# Revolutionizing Payments with Al

Tackling Risks, Challenges and Seizing Opportunities

Karamjit Singh VP, AI Products, Mastercard



#### Disclaimer

The views and opinions expressed in this presentation are those of the presenter and do not necessarily reflect the official policy or position of Mastercard or any of its affiliates. This content is intended for informational purposes only.





Brain Game

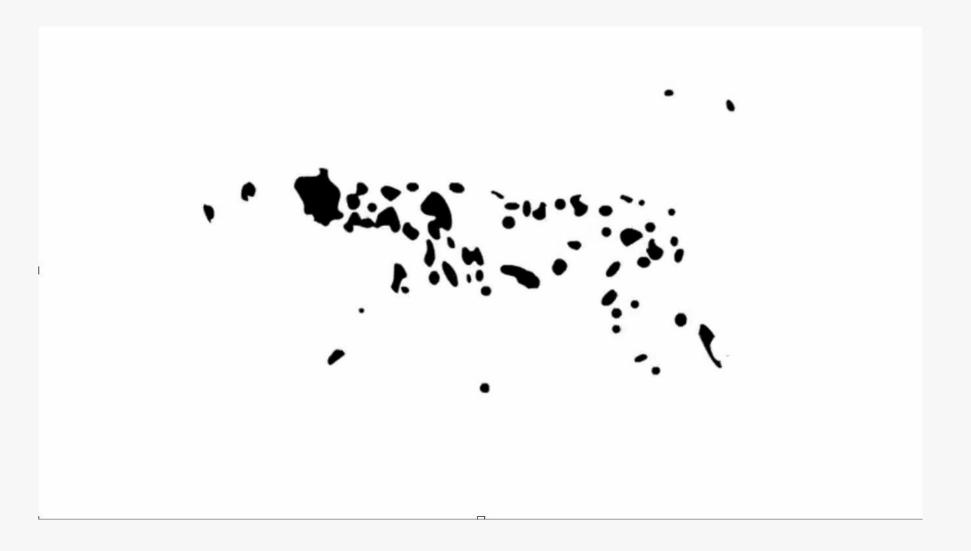
**Trends** 

**Applications** 

Risks and mitigations

Challenges

## How our Brain identifies Missing Values



## Missing Data In Finance



#### KYC

We know a customer through the KYC.

Often data is incorrect; even if correct, it is not complete information about customer



#### **Transactions**

We also have insights about some transactions of the customer. We miss out on many transactions that may not be happening through our platform





#### **Past Experiences**

We have information about how customers have behaved in the past; who is a good customer; who cannot be relied upon



#### **External Information**

Which jobs and occupations are stable and safe; what is the trend going forward; how is the market and competition doing

While we have many information sources, they are all disparate and incomplete

We need a brain that can work even with incomplete data!

## **Key Trends Shaping the Future of Payments**

Explosion in Digital Transactions

- ➢ Globally, 76% of adults had a digital payment account in 2021, up from 51% in 2011. (World Bank, June 2022)
- Over 40% of adults in low/middle-income economies (excl. China) were new to digital merchant payments post-COVID. (World Bank, June 2022)
- U.S. e-commerce surged by 43% in 2020 to \$815.4B. (U.S. Census Bureau, April 2022)

**Insight:** Consumer behavior is fundamentally shifting towards online and contactless payments, with digital wallets and mobile banking gaining prominence.

Rising Fraud Complexity and Velocity

- > 80% of organizations faced payment fraud attempts in 2023, a 15% increase YoY. (Stripe, August 2024)
- Global merchant fraud losses projected to exceed \$362B between 2023-2028.
   (Primer, November 2023)

**Trend:** Fraudsters are leveraging advanced tech like AI for sophisticated attacks (phishing, social engineering, deepfakes). (The Payments Association, December 2024)

**Challenge**: Real-time payments accelerate fraud, demanding faster and more intelligent detection. (EY, November 2023)

Demand for Real-Time, Personalized Experiences

- 90% of consumers desire more personalized brand communication. (Attentive, April 2025)
- > 77% are more likely to buy with relevant product recommendations. (Attentive, April 2025)
- Fast-growing companies see **40**% more revenue from personalization. (Contentful, January 2025)
- > 54% of U.S. consumers want financial providers to use their data for personalization. (MX, May 2024)

**Insight**: Consumers are increasingly willing to share data for relevant and tailored experiences.





#### **Customer Service and Support**

LLMs are used to automate customer interactions via chatbots and VAs

#### **Fraud Detection**

Generative AI can be used to generate realistic but fake data to help train models for detecting fraudulent transactions to capture new and evolving patterns



#### **Customer Service and Support**

LLMs are used to automate customer interactions via chatbots and VAs

#### **Fraud Detection**

Generative AI can be used to generate realistic but fake data to help train models for detecting fraudulent transactions to capture new and evolving patterns

#### **Risk Management**

Generative AI can simulate various financial scenarios and market conditions to help companies and individuals assess risk and make more informed decisions



#### **Customer Service and Support**

LLMs are used to automate customer interactions via chatbots and VAs

#### **Fraud Detection**

Generative AI can be used to generate realistic but fake data to help train models for detecting fraudulent transactions to capture new and evolving patterns

#### **Risk Management**

Generative AI can simulate various financial scenarios and market conditions to help companies and individuals assess risk and make more informed decisions

Generate personalized investment recommendations based on a user's risk tolerance, financial goals, and market trends.



# 01 07 02 03 06 05

#### **Customer Service and Support**

LLMs are used to automate customer interactions via chatbots and VAs

#### **Fraud Detection**

Generative AI can be used to generate realistic but fake data to help train models for detecting fraudulent transactions to capture new and evolving patterns

#### **Risk Management**

Generative AI can simulate various financial scenarios and market conditions to help companies and individuals assess risk and make more informed decisions

#### **Portfolio Management**

Generate personalized investment recommendations based on a user's risk tolerance, financial goals, and market trends.

## Credit Scoring

Simulate different credit scenarios and assess risk more accurately to make more informed lending decisions and provide fairer credit scoring.

#### **Personalized Financial Planning**

Create customized financial plans for individuals by analyzing data about their income, expenses, and goals.



#### **Compliance and Regulatory Monitoring**

Automating compliance checks and monitoring regulatory changes.

#### **Credit Scoring**

Simulate different credit scenarios and assess risk more accurately to make more informed lending decisions and provide fairer credit scoring.

#### **Personalized Financial Planning**

Create customized financial plans for individuals by analyzing data about their income, expenses, and goals.

## **Customer Service and Support**

LLMs are used to automate customer interactions via chatbots and VAs

#### **Fraud Detection**

Generative AI can be used to generate realistic but fake data to help train models for detecting fraudulent transactions to capture new and evolving patterns

#### **Risk Management**

Generative AI can simulate various financial scenarios and market conditions to help companies and individuals assess risk and make more informed decisions

#### **Portfolio Management**

Generate personalized investment recommendations based on a user's risk tolerance, financial goals, and market trends.





#### **Document Analysis and Automation**

Process and analyze complex financial documents to extract key information and automate compliance and reporting tasks.

#### **Compliance and Regulatory Monitoring**

Automating compliance checks and monitoring regulatory changes.

#### **Credit Scoring**

Simulate different credit scenarios and assess risk more accurately to make more informed lending decisions and provide fairer credit scoring.

#### **Personalized Financial Planning**

Create customized financial plans for individuals by analyzing data about their income, expenses, and goals.

## **Customer Service and Support**

LLMs are used to automate customer interactions via chatbots and VAs

#### **Fraud Detection**

Generative AI can be used to generate realistic but fake data to help train models for detecting fraudulent transactions to capture new and evolving patterns

#### **Risk Management**

Generative AI can simulate various financial scenarios and market conditions to help companies and individuals assess risk and make more informed decisions

#### **Portfolio Management**

Generate personalized investment recommendations based on a user's risk tolerance, financial goals, and market trends.





Risks



## Risks

#### **Deepfake-based Fraud**

Risk of convincing deepfakes videos and audios leading to unauthorized access and fraudulent transactions.



#### Risks



#### **Deepfake-based Fraud**

Risk of convincing deepfakes videos and audios leading to unauthorized access and fraudulent transactions.

#### **Phishing Attacks**

Highly personalized and sophisticated phishing attempts targeting customers.





#### **Deepfake-based Fraud**

Risk of convincing deepfakes videos and audios leading to unauthorized access and fraudulent transactions.

#### **Phishing Attacks**

Highly personalized and sophisticated phishing attempts targeting customers.

#### **Data Poisoning**

Injection of false data into AI training sets compromising decision accuracy.





#### **Deepfake-based Fraud**

Risk of convincing deepfakes videos and audios leading to unauthorized access and fraudulent transactions.

#### **Phishing Attacks**

Highly personalized and sophisticated phishing attempts targeting customers.

#### **Data Poisoning**

 Injection of false data into AI training sets compromising decision accuracy.

#### **Synthetic Identity Creation**

Realistic synthetic identities by combining different elements from various real identities.

#### Risks



#### **Deepfake-based Fraud**

Risk of convincing deepfakes videos and audios leading to unauthorized access and fraudulent transactions.

#### **Phishing Attacks**

Highly personalized and sophisticated phishing attempts targeting customers.

#### **Data Poisoning**

Injection of false data into AI training sets compromising decision accuracy.

#### **Synthetic Identity Creation**

Realistic synthetic identities by combining different elements from various real identities.

#### **Cyber Threats**

Generative AI introduces new potential vulnerabilities that can be exploited by cyber attackers.

#### **Risks**

# Deepfake-based Fraud Risk of convincing deep

Risk of convincing deepfakes videos and audios leading to unauthorized access and fraudulent transactions.

#### **Phishing Attacks**

Highly personalized and sophisticated phishing attempts targeting customers.

#### **Data Poisoning**

 Injection of false data into AI training sets compromising decision accuracy.

#### **Synthetic Identity Creation**

Realistic synthetic identities by combining different elements from various real identities.

#### **Cyber Threats**

Generative AI introduces new potential vulnerabilities that can be exploited by cyber attackers.

#### **Preventive Measures**

#### **Advanced Authentication**

Implement multi-factor and biometric authentication for robust user verification.

#### **Fraud Detection Systems**

Deploy Al-driven fraud detection systems to identify and prevent fraudulent activities

#### **AI Model Explainability**

Prioritize explainable AI models for transparent decision-making processes.

#### **Employee Training**

Provide ongoing training to employees on cybersecurity best practices and ethical AI use.

#### **Robust Cybersecurity Measures**

Implement advanced cybersecurity protocols to protect against unauthorized access and security vulnerabilities

**Risks** 

© 22

