7 Things You Need to Know About …

AI in Payments

A quick guide to understanding AI in Payments from the Association of Payment Professionals
Leading the community to safeguard payments

1 | WHAT IS IT?

Artificial Intelligence (AI) is an evolving technology that has recently impacted the payment industry, both good and bad. The Oxford dictionary defines AI as the theory and development of computer systems able to perform tasks that normally require human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages. For the payment industry, this translates into more advanced tools for underwriting and risk monitoring of merchant accounts. AI can support identity management, monitor and predict transaction management, along with creating content for policies and procedures. The payment industry is at the cusp of understanding the impact of innovation from both fraudsters and value-added technology businesses.

2 | HOW DOES IT WORK?

Artificial Intelligence is used for different applications or purposes by fraudsters, processors, and financial institutions, to improve efficiency. From a fraudsters' perspective, Artificial Intelligence has enhanced documentation forgery, online storefronts, and detection responses from their illicit activity. Here are some ways fraudsters are taking advantage of Artificial Intelligence:

- Documentation forgery – quicker processing and supplying of fictious documents: bank statements, identification cards
- Content / images – creating ecommerce storefronts and leveraging AI to create unique appearances
- Collecting large datasets, analyzing results
- Evading detection with automated schemes often utilizing countermeasures of detection
- Content - automated emails requesting payment on false pretenses – impersonating trusted entities

Financial institutions are combatting the efforts of fraudsters by utilizing these enhancements with Artificial Intelligence:

- Automation: streamlining onboarding processes through pattern recognitions, quarantining items for human interaction (identity verification)
- Threat detection: malicious code, prohibited content
- Sender analysis, communication analysis

03 | WHO IS DOING IT?

Many companies have entered into the marketplace bringing their own unique products. Here are some of the major ones:

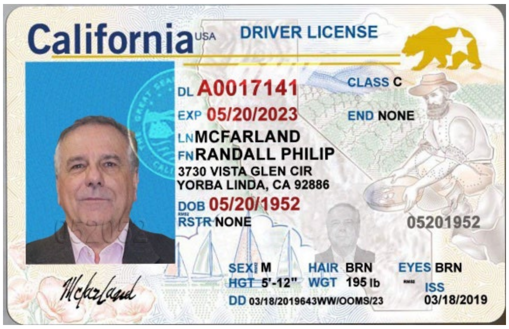
Company	Product	Differentiation
Visa	Visa Advanced Authorization	Real-time fraud detection and prevention
Mastercard	Decision Intelligence	Enhanced security and streamlined payment processes
PayPal	Fraud Protection Advanced	Machine learning for detecting fraudulent transactions and AI chatbots for customer support
Square	Square Analytics	Transaction analysis and business insights for merchants Startups and Innovators
Stripe	Radar	Optimized payment processing and fraud prevention
Plaid	Plaid Insights	Seamless financial data integration and insights
Klarna	Klarna's Credit Risk Assessment	Personalized shopping experiences and credit risk management
Zest	Zest Automated Machine Learning (ZAML)	Credit underwriting through machine learning

There are three key partnership and influencers worth knowing as well:

- **Apple & Goldman Sachs:** Apple Card with AI-powered financial management tools
- **Google & Citigroup**: Digital banking service with AI-enhanced customer experiences
- **Amazon & JPMorgan Chase**: AI-driven payment solutions within the Amazon ecosystem

04 | WHY IS IT SIGNIFICANT?

AI has been much publicized and will have significant impacts on our world and the payments space is no exception. More specifically to risk management, there are both positive and negative impacts. The ability for fraudsters to create merchant accounts is now easier. In the past, you may have seen a fake driver's license, and an underwriter is able to spot nuances such as information that does match other information collected for the underwriting process. (continued on next page…)


California USA DRIVER LICENSE
DL A0017141
CLASS C
EXP 05/20/2023
END NONE
LN MCFARLAND
FN RANDALL PHILIP
3730 VISTA GLEN CIR
YORBA LINDA, CA 92886
DOB 05/20/1952
RSTR NONE
05201952
SEX M
HAIR BRN
EYES BRN
HGT 5'-12"
WGT 195 lb
ISS 03/18/2019
DD 03/18/2019643WW/OOMS/23

This is a fake ID that looks real at first glance but is not.

04 | WHY IS IT SIGNIFICANT?

...continued from previous page.

With AI, fraudsters can not only create a fake ID that is hard to spot, but they can also create fake social media accounts and other documents that create an identity around the merchant that is much more difficult to spot. This puts additional pressure on risk departments to identify and catch fraudsters with real time processing data before the fraudsters process illegal transactions. This increases the risk of financial losses associated with fraud.

At the same time, AI can be used to protect from these criminal endeavors. Using machine learning to analyze the various data points collected during the underwriting process helps weed out fraudulent accounts. AI also allows for machine learning models and the payments space does have access to a large amount of historical data, this can be used to spot fraud in ways that have not been available to the industry in the past.

The significance of this is both positive and negative. The ability to keep up with and prevent financial losses from fraudsters has always been a challenge in the payments industry. AI will continue this trend and may require companies to invest in this technology to keep up with the fraudsters using it in the payments space. Unfortunately, it may take an increase in financial losses to justify the increased investment in AI technologies given the competing investments required in the payments industry.

Common Technologies Behind AI…

Machine Learning: Machine learning algorithms analyze and learn from unstructured data, identifying hidden patterns to make predictions. They're commonly used for fraud detection and process optimization.

Natural Language Processing (NLP): NLP enables systems to understand human language, supporting chatbots and IVR platforms for customer service tasks like billing and payment inquiries with minimal human input.

Predictive Analytics: Predictive analytics uses historical data to forecast future outcomes, such as transaction volumes or the risk of bad debt.

Generative AI: Generative AI creates text, images, or other content in response to prompts, powering virtual agents and chatbots in the payments industry for cost-effective customer support.

This APP publication is for general information purposes only. It does not constitute business or legal advice, and do not represent any undertaking to keep recipients advised as to any or all relevant industry or legal developments. Any information, views, or opinions expressed by contributors to this publication do not necessarily represent the views and opinions held by APP. APP assumes no liability or responsibility for the accuracy, completeness, or usefulness of any information presented in this publication.

05 | WHAT IS THE DOWNSIDE?

The integration of AI in the payments industry presents numerous benefits, but it also introduces several downsides and potential risks that must be carefully assessed and managed. Here we explore some of them:

Dynamic Nature of Cybersecurity and Fraud
AI's sophistication enables both combating and facilitating evolving fraud tactics, requiring constant adaptation of detection and prevention systems. The novelty of AI tools can lead to unprecedented threats, underscoring the need for robust cybersecurity practices and updated threat-detection tools.

Data Privacy Concerns
AI systems trained on user data pose significant privacy risks if confidential information is inadvertently used. Opting out of data usage must be made clear to prevent unintentional breaches.

Reliability of AI-Generated Information
Workers might trust AI-generated information without verification, leading to the spread of incorrect data. Critical evaluation and cross-checking of AI outputs are essential.

Malware and Phishing Risks
Downloading counterfeit AI applications can result in malware infections, compromising sensitive information. Vigilance and education on identifying legitimate AI apps are crucial.

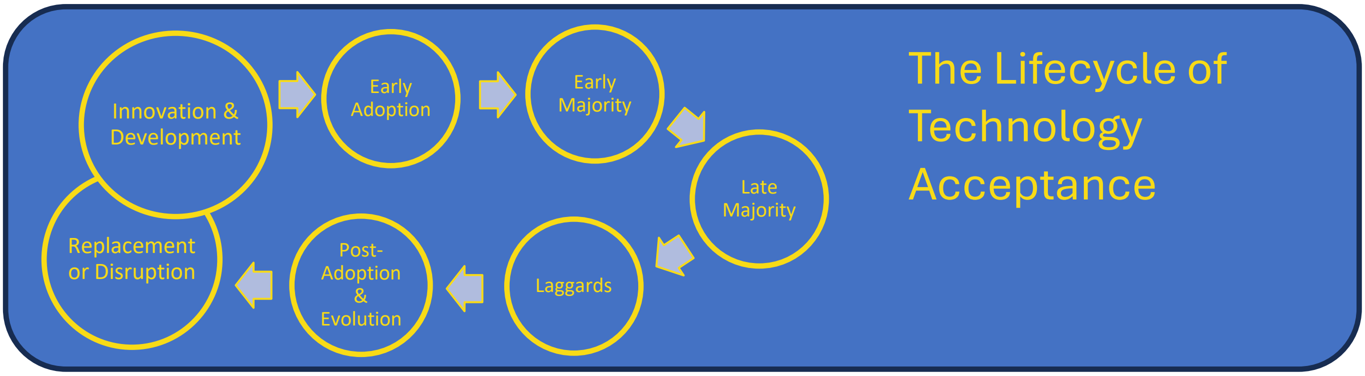
Lack of Rules and Guidelines
Some financial institutions prohibit using generative AI due to risk and regulatory concerns. Clear guidelines and frameworks are necessary to integrate AI technologies safely.

Bias and Discrimination
AI can inadvertently favor certain some sub-segments of your data resulting in unconscious bias on an organizational level.

A comprehensive approach involving robust cybersecurity practices, data privacy protections, critical evaluation of AI-generated information, and proactive countermeasures against AI-facilitated fraud is essential to harness the benefits of AI while minimizing its downsides.

06 | WHERE IS IT GOING?

The introduction to new technical advancements has been often met with fear (the internet for instance). The internet may be the most important tool we use as a society today and payments have clearly benefited from its creation. The use of AI in payments will be seen the same way. It will be feared and scrutinized. Right now, the payments industry is cautious of the use of AI to create “deep fake” media, fraudulent bank statements, fake identification, etc. These fears, although real, should not be the only thing being considered. Once we move past fear and begin to really see the utility of AI, the industry will see a product that can benefit financial institutions, payment processors, merchants, and consumers.



The Lifecycle of Technology Acceptance

We have already seen the use of “Human Taught” or “Machine Learning” AI already through large scale fraud detection systems, data mining, and code creation. Where AI in payments may be going is the use of “Generative AI.” Generative AI can create large language models based on analyzing massive sets of data (the internet) and predict the next number, word, color, etc. We will see companies such as Google perfect their generative AI that can scan a person’s search history, inbox, purchases, and location. This data gathering can then be packaged and delivered as the right message at the right time to drive sales and payments. This type of AI can help monetize a company’s unique data that other companies do not have. Generative AI may be able to interpret transactions where it may help prevent “friendly fraud” while also flagging real fraud. The use of machine learning AI to help detect fraud and the use of generative AI to mine unique data and custom market specific products/services to customers on a larger scale is where AI in payments may be going.

2017 → 20% - percentage of companies using AI in at least one business function.

2024 → 72% - percentage of companies using AI in at least one business function.

Per a 2024 McKinsey & Company Survey

07 | WHAT ARE THE IMPLICATIONS FOR PAYMENTS?

Fraudsters are using AI to generate these supporting documents in tandem with legitimate documents to establish merchant accounts for what can only be surmised for nefarious purposes. The more AI is taught, the better it will become at generating documents that are more likely to pass scrutiny.

Identity Documents

- Photo and text being too clear and crisp. Check the metadata of all images.
- Use common sense. Measurements should add up. For example, an individual's height of 5'12" would never be on a government-issued ID.
- The photo part of the photo ID should fill the portrait box entirely.
- Ideally, you should require both sides of the identification. Use a barcode scanner, typically available for free from most app stores, to read the barcode and compare it to the information on the front of the ID.

Financial Documents
The running balance may not always reconcile. Dust off the 10-key and take a moment to run the numbers

- Compare the statements from one month to the next. Look for inconsistencies in font type, size, and alignment. Your attention to detail is vital in this process.
- Take a moment to examine the transactions on the statement.
    - Look for geographic discrepancies. There are no Publix's in Brooklyn, and there are no Wegman's in Los Angeles.
    - Deposits should add to the balance, and withdrawals should deduct from the balance. Sometimes, these types of transactions are inversed because AI doesn't understand how banking works.

Of course, AI can also be used to fight fraud. Tools are helping to identify fraudsters using bogus documents. And AI tools are being used to analyze large data pools to identify patterns.

This Seven Things publication was produced with contributions from members of APP's Strategic Interest Group on Fraud Trends.

Contributors
James Filomena: AVP and Risk Officer, Esquire Bank
Jonathan Corona: COO, MobiusPay
Jekabs Sliede: Managing Director, OmmPay
Kevin Lambrix: SVP, Gravity Payments
Mark Creizman: Director, Material Connections LLC, Pay.com
Julie Schwartz: VP and Senior Compliance Office, Esquire Bank
Jason Ondriezek: Risk Manager, Fortispay

About APP

The Association of Payment Professionals (APP) is a volunteer-driven, nonprofit, membership organization committed to safeguarding the payments ecosystem through education, collaboration, and leadership.

www.paymentpros.org info@paymentpros.org