BECKER'S HEALTHCARE

mastercard

# Staying one step ahead of fraud, waste and abuse

## How healthcare organizations are leveraging AI and advanced technologies

Frequent, high-profile headlines about healthcare fraud have become the norm, and it's no surprise since cybercriminals and other bad actors are continually evolving their methods for perpetrating crime. While high-dollar cases typically get the most attention, healthcare organizations know the reality: they lose money whenever fraud occurs and even small losses can quickly add up.

*Becker's Hospital Review* recently spoke with two cybercrime and fraud experts from Mastercard about the potential for artificial intelligence to uncover fraud, waste and abuse in the healthcare sector:

- Amyn Dhala, Chief Product Officer, Brighterion, a Mastercard company
- Tim McBride, Director, Healthcare Product Development and Innovation, Mastercard, AHFI

### Health plans are overwhelmed by fraud and the pandemic has only exacerbated the situation

Given the sheer volume of fraudulent activity and improper healthcare payments, it's simply impossible for health plans to pursue every instance of potential fraud. Health plans are also strapped for resources. As a result, it is only logical that high-dollar cases are the highest priority. Many lower-value cases fall by the wayside, but these can have a broad impact on patients or the quality of care.

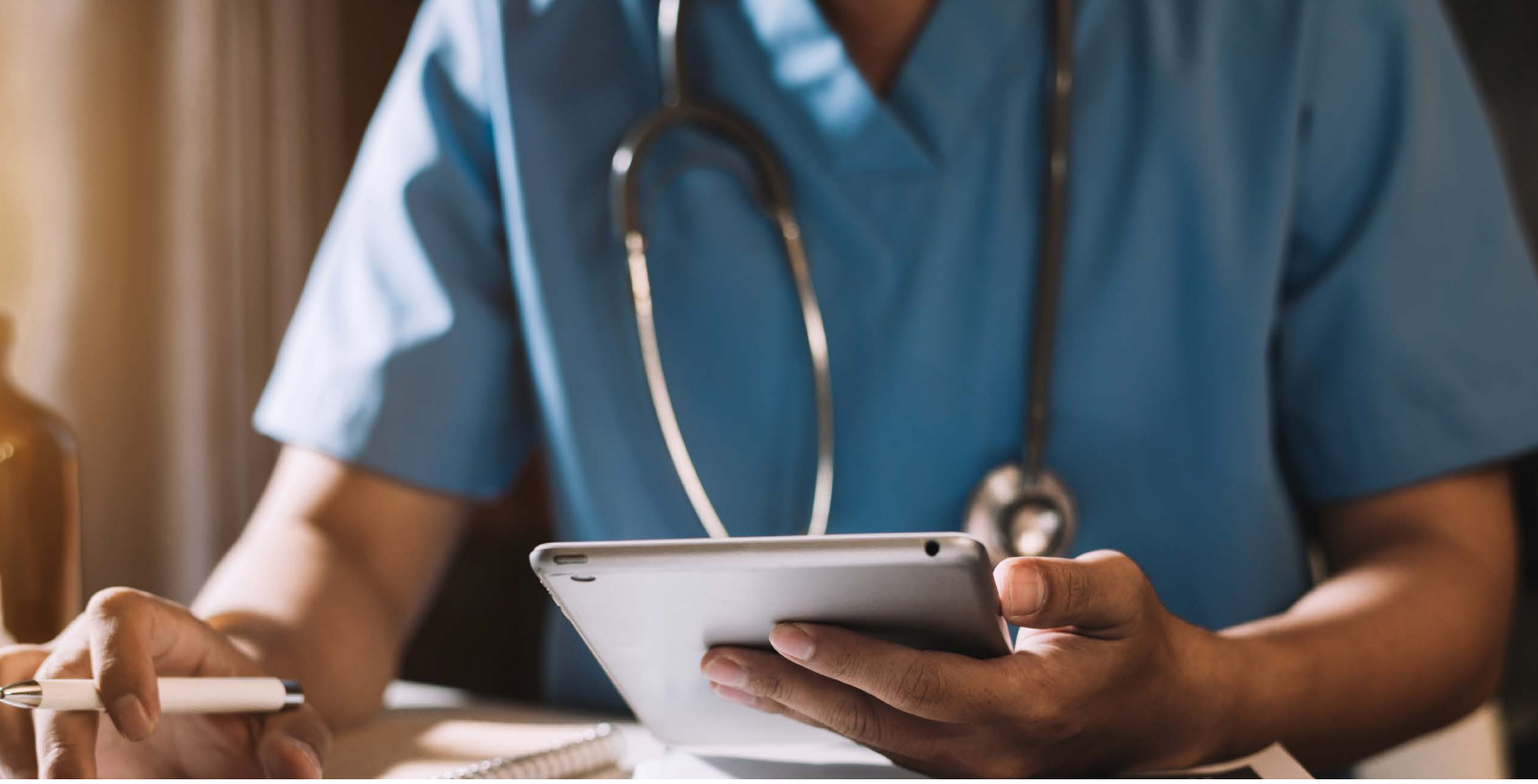
Unfortunately, the COVID-19 pandemic opened the door for even more cybercriminals to increase their fraudulent activity. As telehealth requirements were relaxed and more people worked from home, it became easier for fraudsters to find ways to submit improper healthcare claims. Many new schemes emerged, such as increases in applied behavior analysis therapy claims.

Over the last two years, special investigations units at health plans and within the law enforcement community have seen growing backlogs of fraud cases. The pandemic has highlighted the need for healthcare organizations to shore up cyber vulnerabilities and prepare for potential breaches.

### Many organizations use rules-based fraud protection, but this approach has significant drawbacks

Rules-based fraud protection uses algorithms to identify and alert organizations about patterns or behaviors that are indicative of fraud, waste and abuse. Although rules-based systems are effective, they are expensive to develop and maintain. In addition, they are rigid and limited in reach since they require known patterns of behavior.

Business rules and algorithms can't work unless the problems, patterns or behaviors that organizations are looking for have already occurred. This unfortunately makes it impossible to protect against new and unfamiliar methods of fraud, waste and abuse.



To develop rules, teams must first track data and create hypotheses. This can be a costly and arduous process. Often, rules and algorithms work very well in the beginning to prevent fraud. Over time, however, rules must be maintained to ensure that they remain relevant and effective.

"In the beginning, algorithms and rules find all kinds of fraud," Mr. McBride said. "You're opening and closing cases and preventing fraud. It's all rainbows and butterflies! If you don't invest in rules, they can become stale and quit working altogether as fraud techniques evolve. When fraudsters change their schemes, health plans are on the hook to update their rules or create entirely new ones."

This is problematic since rules development is both expensive and time consuming. Another major disadvantage of algorithms and rules-based systems is they often generate false positives. As a result, organizations must spend valuable time and resources sifting through erroneous alerts, in their efforts to get to the information that matters.

## Leading healthcare organizations are turning to AI for data protection and fraud prevention

With AI solutions like Brighterion from Mastercard, dependence on business rules and algorithms for fraud detection can be reduced, augmented or even completely eliminated.

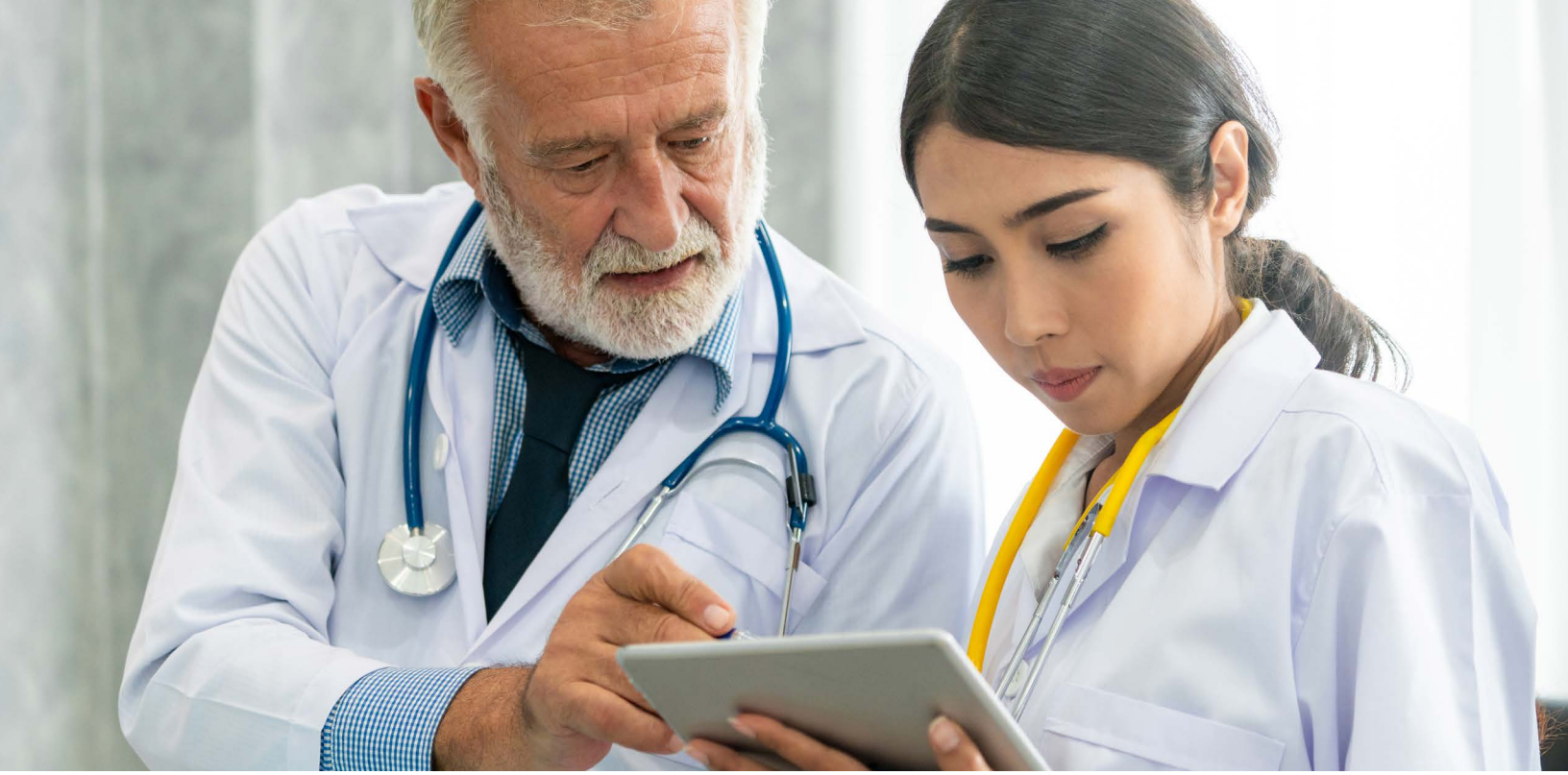
"We've trained Brighterion's artificial intelligence ensemble model for healthcare fraud, waste and abuse to understand today's fraud schemes, as well as institutions' decisioning processes," Mr. McBride said. "This enables our models to detect more fraud with incredible accuracy."

Brighterion's technology performs a 1:1 comparison for each data point, creating unparalleled analysis on every claim presented to the model. This delivers insights that rules and algorithms can't provide.

In addition to detecting anomalies in data ecosystems, Brighterion finds and alerts on even minor differences that fraudsters may experiment with when trying to evade traditional hard-coded rules or algorithms. Brighterion's robust ensemble model can detect healthcare fraud at the claim and provider levels in real time.

"This enables payers to evolve their fraud-fighting strategies to be more like those used in the financial services industry — that is, real-time interventions for each claim, rather than letting claims build up," Mr. Dhala said.

The insights delivered by Brighterion are translated to a score, which gives organizations the confidence to automate decisioning above certain thresholds. Automation frees time for investigators to focus on the higher-value or more complex cases they may have put on the back burner, while sorting through the large volumes of false positives generated through rules-based systems.



## When adopting AI for fraud detection, healthcare leaders must be aware of common obstacles and best practices

As health organizations begin implementing AI-based fraud prevention and protection solutions, many find that their contracts don't allow for AI-based decisioning and denials. It's important to ensure contracts are inclusive of AI insights and scoring as a tool for denials.

In addition, data and behaviors may not be labeled, which makes it more challenging to train AI models and measure their efficacy. It's crucial to first identify the organization's use cases, based on data availability, problem statements and goals. Next, teams must analyze the quality and completeness of data sets intended for use in modeling. This includes labeling the behaviors that AI-based systems need to learn.

On the people side, the importance of change management can't be overlooked. If employees don't understand why AI systems are being deployed, they may show significant resistance or refuse to adopt the solutions altogether. Before, during and after integration of AI technologies for fraud detection, it is essential to be inclusive of all stakeholders. Leaders must emphasize that AI is meant to augment decision-making and to provide new insights. The goal is for all employees to view AI as a companion, rather than a replacement.

## Conclusion

The problem of fraud in healthcare shows no sign of abating. The pandemic, however, has generated important lessons for leaders. Savvy organizations are transitioning their fraud detection and prevention strategies away from rigid rule-based systems to more powerful, AI-based solutions. With tools like Brighterion, health plans and health systems will be better prepared for the next unexpected event on the horizon — whether that's a pandemic or something else.