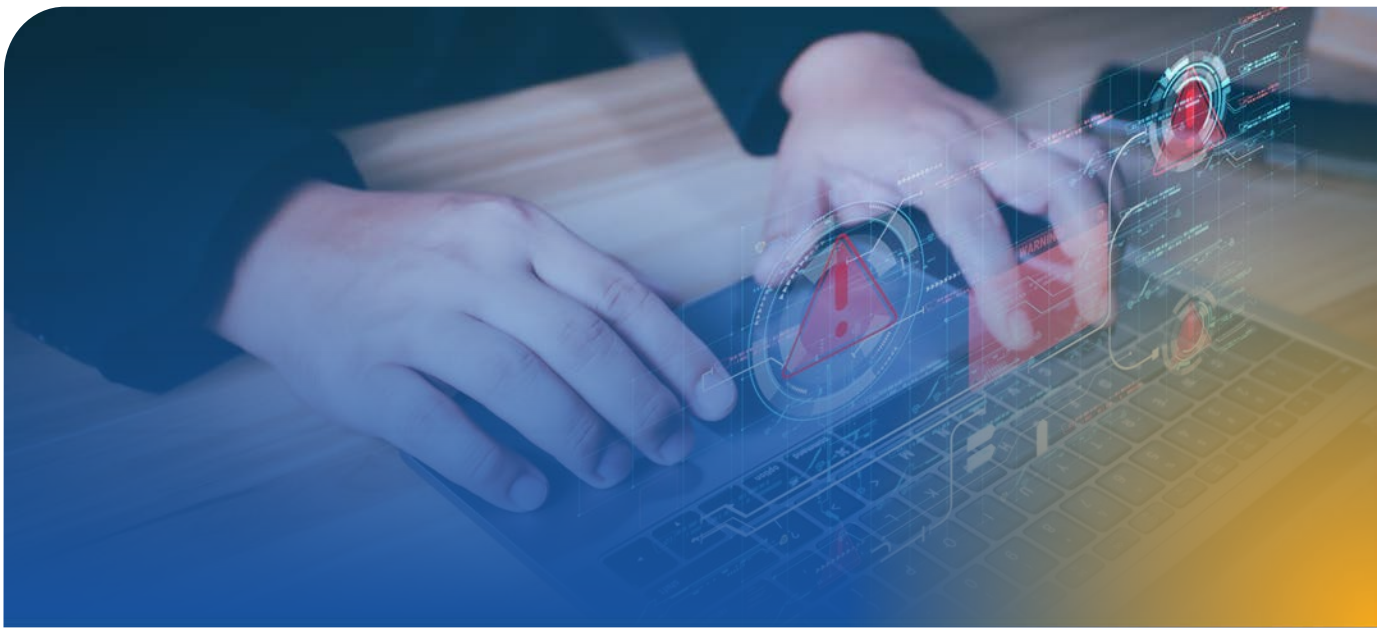
Multi-Factor Authentication (MFA) and Identity Verification: These advanced methods use biometrics, OTPs, and knowledge checks to reduce account compromise risk.

Collaborative Intelligence and Threat Sharing: Institutions share fraud intelligence to enable early detection and uncover patterns not visible in isolation.

While essential for baseline security, these methods are largely reactive. Modern fraud demands proactive prevention, as traditional and hybrid systems limited by rigid rules, fragmented data, and delayed responses struggle to counter fast-evolving threats. The key gaps that amplify systemic vulnerability include:

- High False Positives
- Limited Adaptability to New Fraud Techniques
- Siloed Data
- Reactive Detection
- Resource-Intensive Processes
- Inadequate Identity Verification

The inability of static systems to learn and integrate real-time, cross-channel data creates an unacceptable critical gap, necessitating a complete shift toward dynamic, intelligent defense architecture.



© 2026, Opus Technologies

Generative AI as the Catalyst for Security Resilience

Automation combined with Generative AI is delivering a fundamental breakthrough in payment fraud detection, offering a decisive advantage in prevention and control.

Generative AI strengthens defenses across multiple layers of the fraud management lifecycle:

Exhibit 4: Layers of capability in fraud detection using GenAI

01 **Deepfake Detection**
Leveraging Generative AI-powered deepfake detection is essential to counter payment frauds, where advanced synthetic media is used to manipulate biometric or identity verification systems and exploit financial platforms.

02 **Potential in Fraud Detection**
Generative AI holds significant potential in enhancing fraud detection for payment systems by identifying complex patterns, synthetic identities, and anomalies that traditional methods often miss.

03 **Proactive Fraud Prevention**
Generative AI enables proactive fraud prevention in payment systems by predicting and identifying threats before they occur.

04 **Synthetic Data Generation**
Generative AI can create synthetic data to simulate payment fraud scenarios, enhancing model training and improving fraud detection accuracy without compromising real user data.



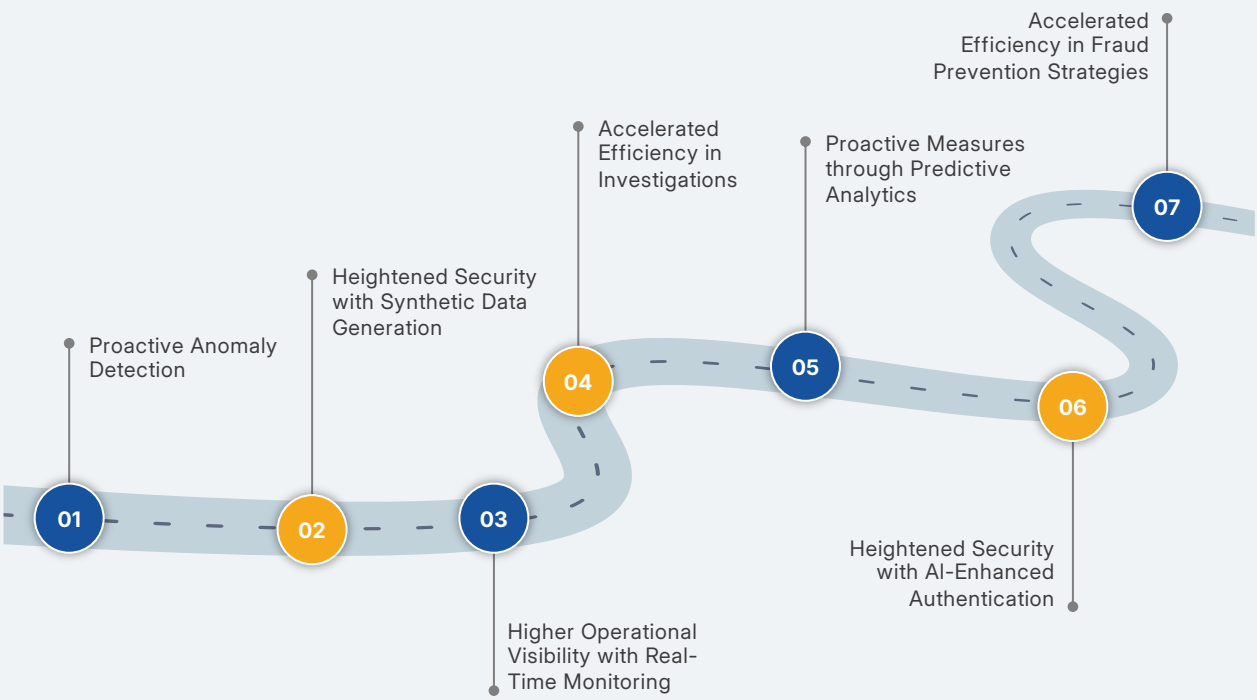
© 2026, Opus Technologies

Operationalizing AI Intelligence for Seamless Defense

Fraud detection has become a critical, non-negotiable pillar of today's digital commerce ecosystem. Financial service providers are increasingly adopting advanced AI to strengthen their offerings and address rising fraud risks across the payments landscape. Technologies such as Deep Learning, Machine Learning (ML), and Natural Language Processing (NLP) equip banks, acquirers, and payment processors with deeper analytical insights, enabling smarter decisions and more accurate fraud prevention.

By seamlessly integrating AI into existing payment platforms, organizations achieve higher detection precision, faster response times, and reduced operational costs. AI-driven fraud prevention also allows teams to shift focus from manual intervention to strategic innovation, while immediately lowering fraud exposure and improving transaction security and efficiency. The diagram below illustrates how Generative AI is driving this shift from reactive monitoring to proactive, intelligent prevention through early anomaly detection, synthetic data generation, real-time visibility, faster investigations, predictive analytics, and enhanced authentication.

Exhibit 5: How is Generative AI Transforming fraud detection?



Source: Generative AI in Fraud Detection: Transforming Financial Security

The AI Blueprint: Core Capabilities Redefining Fraud Strategy

AI fundamentally redefines detection strategies through its core capabilities:

Automatic Anomaly Detection: AI analyzes high-volume, real-time payment data to spot subtle fraud patterns, helping providers stay ahead of evolving threats and reduce financial losses.

Synthetic Data Generation: AI generates synthetic fraud data to supplement limited real data, improving model accuracy and strengthening fraud detection.

Pattern Recognition and Proactivity: AI uncovers complex patterns and analyzes trends to boost accuracy, enabling a shift from reactive to proactive fraud prevention.

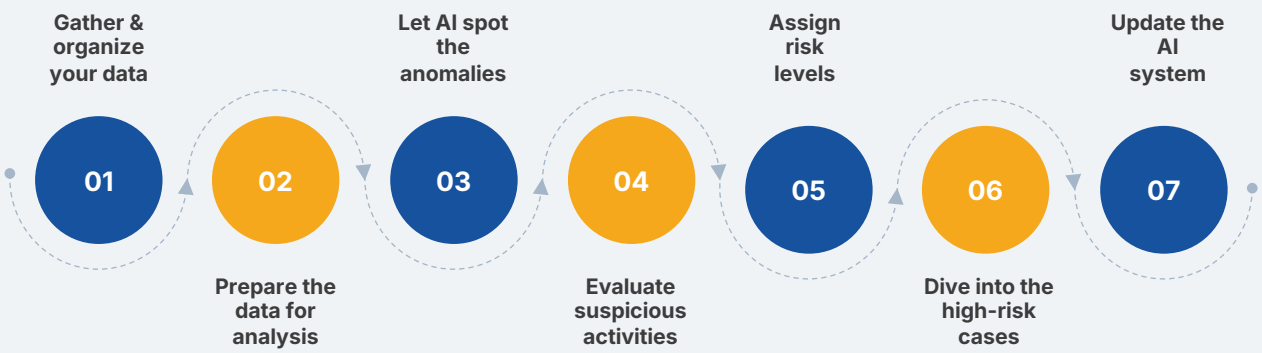
False Positive Reduction: AI's self-learning reduces false positives, saving time and resources and allowing teams to focus on high-risk cases.

Real-Time Analysis: AI processes massive data in real time, enabling instant decisions to detect and stop fraud before losses occur.

Adaptive Learning: Unlike rule-based systems, AI adapts to evolving patterns and learns continuously to detect and stop new fraud threats autonomously.

Below diagram illustrates an AI-driven fraud investigation lifecycle, from data ingestion and preparation to anomaly detection, risk scoring, analyst review, and continuous model improvement for smarter, faster fraud response.

Exhibit 6: Investigate Financial Fraud with AI



Source: AI-Driven Fraud Detection: Reshaping Financial Security

Strategic Business Value of AI-Powered Fraud Detection

Implementing an advanced AI-powered fraud detection solution represents more than an IT security upgrade; it is a strategic imperative that offers payment providers numerous competitive advantages beyond enhanced security. AI adoption delivers quantifiable and non-quantifiable benefits directly impacting the bottom line and long-term viability:

Optimized Operational Costs: Automating manual processes and workflows enables providers to cut costs and minimize human errors, resulting in highly efficient operations and reduced overhead. This directly lowers investigation costs, reduces losses from fraud, and optimizes resource allocation.

Accelerated Payment Processing: AI-powered detection accelerates payment processing by quickly and confidently validating transaction risk. This ensures secure and seamless fund transfers while eliminating unnecessary friction points.

Scalability and Multi-Channel Protection: AI dynamically scales with explosive transaction volumes, adapting across cards, digital wallets, banking, and e-commerce to ensure consistent, enterprise-wide fraud protection. Systems automatically adapt to new users, geographies, and payment methods without requiring major reconfiguration.

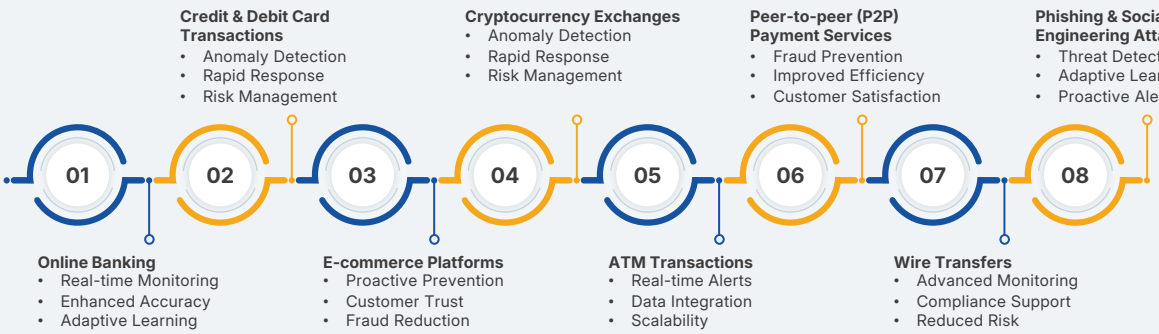
Regulatory Compliance and De-risking: AI enables continuous regulatory compliance by automating monitoring, reporting, and audit trails across AML, KYC, PSD2, and PCI-DSS. Proactive risk detection reduces penalties, mitigates reputational risk, and ensures ongoing regulatory alignment.

Increased Approval Rates: Traditional rule-based systems often decline genuine transactions, leading to lost revenue. AI refines risk scoring using sophisticated behavioral data, drastically reducing false alerts while maintaining stringent security. This directly improves approval rates, boosting both revenue and customer experience.

Enhanced Customer Trust and Experience: AI ensures that legitimate transactions are processed promptly, thereby minimizing the likelihood of operational friction. Furthermore, demonstrably enhanced security fosters deep customer trust, reinforces brand reputation, and cultivates long-term loyalty and increased customer lifetime value.

Adopting AI-driven fraud detection delivers a clear strategic advantage through more accurate risk assessment, real-time intelligence, and data-driven decisions. It reduces losses, improves efficiency, and strengthens customer trust, enhancing profitability and long-term resilience across payments, banking, and digital channels.

Exhibit 7: Benefits of Gen AI in Financial Fraud Detection



Source: Generative AI in Fraud Detection: Transforming Financial Security

© 2026, Opus Technologies

Building the Data Foundation for Intelligent Fraud Management

The effectiveness of AI-driven payment fraud detection is fundamentally determined by the strength of the underlying data foundation. AI is not a standalone technology investment; it is a data-led capability that requires broad, timely, and trusted information to deliver measurable business value. Institutions that treat data as a strategic asset are best positioned to realize the full benefits of AI adoption.

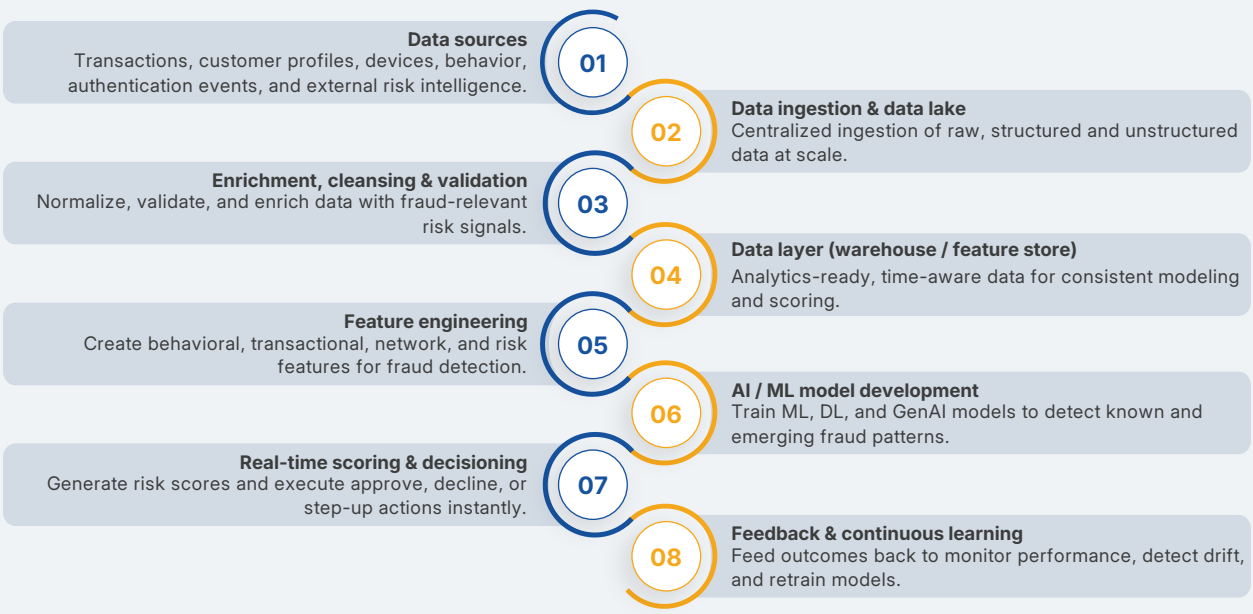
Enterprise-Wide Data Requirements

AI-driven fraud detection requires an enterprise-wide view of the payment lifecycle covering transactions, customers, merchants, and networks. This unified visibility allows AI models to surface subtle risk signals that are typically missed in siloed or fragmented environments. Comprehensive data coverage directly enables higher approval rates, lower fraud losses, and enhanced customer experience. High level data categories include:

- Transactional data
- Customer & behavioral data
- Fraud & labeled data
- Network & ecosystem data
- Real-time & contextual signals
- External and synthetic data

Effective AI-based fraud detection depends on a robust, governed, and continuously evolving data lifecycle. The accuracy, explainability, and scalability of AI models are directly tied to how data is sourced, processed, enriched, and operationalized across the enterprise. Below diagram highlights the steps involved in data preparation for AI models:

Exhibit 8: From Data to Decisions: AI in Payment Fraud Detection



© 2026, Opus Technologies

Data Governance, Security, and Regulatory Readiness

Robust data governance is a prerequisite for successful enterprise AI adoption. Data must be trusted, secure, auditable, and fully aligned with regulatory requirements such as PCI DSS and data privacy mandates. Strong governance frameworks materially reduce regulatory exposure, reinforce confidence among customers and ecosystem partners, and enable AI initiatives to scale responsibly.

An enterprise-wide, well-governed data foundation allows AI systems to deliver sharper risk insights, faster decision-making, and continuous improvement directly advancing strategic priorities such as cost efficiency, revenue protection, regulatory de-risking, and long-term operational resilience.

In summary, data readiness is not a technical prerequisite, it is a board-level strategic enabler. Organizations that invest in the right data capabilities position themselves to move from reactive fraud management to proactive, intelligence-driven risk prevention.

AI-Powered Fraud Detection: Outsource or In-House?

Financial institutions are increasingly leveraging AI to combat payment fraud, choosing operating models that align with strategic priorities, risk appetite, and speed-to-market goals. Many strike a balance between rapid deployment and long-term control: outsourced AI platforms deliver fast rollout and immediate analytics, while in-house AI capabilities provide tailored solutions and competitive differentiation. Selecting the right model enables faster fraud detection, reduced operational risk, and enhanced customer trust. The next section highlights leading AI-powered tools that drive these outcomes.



© 2026, Opus Technologies

Analyzing AI-Powered Fraud Detection Tools and their Key Features

The landscape of payment fraud detection is rapidly evolving, fueled by advancements in AI. Leading platforms are leveraging machine learning, behavioral biometrics, and real-time monitoring to significantly enhance the detection and prevention of fraudulent transactions across the financial ecosystem. The following platforms exemplify the key capabilities required for next-generation mitigation:

1. Feedzai Risk Platform

This platform integrates behavioral, monetary, and non-monetary data to detect complex fraud patterns that traditional systems often overlook. It combines Artificial Intelligence, Machine Learning, and expert human insight to safeguard revenue, reputation, and customer trust.

Core Capabilities:

- **Real-time Machine Learning:** Utilizes machine learning for real-time transaction monitoring to detect anomalies and potential fraud instantly.
- **Multi-Channel Support:** Supports comprehensive payment channels, including card, ACH, online, mobile, in-store, and ATM transactions.
- **Unified Compliance:** Provides a consolidated platform for both fraud detection and Anti-Money Laundering (AML) compliance.

2. Sift Digital Trust & Safety Platform

Sift leverages a massive global data network to detect and prevent fraud in real-time, focusing on minimizing both false positives and false negatives.

Core Capabilities:

- **Behavioral Analysis:** Utilizes real-time machine learning models to analyze user behavior and identify potential threats across the customer journey.
- **Holistic Protection:** Offers features for account takeover (ATO) protection, payment fraud detection, and content moderation.
- **Customizable Risk:** Offers customizable risk thresholds to tailor fraud detection settings to individual business risk appetites precisely.
- **Seamless Integration:** Designed for integration with existing systems through robust APIs and SDKs.

3. ARIC™ Risk Hub by Featurespace

Widely adopted by banks, e-money institutions, and payment processors, ARIC is designed to detect subtle anomalies, such as transaction laundering or rapid, high-velocity fund movements.

Core Capabilities:

- **Contextual Behavioral Analysis:** Leverages machine learning to analyze behavioral data across past, current, and future timelines to uncover peer group activities and evaluate potential scam behaviors.
- **Continuous Adaptability:** The system continuously evolves according to new transaction patterns and fraud trends, ensuring models remain relevant without manual intervention.
- **Self-Improving Models:** Models refine and self-improve over time, eliminating the need for periodic manual retraining.
- **Enhanced Protection:** Offers robust defense against scams, account takeovers, and payment fraud while preserving customers' ease of use.

© 2026, Opus Technologies

4. ComplyAdvantage Mesh

This is a leading SaaS-based risk intelligence platform designed to unite global data to combat financial crime holistically.

Core Capabilities:

- **Alert Prioritization:** Uses machine learning and rules-based algorithms alongside ID clustering and graph analysis to identify and prioritize suspicious activities and reduce false positives.
- **Real-Time Sanctions Screening:** Scalable to billions of transactions, it detects sanctioned entities in real-time and provides a single consolidated view of payment alerts.
- **Non-Compliance Reduction:** Minimizes the risk of regulatory non-compliance through real-time sanctions and data intelligence.

5. AI Risk Platform by Sardine

Sardine's platform consolidates vendors and enhances operational efficiency, offering advanced features like device intelligence and behavioral biometrics.

Core Capabilities:

- **Automated Risk Decisioning:** Automates risk decisioning to improve fraud catch rates and detect money laundering significantly.
- **Scam Protection:** Proactively protects customers from scams by identifying and blocking malicious activities before losses occur.
- **Comprehensive Platform:** Provides a unified platform for fraud detection, credit assessment, and regulatory compliance.



© 2026, Opus Technologies

Strategic Outlook Directives for Future Security

The future of fraud detection lies in advanced AI that outperforms traditional rule-based systems by analyzing vast and complex datasets. Combining ML and deep learning enables more accurate detection by uncovering subtle anomalies, behavioral patterns, and hidden fraud schemes that conventional methods miss.

AI-powered fraud detection solutions can provide a wide range of real-time checks, including:

- **Real-time Decisioning:** AI systems must analyze payment data instantly, enabling the swift detection and flagging of suspicious activity. This significantly accelerates response times and is critical for minimizing financial losses in high-velocity environments.
- **Comprehensive Behavioral Analysis:** AI must monitor customer behavior across all channels, including social media, online interactions, and transaction history, using a comprehensive approach to detect inconsistencies and anomalies that reliably indicate payment fraud.
- **Collaborative Intelligence and Data Sharing:** AI-powered platforms are essential for enabling seamless data sharing among financial institutions. This harnesses collective insights, allowing the industry to detect and anticipate emerging and evolving fraud tactics more effectively.
- **Model Transparency and Interpretability:** As AI models grow more advanced, transparency in decision-making is essential to build trust, enable human oversight, optimize performance, and mitigate bias.



© 2026, Opus Technologies

Establishing AI Intelligence as the Foundation for Future Payments Resilience

In an evolving threat landscape, payment fraud remains a critical risk, requiring providers to shift from reactive to proactive defense. Leading platforms are adopting AI, ML, and Generative AI to enhance fraud prevention through real-time detection, adaptive learning, and advanced threat recognition.

Collaborating with trusted AI-powered fraud detection vendors enables payment providers to accelerate essential digital transformation with certainty. This strategic move not only dramatically enhances fraud prevention capabilities but also promotes organizational innovation, improves operational efficiency, and builds long-term resilience against today's constantly evolving threat environment.

In the critical battle against payment fraud, the organizations that lead will be those that embrace intelligent automation and predictive analytics. Realizing transformation at this scale requires a thorough assessment of current legacy systems and seamless integration with advanced AI technologies, supported by a partner with deep domain knowledge and technical proficiency. Opus Technologies acts as a strategic enabler, enhancing fraud prevention efforts while fostering innovation and long-term resilience for payment service providers.



© 2026, Opus Technologies

About the Author



Viddyulata Limkar
Consultant

Viddyulata Limkar has over 15 years of consulting experience in the IT industry, with a strong focus on the Banking and Payments domain. She has worked extensively with leading organizations in the BFSI sector, establishing herself as a seasoned payments consultant with comprehensive expertise across the entire payments lifecycle from initiation and orchestration to processing, tokenization, clearing, and settlement, Authorization, Online, and Card payments, with hands-on experience in leading payment switch platforms such as Connex and Base24 Classic. Her professional journey includes engagements with renowned firms such as Infosys, Capgemini, Accenture, HCL and other global financial institutions.

© 2026, Opus Technologies

References

1. The evolving landscape of payment fraud | Thredd
2. Combating fraud in the era of digital payments - PwC India
3. 12 Online Payment Frauds Types (How to Avoid them)
4. Fraud Prevention and Chargeback Fraud Protection | Riskified
5. Generative AI in Card Fraud Detection: Benefits, Use Cases, and Industry Impact
6. Transaction Fraud Solution for Banks | Feedzai
7. Top 10 AI Fraud Detection Tools for Online Payments in 2025: A Comprehensive Guide - SuperAGI
8. AI in Financial Fraud Detection: The Comprehensive Guide 2025 | SmartDev
9. ARIC™ Risk Hub | Financial Crime & Fraud Software | Featurespace
10. Mesh
11. 13 Best fraud detection software solutions in 2025
12. Sardine: The AI risk platform for fraud, credit, and compliance
13. Nacha FBI's IC3 report
14. Nilson Report on Card Present Losses
15. Generative AI in Fraud Detection: Transforming Financial Security
16. AI-Driven Fraud Detection: Reshaping Financial Security

© 2026, Opus Technologies



Opus is a trusted engineering partner to payment providers, banks and fintechs navigating change in a real-time, digital-first world. We solve for business value—accelerating go-to-market, unlocking future readiness, and powering transformation at scale.

Our promise is simple: Business Value Acceleration. Realization. Maximization.

We deliver on this promise through the Opus trifecta—a domain-native engineering skillset, a value-creation mindset, and a toolset that drives business agility. From MVP (Minimum Viable Product to MPT (Maximum Possible Transformation), Opus turns engineering into business advantage.

Contact us

info@opustechglobal.com

www.opustechglobal.com

