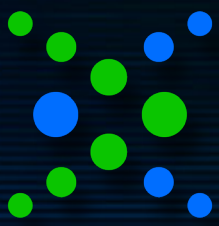
ARTIFICIAL INTELLIGENCE:

RAPIDLY REDEFINING THE PAYMENTS LANDSCAPE

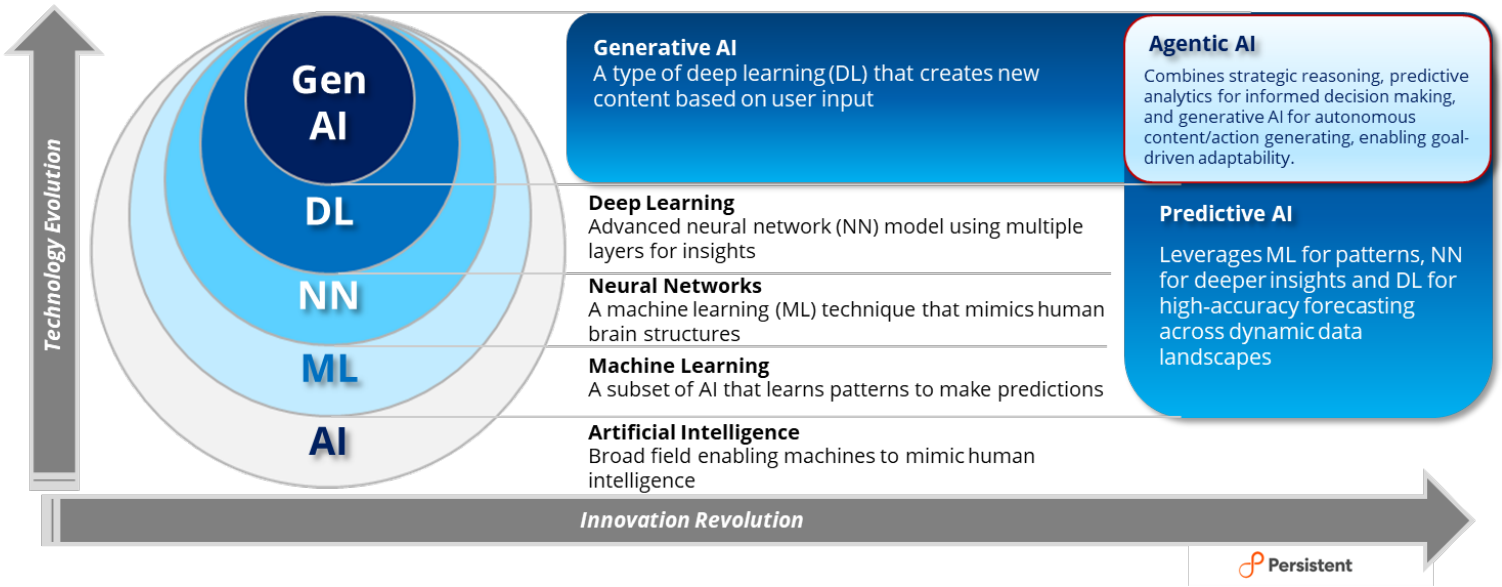


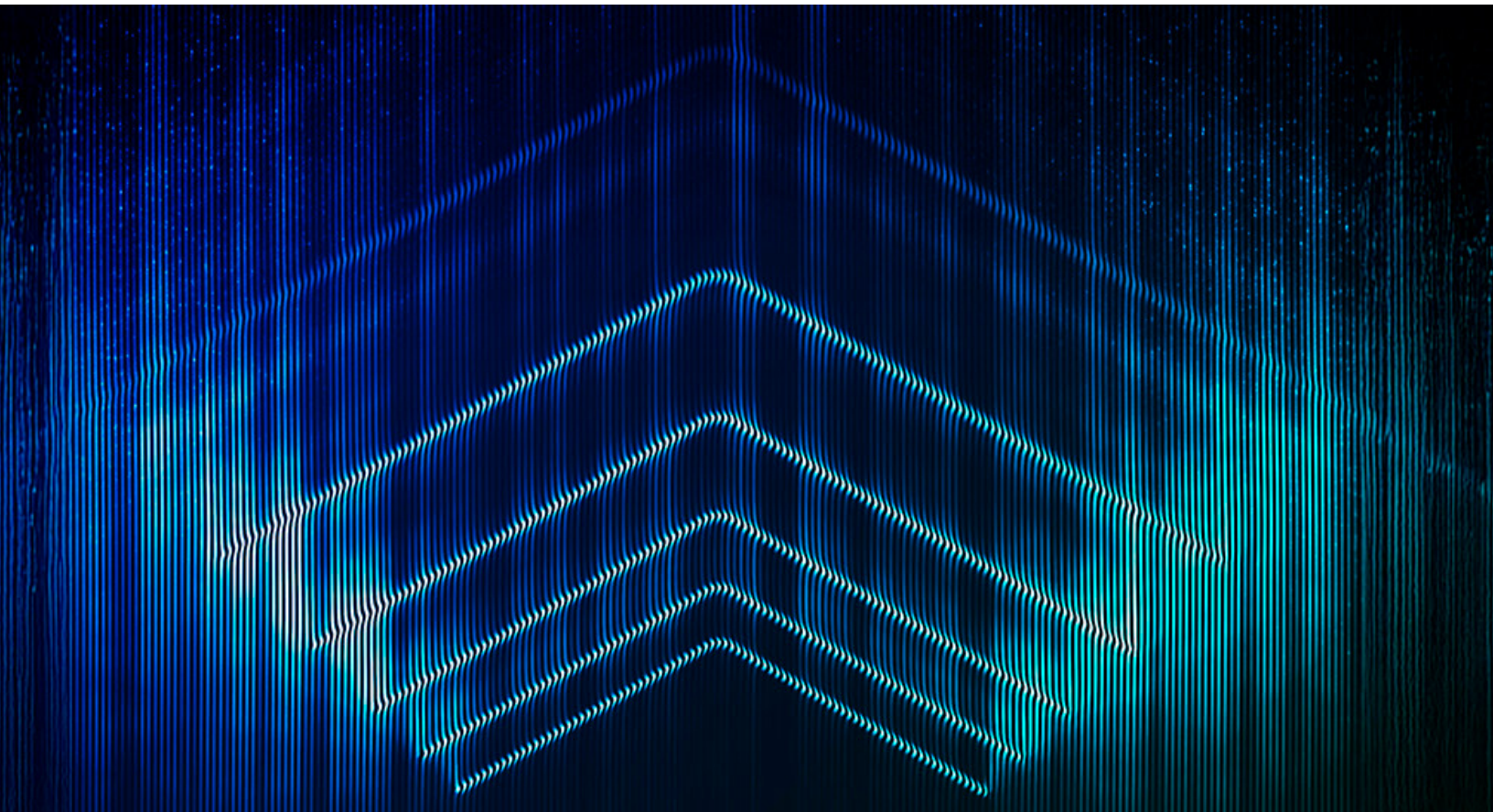
Payments Innovation Alliance®

ARTIFICIAL INTELLIGENCE: SETTING THE STAGE

Artificial intelligence (AI) is regarded as both an evolutionary and revolutionary phenomenon. The evolution of continuous technological advancements and tools is enhancing efficiency and functionality. Concurrently, AI will result in completely new business models and applications – revolutionizing the realm of innovations that appeared to be science fiction only a short time ago.

While there are three general terms used to define today's capabilities – generative, predictive and agentic – the line between these terms is already blurring as shown in the diagram.





	Generative AI	Predictive AI	Agentic AI
Definition	**Generative AI is reactive and focuses on a specific task.** It generates new content such as text, images, video, music, and software code by learning from existing data and user input.	**Predictive AI is forward-looking.** It recognizes patterns from historical data to forecast future trends and outcomes.	**Agentic AI is proactive and focuses on achieving a goal with minimal human oversight.** It exhibits autonomy, memory and intent using tools that dynamically plan, source, and adapt to achieve the intended goal.
Benefits	• Performs specific tasks that require human intervention for new tasks. • Limited decision-making because the generated outputs are based on an existing data set and the user's prompts. • Easy-to-use tools that are readily available in most browsers.	• Makes informed predictions based on historical data, statistical algorithms and machine learning that can aid with new account opening and loan decisioning. • Analyzes existing patterns that can help detect potential money mules and money laundering.	• Solves complex tasks to achieve a goal without human intervention. • Can manage complex multi-step processes like personal shopping to buy, book, subscribe, and transact on a user's behalf. • Readily sifts and differentiates information sources for quality and reliability, increasing the degree of trust in its decisions. • Quickly learns human values and preferences to align with decisions and actions.
Challenges	• May create "hallucinations" with incorrect data, or image errors such as missing parts or fabricated information.	• Limited to existing data and patterns that may miss novel scenarios and be subject to inherent biases.	• Multi-agent systems can pose risks that are hard to detect as a result of poorly designed systems, aggressive optimization, cascading "hallucinations," and errors. • Autonomy can lead to unintended consequences if not properly managed (e.g., misrouted payments). Clearly defined goals, feedback loops, and safeguards are required to ensure alignment with the user's intentions.

PAYMENTS TRANSFORMATION AND USE CASES

The payments landscape is being redefined with AI capabilities that can enable new offerings, help combat payments fraud and significantly transform the user experience and back-office operations. It is certain more applications will evolve and become increasingly complex and far-reaching.

Hyper-personalized experiences that tailor offers, payment plans, and even interfaces based on a user's behavior. Spending habits, savings goals, and life events can be analyzed to offer tailored product recommendations and budgeting tools. Instead of one-size-fits-all, the user feels that their financial institution knows them.

Enhanced security with biometric authentication (like facial recognition or voice ID) and behavioral analysis can increase security without adding friction. Anomalies can detect how a person types or swipes, flagging potential fraud before it happens.

Smarter, faster transactions that optimize payments routing, leading to fewer false declines resulting in smoother checkouts and higher approval rates.

Smarter customer support that deploys chatbots and virtual assistants to handle routine queries 24/7—everything from checking balances to disputing charges. And they're getting better at understanding natural language, so the experience feels less robotic and more like talking to a helpful human.

Faster, frictionless transactions that help speed up everything from loan approvals to fraud detection. For example, it can assess creditworthiness in seconds using alternative data, or flag suspicious activity in real time to protect the user's account.

Agentic payments where AI agents autonomously execute financial transactions. Think virtual assistants that not only suggest purchases but actually complete them—with pre-set rules.

Sample Payments Use Cases		
Generative AI	**Predictive AI**	**Agentic AI**
• A financial institution or payments provider can generate payments test files.	• A financial institution or payments provider can detect and monitor payment anomalies of patterns (frequency, amount, payees, user behavior, etc.).	• A financial institution, payments provider or end user can optimize payments routing to improve speed, efficiency, and cost-effectiveness.
• An authenticated utility customer can query, "Why did my bill change?"	• A lender can readily assess an application to detect fraud or make better credit decisions.	• Agentic commerce uses AI-powered agents that know a user's preferences, budget and values. It connects to the user's digital identity and payment credentials to buy, book, subscribe, and transact on the user's behalf.

PAYMENT FRAUD THREATS

Fraudsters are getting disturbingly clever with AI, and the payments industry is feeling the heat. AI has lowered the barrier to entry for fraudsters to perpetrate financial crimes. There are now black-market platforms offering "fraud kits" powered by AI—complete with fake documents, phishing scripts, and even chatbots that mimic customer service agents. It's organized crime, reimagined as a SaaS model.

A recent report found that AI was involved in 42% of all financial fraud attempts, yet only 22% of firms had AI defenses in place.[1] That gap is a flashing red warning light.

Illustrative Payments Fraud Threats

Generative AI	Predictive AI	Agentic AI
• Synthetic voices or images built from real and fabricated data – known as "deepfakes" – can be used to make people believe something is real when it is not. These identities can pass standard Know Your Customer checks, open bank accounts, and apply for loans, with funds vanishing before detection. • Voice clones may bypass biometric security and be used to impersonate executives resulting in unauthorized wire transfers. • Companies and individuals can be imitated with AI tools that can manipulate text messages, emails, and social media with results that are more convincing than ever before. In seconds, a message can reference a person's recent vacation, child's name, or employer with hyper-personal phishing attacks.	• Legacy fraud detection systems often rely on static rules. Behavior can be adapted in real time by learning from fraud detection systems to avoid triggering alerts. Techniques may include transaction splitting or timing manipulation.	• Hijacked or spoofed AI agents can be changed to modify the goal or user preferences to achieve automated money laundering across multiple jurisdictions.

1 Signicat report Battle Against AI-Driven Identity Fraud

THE RISK OF SITTING ON THE SIDELINES

AI is no longer a futuristic concept—it's a competitive edge. The question isn't whether the payments industry should pay attention. It's whether it can afford not to. Payments industry stakeholders that resist adopting AI risk becoming irrelevant.

Customer Attrition Risk

Modern customers—especially Gen Z and millennials—expect personalized, digital-first experiences. A 2024 study found that over half of these consumers would consider switching financial institutions for more tailored digital services.[2] Without AI, financial institutions and payments providers struggle to meet those expectations.

Data Underutilization Risk

Data is a strategic asset. Companies risk leaving value on the table when unable to use data to drive AI models that provide meaningful insights.

Operational Inefficiency Risk

AI streamlines everything from fraud detection to loan processing. Financial institutions and payments providers that don't use it remain bogged down by manual processes, slower decision-making, and higher costs.

Regulatory Risk

Avoiding AI doesn't mean avoiding complexity. Regulators are increasingly expecting financial institutions to use advanced tools for compliance, monitoring, and reporting. Falling behind can mean higher scrutiny and missed efficiencies.

Revenue Loss Risk

AI-driven personalization and marketing can generate significant additional revenue. Those who opt out leave that money on the table—and risk falling behind more agile competitors.

Risk Management Risk

AI can enable real-time fraud detection and predictive credit scoring. Without it, financial institutions and payments providers rely on outdated models, increasing exposure to fraud and bad loans.

2 Persado report The State of AI in Financial Services Marketing: Expectations, Uses and Impact

CALL TO ACTION

AI is changing the payments landscape for all financial institutions, payments providers, and organizations making or receiving payments. In addition to creating an implementation road map and culture that welcomes intelligent automation, it is important to address three key considerations:

- AI models and outputs are auditable.
- New concerns around data privacy, algorithmic bias, and regulatory oversight.
- Best practices and policies that address the ethical use of AI.

The future of payments will be built by those who leverage AI, not those who watch from the sidelines. Invest in understanding, piloting, and scaling AI capabilities.

This document was developed by the Cybersecurity & Payments AI Project Team of Nacha's Payments Innovation Alliance.

The Payments Innovation Alliance is a membership program that shapes the future of the payments industry and develops thought leadership relevant to financial service institutions. The Alliance established the Cybersecurity & Payments AI Project Team to help organizations understand and respond to evolving threats related to potential cyberattacks. Visit the Cybersecurity & Payments AI Project Team page to see more resources developed by the team.