Detect fraud, waste and abuse...before you pay

DATASHEET

"Mastercard has revolutionized a highly rules-based, inefficient payment fraud space by leveraging its AI technology in its card network to identify and stop fraudulent card payments on a real-time basis. The company is now capitalizing on that experience and applying it to tackling FWA in healthcare payments."

Aite Group Report: *Putting AI to Use in Fraud, Waste, and Abuse*

Proven technology

74%

74 of the top 100 U.S. banks use Mastercard AI

2000+

clients world-wide use Mastercard AI

150b+

transactions are processed annually using Mastercard AI

Mastercard® Healthcare Solutions' powerful advanced AI platform detects fraud, waste and abuse (FWA) before claims are paid.

The healthcare industry loses at least $450 billion each year to fraud alone.[1] Payers detect only a small fraction of suspicious claims, resulting in rising healthcare costs and higher premiums for patients. But in an industry where many investigators consider a 20% false positive rate acceptable, Mastercard sees the opportunity for improvement.

With proven AI capabilities used in the financial services industry and by governments around the world, Mastercard can help payers detect erroneous and fraudulent claims — before they reimburse providers.

Healthcare fraud is complex

Healthcare fraud schemes are increasingly complex, and many cannot be detected by payers' current payment integrity solutions or through manual investigation. Phantom billing companies, upcoding, excessive billing, and other schemes are costing payers billions of dollars each year.

Fraudulent transactions come in many disguises, most falling within four categories: claims, providers, members and pharmacies.

Payers may be healthcare insurers, third-party administrators, or government-funded plans like Medicare or Medicaid. In each case, they process claims and approve or decline payments. But there are many steps involved.

Received claims are adjudicated and approved for payment. Some secondary editing may occur prior to payment, and coding errors or waste may be noted. Once approved, payers remit funds to the claimant. But it's only after payment has left the claims ecosystem that fraud analysis usually begins.

Whether it's picked up by manual review or legacy software solutions, identifying fraud on already approved and paid claims is a real problem. Many of these post-pay solutions are labor intensive and have high levels of false positives.

Fragmented legacy claim management systems make the task even more difficult. It comes as no surprise that payers' fraud investigators are overwhelmed with alerts and struggle to keep up. As a result, only five to ten percent of suspicious or fraudulent claims paid out are ever recovered.[2]

The bottom line for payers: complex contracts, coding, management costs and regulations are limiting profits and compressing margins.

---

1   CMS.gov, "National Health Expenditures 2022 Highlights," (accessed January 29, 2024).
2   NHCAA

From pay and chase to prevent and save

Imagine being able to:

Assess new providers to reduce onboarding risk

Continuously monitor provider behavior and risk levels

Manage daily transaction fraud risk in real time

Address omnichannel fraud across vectors, channels, transactions

Mastercard Healthcare Solutions: revolutionizing AI that's efficient and scalable

Mastercard Healthcare Solutions is building on its long-held success in healthcare payments to address FWA. With the same advanced artificial intelligence it uses to prevent fraud for the financial services industry, Mastercard helps payers detect erroneous or fraudulent claims — before reimbursing providers. AI models can be tailored to identify healthcare claims fraud, prescription abuse, upcharges, phantom billings, and many other FWA challenges.

Detect more fraud—before reimbursing healthcare claims

At Mastercard, fraud detection begins the moment a claim is received for analysis. Processing more than 1 billion transactions per day, Mastercard's AI analyzes thousands of data points and hundreds of decision points to flag suspicious activity. These same tools are applied to healthcare claims data, identifying anomalies that require investigation.

Mastercard leverages its proven AI technology to bolster detection of FWA. AI creates prospective (pre-pay) models built by identifying anomalies found in historical claims data (post-pay). The pre-payment model identifies FWA before the payer sends good money for bad claims, significantly reducing the need for inefficient pay-and-chase activities.

Since the technology enables live updates to existing models based on real-time claims experience, Mastercard's AI reduces "digital noise" and automates some of the manual processes involved in maintaining and updating existing rules-based technology.

As a result, false positive alerts are greatly reduced, anomaly detection is significantly increased, and payers' investigators can focus on highly likely fraud. Mastercard technology is efficient, scalable, and provides unprecedented detection.

How it works

1. **Provider updates PMS, codes claim**

2. **Post-pay trend analysis**

   Mastercard AI analyzes 24 months of data, identifies suspicious claims and automatically creates new models to enhance both pre- and post-payment

3. **Payer sends payment and claim file**

4. **"Prevent & Save" pre-pay analytics**

   Leveraging post-pay analytics, Mastercard AI applies new learnings to future claims before they are paid, resulting in even more savings
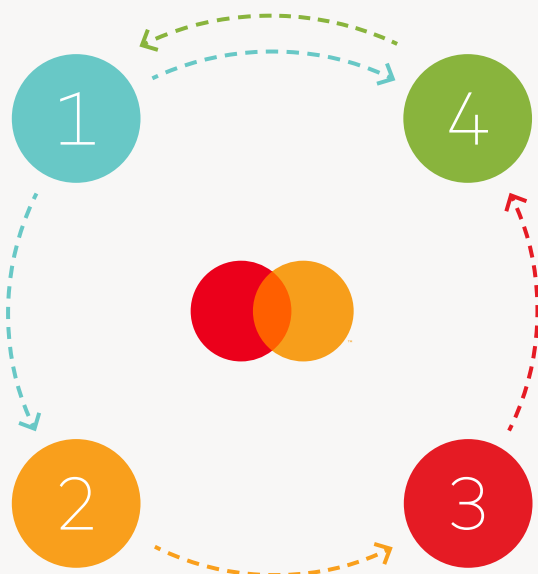
Our technology

Any data, any format

Current and future data can be received from any source, in any format, and be enriched using both AI and machine learning. Unsupervised and supervised learning improve outcomes over time, creating AI models that grow and mature with the evolving behaviors of fraudsters.

Distributed AI storage

Mastercard's AI for fraud, waste and abuse brings a powerful, distributed file system specifically designed to store knowledge and behaviors. This distributed architecture allows lightning speed response times (below 10 milliseconds) as well as end-to-end encryption and traceability. The distributed architecture allows for unlimited scalability and resilience to disruption as it has no single point of failure. Our customers benefit from 99.99% average uptime.

Smart Agents: moving beyond rules-based AI

Mastercard's Smart Agent technology creates an end-to-end suite of profiling and modeling capabilities that continuously adapt and improve results. This seamless combination of advanced AI tools delivers personalized decisions. Evolving models scale with your data, increase detection rates, and decrease operational costs and false positives.

Legacy solutions pull from a small set of AI tools, creating a one-size-fits-all solution.

How Smart Agents work

1. Data collection
Collect data on individual entities (e.g. users, accounts, devices) directly from customer data streams in real time

↓

2. Data tracking
Create and associate unique identifiers to each entity to track over time

↓

3. Data enrichment
Consolidate entity data into a single dataset, while adding or removing data fields based on statistical relevance

↓

4. Model development
Build, train, and iterate AI model to identify patterns based on incoming entity behaviors

↓

5. Entity scoring
Generate a real-time score for each individual entity, which feeds into the customer's decision engine (e.g. for relevant targeting, risk flagging)
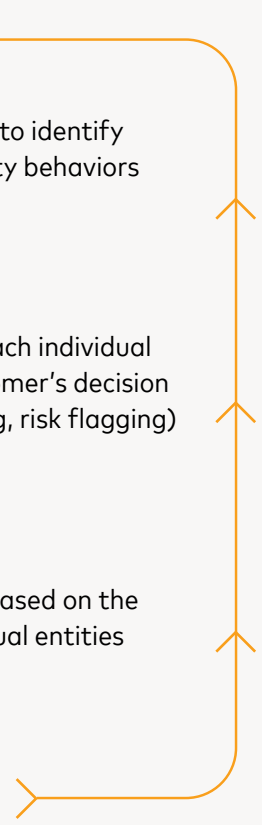
↓

6. Adaptive learning
Refresh the model's knowledge based on the evolving data patterns of individual entities

↓

New entity data feeds back into model development

From data to intelligence in just a few weeks with AI Express

Experience the benefits of Mastercard's AI technology in a matter of weeks. AI Express provides the specific tools to solve your unique challenges. Our experts will work with you to develop a deep understanding of your needs and give you hands-on experience with our AI tools. We will help you collect data, collaborate on outcomes and develop your AI model in less than two months, providing the quickest time to value in our industry.

We are so convinced you'll be happy, we build and test your solution before you need to commit.

Six phases of engagement from discovery to deployment

1 **Business understanding:** determine business objectives and success criteria

2 **Data understanding:** collect, describe, explore and validate data

3 **Data preparation:** select, clean, construct and integrate data

4 **Modeling:** Select modeling techniques and determine model building iterations

5 **Evaluation:** evaluate results and review processes to determine next steps

6 **Deployment know-how:** review deployment options and create a high-level deployment plan

6 - 8 WEEKS

● **MASTERCARD & CUSTOMER** ● **MASTERCARD** **CRISP-DM METHODOLOGY**

Features and benefits

FEATURE	BENEFIT
Created by an experienced, innovative company with proven fraud prevention technology	Have peace of mind, security and longevity
Provides accurate post-pay data analysis to "prevent and save"	Get early ROI: detect and prevent fraud before claims are paid to avoid "pay and chase"
Complements and supports special investigation units (SIUs) and other payment integrity partners	Have increased operational efficiency: Focus on actual FWA and complex cases
Combines the right tools to create a unique AI model for each customer's needs	Solve targeted business problems
Receives any data, in any format	Get instant insights and efficient claims processing
Allows real-time insights: upload time less than 10 ms (high throughput response time)	Prevent more fraud with proactive defenses that adapt to change in real time
Provides extraordinary scalability, twice that of our closest competitor (Aite Group analysis)	Have a technology that grows with your business, future-proofing operations
Builds your unique AI model in weeks with AI Express	Be ready to deploy and see immediate ROI
No database requirements: our distributed file system guarantees no single point of failure	Stay immune to failure and disruption
Automatic updates to the AI model based on actions taken, identifying changing behaviors	Be ready to adapt and stop ever-changing fraudulent behavior

To learn more contact one of our **AI experts** →   Visit our **website** →