# AI for payments security

Małgorzata Domagała

VP, Products and Solutions

# The constantly shifting payments landscape is making it increasingly difficult to maintain resiliency and deliver a disruption-free payment experience

Three key challenges:

## Complex Payment Rails & Systems

- Need to support all rails (A2A, Blockchain, Cards, Data)
- Shift from batch processing to a 24/7 model
- New, disruptive and more nimble fintechs possessing greater resiliency

## Rising Cyberattacks

The increased weaponization of cyberattacks is expected to see cybercrime costing companies

**$10.5T**

per annum worldwide by 2025[1]

## Evolving Regulations

Developing global realities call for new regulations demanding compliance:

- Digital Operational Resilience Act (DORA)
- U.S. executive order on improving the nation's cybersecurity industry
- 150+ countries have or will enact localization laws, accelerating nationalistic payment preferences

1. CYBERSECURITY VENTURES RANSOMWARE MARKET REPORT. 2022

# What is important in fight for payments security?

## Collaboration

leverage the collaboration of multiple banks in a country, analysing their transaction data, to provide the next level of insights to mitigate against these challenges in a market

## Scale

billions of real time and batch payment transactions, as well as millions of fraud and ML data point each year from numerous countries around the world.

## Power of network

focusing and specialising in developing cross (Intra) bank- network level solutions to mitigate against Scams, Fraud and Money Laundering

## Right use of data

Data used in the right way has the power to transform the fight against fraud, scams, and money laundering

# What is means to use data responsibly?

## Mastercard has committed to a set of data responsibility principles to which we will hold ourselves accountable – PRIVACY BY DESIGN

### Security & Privacy

Best-in-class security and privacy practices

### Transparency & Control

Clear and simple explanation of data collection, use and sharing – giving individuals control

### Accountability

Keeping individuals and their rights at the center of data practices

### Integrity

Deliberate minimization of biases, inaccuracies and unintended harm

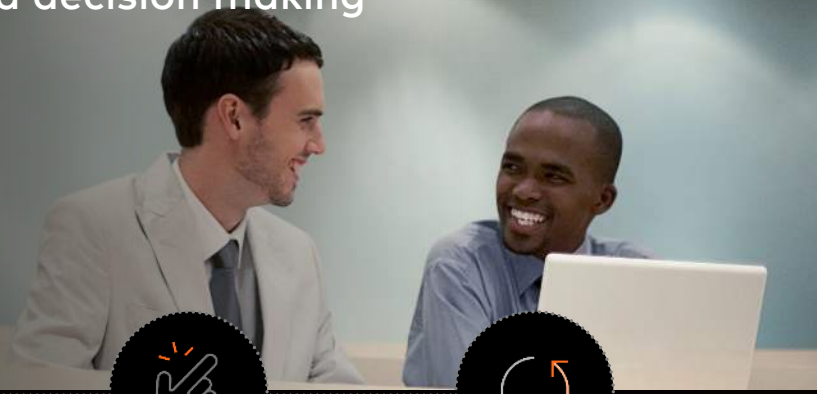
### Innovation

Constant data innovation that benefits individuals through better experiences, products and services

### Social Impact

Using data to identify opportunities to positively impact society

# AI is supposed to help with intelligent and informed decision making



## What is the recipe for the high quality and successful solution?

### World-class AI technologies

State-of-the-art technologies, including: deep neural networks and XGBoost; techniques to better understand behavior, like compound velocities, target encoding, account range profiling; optimization techniques to fine-tune the model.

### Network insights

AI models evaluate thousands of data points from Mastercard's network-level consortium, including historical and real-time merchant insights (such as average ticket, fraud rate, velocity count).

### Brand-agnostic

DI can score transactions not processed by the Mastercard network, allowing issuers to have one solution for an entire portfolio.

### Real-time

<100 milliseconds

Scores are delivered in real-time through the authorization message in under 100 milliseconds.

Scores are also available through Mastercard's hosted portal, The Fraud Center.

### Consistent model refreshes

Model refreshes are provided annually to account for the most recent fraud trends, guarantee stability and improve detection — at no additional cost or effort from the issuer.

**Our example: Decision Intelligence enables issuers to increase approvals on low-risk genuine transactions while reducing transaction fraud through accurate detection**

# Leveraging rich data and network intelligence, AI -boosted platform can provide risk assessment and enable safe and convenient transactions

Transaction Data

MC data

## Transaction Data

information such as amount, currency, date, time, etc.

## Cardholder Data

information such as account number, shipping address, etc.

## Device Data

information such as IP address, device info, channel data, etc.

## Merchant Data

information such as name, category, country, etc.

## Mastercard Network Intelligence

long and short term data such as velocities, ratios, past risk scores, authentication approvals, authorization history, chargeback data, etc.

# Retail fraud is the most common fraud as it targets the weakest link – the end human

The problem: Through social engineering and cyberattacks, fraudsters trick consumers into making payments into accounts they control

- Scams, such as impersonation, involve the legitimate customer making the payment
- With more end point protection in place, fraudsters target the weakest link: the end human
- This leads to challenges when relying on traditional end point/channel protection

# The most significant types of Payee Scams

## TYPES OF PAYEE SCAMS

### Advance Fee Scams

The victim is scammed into paying a fee to release a higher value payment in return.

### Investment Scams

The victim is scammed into investing in a fraudulent investment scheme

### Imposter Scams

The victim is duped by fraudsters pretending to be law enforcement or a bank security department. The victim believes they are sending money to a 'safe account'.

### Invoice/Mandate Scams

The victim is duped into paying an invoice of bill to a known 3rd party by posing as the 3rd party in an email communication.

### Romance Scams

The victim is scammed into paying funds to someone they met online, after being manipulated and lured into a false sense of security

### Purchase Scams

The victim is scammed into paying for non-existent goods.

### CEO/ Business Email Compromise Scams

A fraudster gains access to a business email account and then impersonates an executive (or other person of authority), scamming an employee into issuing a payment to an account they control.

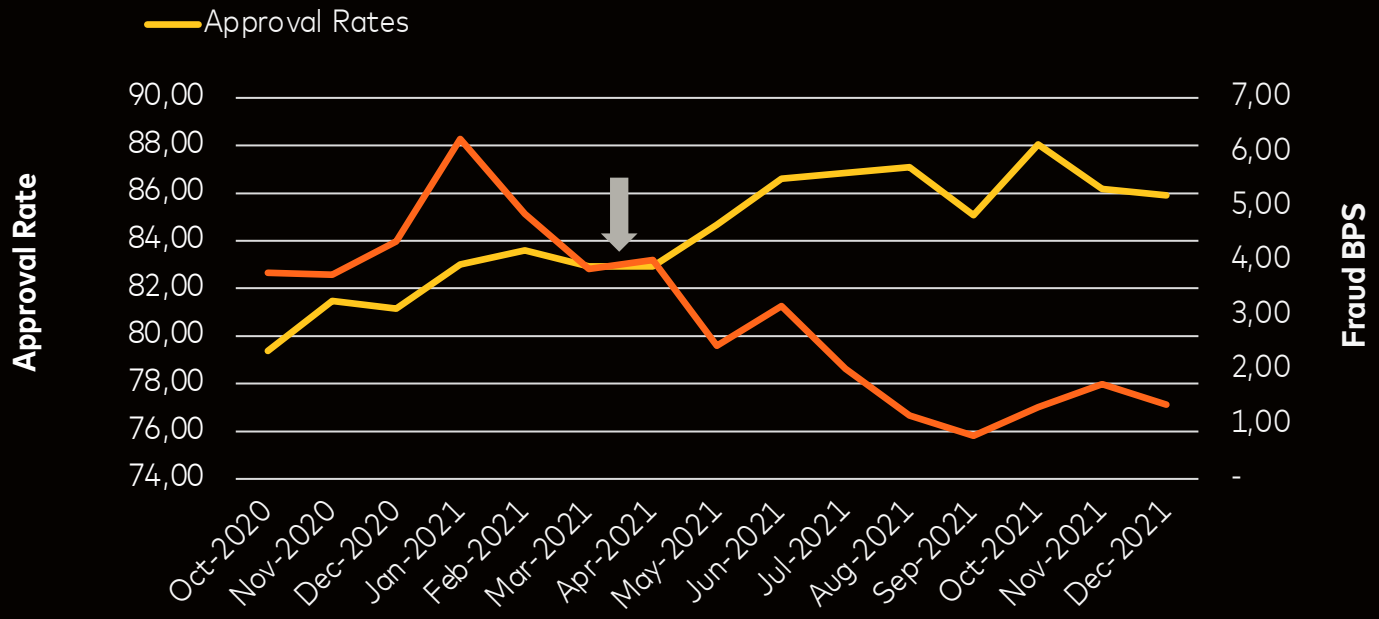
# Rightly used AI can improve approval rates while decreasing fraud bps and does not require the trade off

A large acquirer in MEA has seen significant improvements in both their approval rates and their fraud BPS since implementing Brighterion AI.

## Highlights

- Brighterion AI was implemented in MPGS in Q1/Q2 of 2021
- Between Q4 2020 and Q4 2021, one MEA acquirer saw 7.4% increase in approval rates (81% to 87%)
- Over the same timeframe, this acquirer saw a 2.7x drop in fraud BPS (3.98 to 1.46)

## Large MEA Acquirer[1]




1. *Internal analysis of fraud data reported to Mastercard, June 2022 .*

# Collaboration is critical for impressive results and high impact

## 1) **Pilot Results (Carried out in 2021) – Nine leading UK Institutions**

Preventing the significant threat of P2P payments frauds and scams, by generating risk scores and metadata as part of a real time pre-authorisation / pre transaction flow. Tested with nine FI's in the UK


Value detection at typical false positive levels


Value detection with half the false positives


More missed fraud prevented at half the false positives


Estimated monthly incremental savings

## 2) **Production Results (launched Jan 2023, eight FIs) – Feedback from one leading UK FI**

*"In just 4 months, the bank says it has dramatically increased its fraud detection. Based on TSB's results, the amount of scam payments prevented over a year would equate to almost £100m1 saved across the UK, should their performance be mirrored by all banks". Media release as of 6th July (embargoed until then)*

- "Detect fraud that we have previously been unable to target effectively – these include **purchase, impersonation and romance scams**"
- "The addition of the score has **halved the false positive rate** for some rules in use leading to increased operational efficiencies"
- "Has proven effective combined with other vendors scores (e.g. device, behaviour) has led to the creations of some very effective rules with **good single digit false positive and high detection rates**"

# Legal Disclaimer



Information in this document or in any report or deliverable provided by Mastercard in connection herewith relating to the projected impact on your financial performance, as well as the results that you may expect generally are estimates only. No assurances are given that any of these projections, estimates or expectations will be achieved, or that the analysis provided is error-free. You acknowledge and agree that inaccuracies and inconsistencies may be inherent in both Mastercard's and your data and systems, and that consequently, the analysis may itself be somewhat inaccurate or inconsistent.

The information, including all forecasts, projections, or indications of financial opportunities are provided to you on an "AS IS" basis for use at your own risk. Mastercard will not be responsible for any action you take as a result of this document, or any inaccuracies, inconsistencies, formatting errors, or omissions in this document. Mastercard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, Mastercard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not Mastercard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, Mastercard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third-party patents, copyrights, trade secrets or other rights.

# Thank you

**Małgorzata Domagała**
malgorzata.domagala@mastercard.com