E-BOOK

The power of today's market-ready AI to reduce transaction fraud

Contents

Transaction fraud management: the evolution of AI

2030 outlook[1]

$79t

Total payment card volume

$49b

Lost to payment fraud

73%

Estimated CNP fraud in 2023[2]

Transaction fraud is evolving, but so are the artificial intelligence (AI) solutions combating it. Today's market-ready models address transaction-level fraud and are ready to use in any market or region in the world.

Transaction fraud is one of the biggest risks for players in the payments industry. Acquirers are liable for fraud while PSPs, payment facilitators and merchants are concerned with approvals, wanting to ensure a frictionless customer experience. By 2030, when total payment card volume is expected to hit $79.14 trillion worldwide, Nilson[1] predicts the payments industry will lose an estimated $49.32 billion to payment fraud. In 2023, an estimated 73% of card fraud was incurred through card-not-present (CNP) transactions.[2] Even as fraudsters develop new schemes, the increasing efficacy of artificial intelligence (AI) models that identify fraud makes them more responsive and highly accessible.

But not all AI systems are equal. Acquirers and payments processors want more data points to analyze in order to increase fraud detection, such as customer data and mobile bank sessions. they want real-time analytics and faster transactions. In short, they want their AI to do more.[3]

Even in the age of modern AI, cumbersome model building, data silos, customer data requiring deep integration, heavy customizations and long cycles can bog down deployment and eventual results.

Modern models are developed with international anonymized and aggregated transactional data. They are fast, robust and experienced in recognizing fraud patterns from across the global marketplace. As transaction fraud continues to evolve, the model learns and incorporates this new information into its fraud prevention capabilities.

Global transaction data

Training of powerful, highly scalable AI models

Global market-ready acquirer solutions

62%

Of acquirers want additional analytics

Acquirers said increased detection rates, fewer false positives and explainability were also key

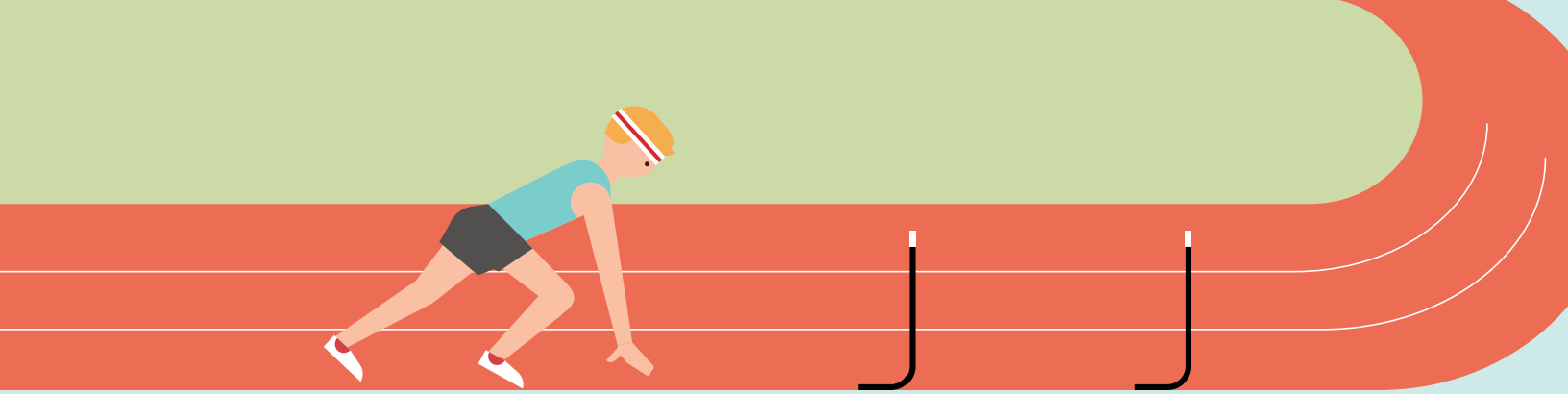
AI innovations for transparent problem solving

Using AI to detect and prevent transaction fraud isn't a new concept. Financial institutions and merchants have been using a variety of AI solutions for many years. Acquirers say additional analytics to detect fraud will be an important factor in their choice of an AI solutions provider. They also said increased detection rates, fewer false positives and explainability were key.

The most common challenges when using AI for transaction fraud are:

- AI implementation may take months or years
- Increased and changing transaction fraud
- Global compliance requirements
- Black box, unexplainable models
- The need to reduce fraud while increasing approval rates
- The expense of AI balanced with ROI
- That AI can be difficult to use
- Excess friction
- High incidence of false positives

These innovations provide financial institutions and merchants with AI models trained on a broader range of fraud patterns and are ready to go live in a fraction of the time needed for customized models.



How market-ready models are poised to solve today's challenges

Today's innovative market-ready models are true turnkey solutions. The models are production-ready and deployment can begin immediately.

The problem of increased and changing transaction fraud is solved with models that can recognize anomalous patterns in real time as a result of their training.

In the past, users struggled with the ease of use. Modern solutions have advanced APIs that are user friendly and feature customizable attributes.

1. AI implementation with a lighter lift

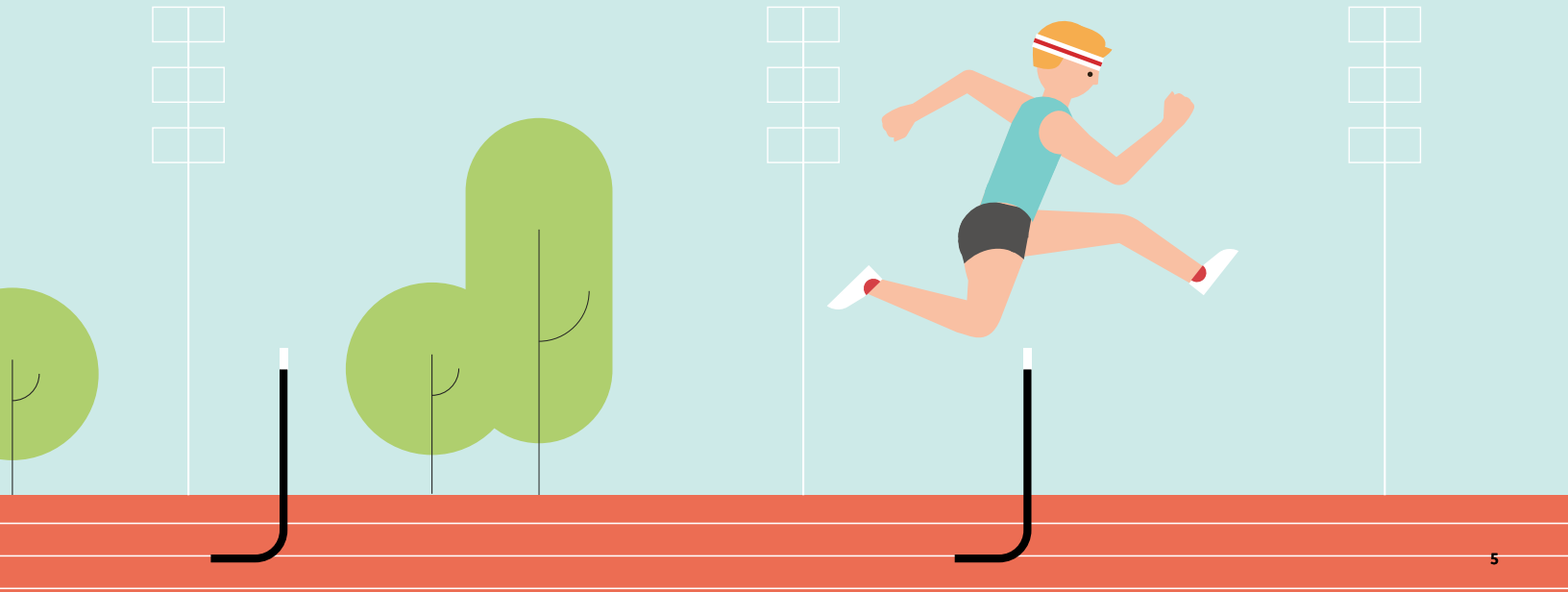
By nature, market-ready models are use case focused. When built and trained by companies with extensive use case experience, the model is ready to deploy quickly with the transaction data provided by the customer.

The model's training is not unlike that of an Olympian when compared to a recreational athlete. The weekend warrior is often self-taught or has trained with friends. When they set a new goal or experience an injury, they seek further training for improvement.

The Olympian, on the other hand, has been trained for their challenge by the best coaches in the world. They have encountered each competitive challenge and repeated the correct action hundreds or thousands of times. Their muscle memory leads them to make the right decision, or alter course based on previous learnings. In time, they become faster and more accurate.

The formula for a winning AI model includes providers with extensive AI model-building experience and access to the right data sets. Models may be trained with anonymized third-party data (such as credit scores) and global payments network data. Small samples of the acquirers' transaction data will be used to initiate the model at deployment.

Being able to immediately deploy out of the box saves both time and money.



Well-trained models enable pattern recognition that makes transaction decisions in the moment without having to draw data from its own or other networks.

2. Models evolve with increased and changing transaction fraud

Digital disruption caused by COVID-19 increased transaction volumes as shoppers turned to online ordering using credit, debit and prepaid cards. As a downstream result, more than nine out of ten acquiring banks experienced increased fraud.

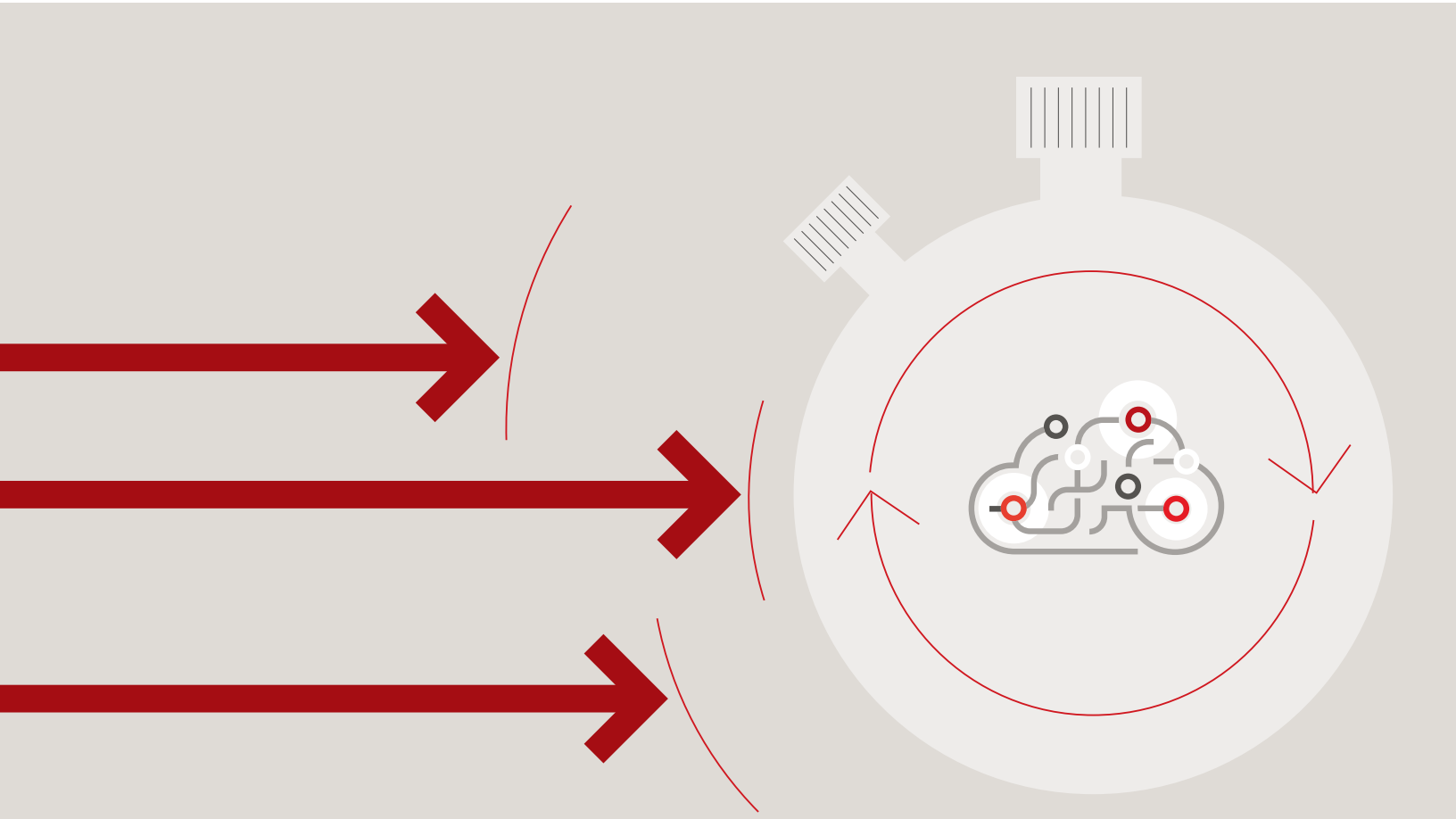
Fraud has always followed the marketplace and, naturally, that hasn't changed. It evolves with trends, modes of purchase and opportunities for new purchasing streams. Cyber criminals follow these trends and access AI solutions designed to collect user credentials and commit transaction fraud attacks.

When acquirers use AI trained with anonymized and aggregated transactional data from around the world, it is exposed to patterns of legitimate and fraudulent transactions from around the globe. Recognition of fraud, regardless of sophistication, is more accurate and efficient. It then improves its already highly-performant fraud prediction as it learns from the business's daily transactions.

Speed matters in self-learning AI

Well-trained models enable pattern recognition that makes transactional decisions in the moment without having to draw data from its own or other networks, which causes network latency. Low latency is critical for high-volume, high-speed real-time transactions and analytics.

Processing speed is a critical aspect of self-learning. Low latency enables AI's self-learning function to update pattern recognition to prevent emerging fraud. When an attack launches, merchants and acquirers need confidence that an AI solution can react immediately to secure the ecosystem.

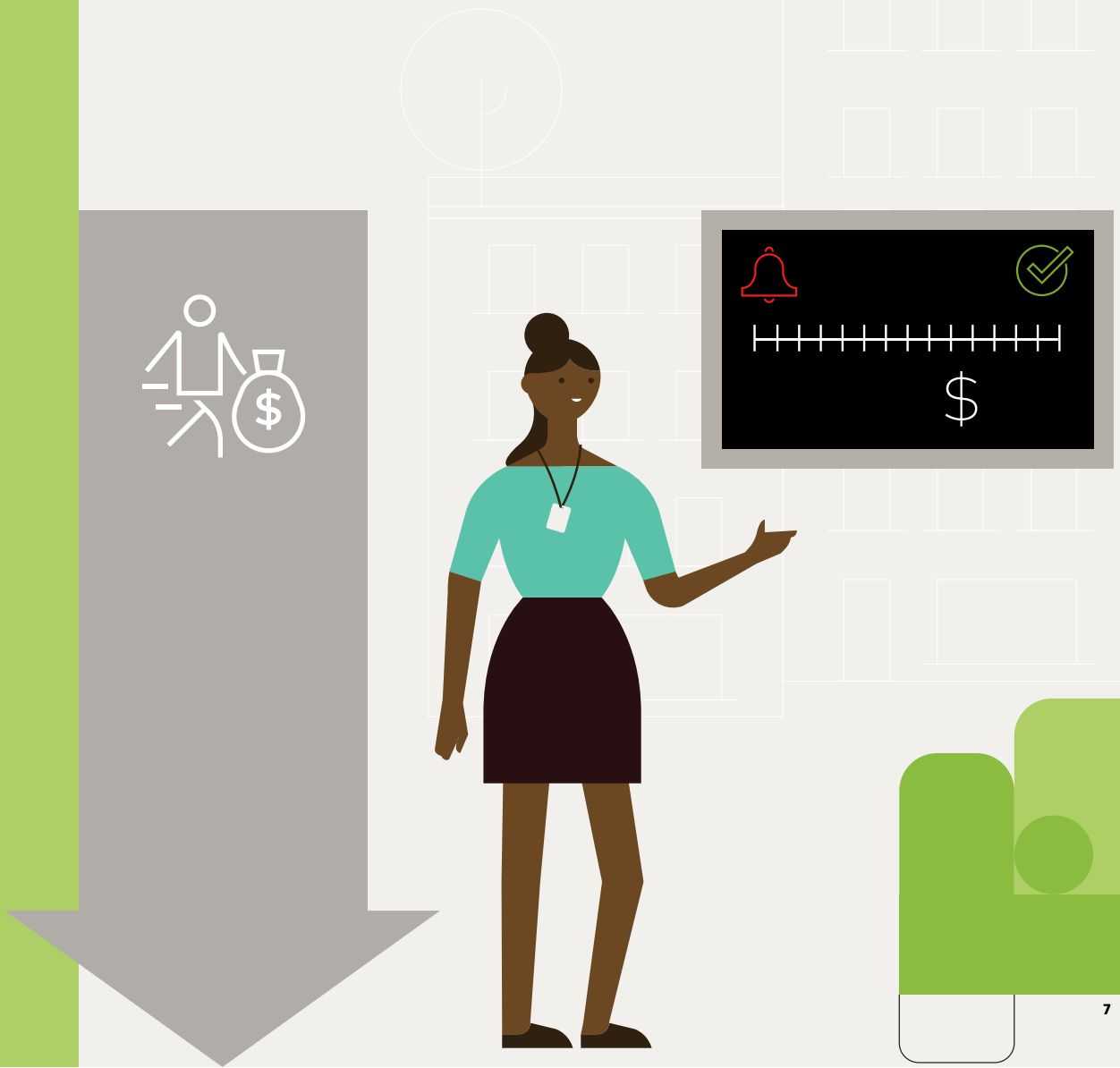


3. Reduced fraud and increased approvals = improved ROI

In 2022, global card fraud reached US$49.15 trillion, directly affecting acquirers' profitability.[4] However, the goal of increased approvals must be balanced with reduced fraud to determine a stabilized ROI.

Today, financial institutions and merchants can choose the decline threshold that best fits their risk appetite, taking into consideration the trade-off between fraud detection rates and false-positives rates. A higher score potentially means more risk, so an organization might choose a lower threshold to better identify fraud, a higher threshold to lower false positives, or maximize total ROI by taking into consideration both the cost of fraud and the cost of false positives to the bottom line. Thresholds can be adjusted moving forward to fine-tune the model performance to each business's needs.

As the model continuously learns and updates based on anonymized and aggregated transactional data, the solution continues to improve by recognizing patterns of complex fraud. Each transaction enables real-time decision-making while contributing to accurate fraud predictions for future events and decreasing operational costs and false positives.



Good explainable AI is simple to understand yet highly personalized for each given event.

4. AI models must include explainability

While explainability was not the number one concern for acquiring banks, Fintech Nexus reported that 27% of bank executives feel explainable AI is a barrier barriers to wide adoption to meet the challenges of fraud and money laundering.[5] Being able to understand how the AI model makes decisions builds trust in fraud fighting technology.

Traditional AI models are developed and trained with historical data and learn to predict events and score transactions based on past events. Once the model goes into production, it receives millions of data points that interact in billions of ways.

The problem is that traditional machine learning models make these decisions in closed environments, understood only by the teams that build them.

Preferred market-ready models are developed using explainable AI (sometimes known as "white box" models), assigning reason codes to decisions and making them visible to users. Users can review these codes to both explain decisions and verify outcomes.

The power of global transaction data

Results

2-3x

Increase in fraud detection

7.4%

Increase in approvals

Using market-ready Brighterion AI, one acquirer saw an increase in fraud detection of 2–3x and an increase in approvals of 7.4% in the first year.

Mastercard's market-ready Brighterion AI models revolutionize the way transaction-level fraud is detected and managed. Our data scientists and innovators have built and trained these new models with anonymized and aggregated Mastercard network data. Together, Mastercard and Brighterion AI address financial institutions' and merchants' pain points head-on.

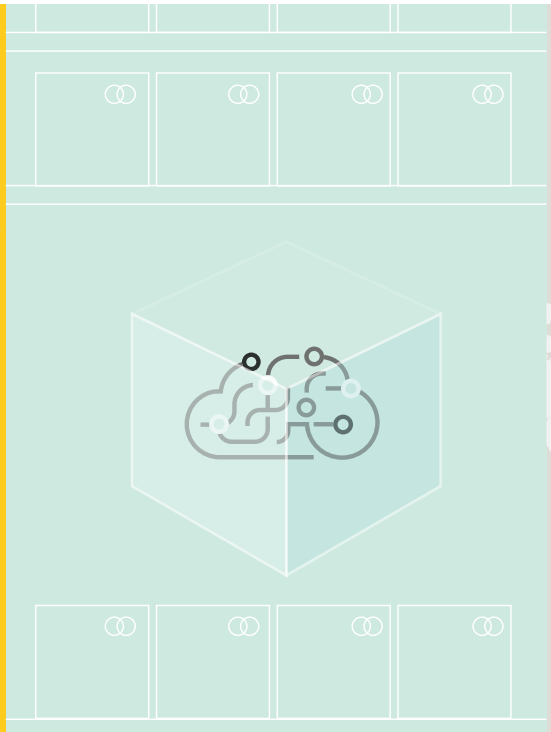
Out-of-the-box transparency

Regulatory compliance and explainability are built into the model based on Mastercard's worldwide expertise. Organizations can be confident that models meet global compliance requirements.

Explainability is a feature of model building that provides insights by categorizing anomalous transactions to certain high-risk patterns. Transactions are assigned a reason code that most accurately categorizes the transaction, and that reason code is associated with a summary and a set of conditions.

The summary contains easy-to-understand fraud patterns, such as "suspicious card testing activity," and includes a few rule-like conditions that help classify the transaction to the reason code, such as "card has low authorization amount" and "no transactions on this card 4-8 weeks ago."

Fraud analysts are familiar with the "if-then" conditions of fraud rules, so by providing a clear classification of the transaction using conditions, Brighterion AI provides insight in a format that is familiar and easily understood.



Intuitive, flexible and easy to use

Brighterion AI's fresh, modern and configurable interface enhances usability and integrates easily with existing solutions. Customers have the option to use Rules Management, Case Management and Business Insights modules.

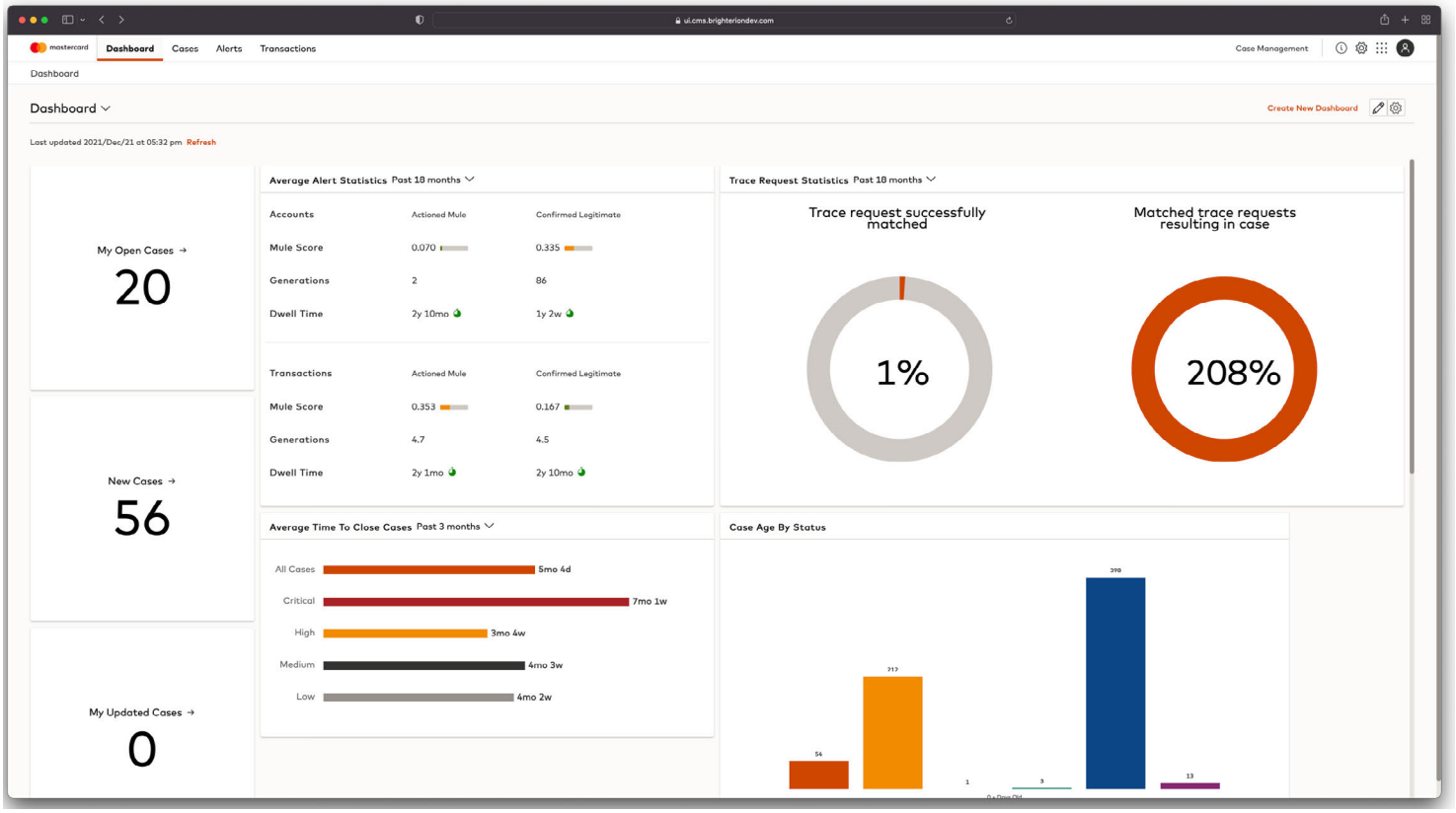
The cloud-native platform, delivering a remarkably low latency of 100-120 ms, can also be deployed on-premise with a speed of just 10 ms.

<10 ms

On-premise

100-120 ms

In the cloud



Key features of market-ready Brighterion AI

Rules Management module: writes, tests and manages business rules in an intuitive user interface, including:

- Rule creation and editing
- Profile transactions
- Rule testing
- Rule performance reporting

Case Management module: investigates and evaluates flagged transactions in an intuitive user interface, including:

- Case management and administration
- Users, groups and roles
- Reporting
- Audit and traceability

Business Insights module: real-time business intelligence and customizable reports on the go, including:

- Self-serve analytics
- Standardized reporting
- Actionable intelligence
- Aggregated metrics for merchant portfolios

~30

Data elements to integrate

Immediate deployment and simplified integration

A key barrier to AI adoption is the complexity of integration. Market-ready Brighterion AI solves that problem. In the past, businesses were required to extract hundreds of types of labeled data elements for training the model. By eliminating the need for that historical acquirer data, Brighterion AI reduces the requirement to around 30 data elements, with the option for customers to send additional data elements to be used in the Rules, Case Management and Business Insights modules. Models are production-ready out of the box.

Acquirer integrates data flow via API

Acquirer sends data to initialize model while team customizes API interface

Brighterion returns risk scores to acquirers via API

Transaction Fraud Monitoring's ease of use makes it an ideal value-added product for financial institutions to offer small-business customers.

Summary

The world quickly pivoted to an e-commerce marketplace in 2020. Parallel to that increase, transaction fraud grew in both volume and ingenuity.

Financial institutions and merchants need fraud prevention tools that scale with their quickly growing businesses while continuing to process large volumes of transactions and prevent fraud. Today's AI solutions also must evolve to detect transaction fraud while ensuring acquirers adequately manage risk and optimize their ROI.

Market-ready AI models built for transaction fraud and trained on global anonymized and aggregated data are more robust and experienced than any legacy AI solution. Informed by fraud pattern recognition from Mastercard's global transactions, Brighterion AI is the most advanced AI fraud prevention tool available.

These innovations provide acquirers with AI models trained on broader experience and are ready to go live in a fraction of the time needed for customized models. Acquirers should expect no less.

---

1. NILSON, *Nilson Report Issue 1209: Card Fraud*, December 2021.
2. Insider Intelligence, *Card-not-present fraud to make up 73% of card payment fraud*, (accessed April 2024).
3. Finextra, *Seeking Approval: Acquirers vs. Transaction Fraud*, October 2022.
4. Nilson Report, *Issue 1254*, December 2023.
5. Fintech Nexus, *AI perspectives: Transaction Fraud*, 2023.

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