Fight Financial Crime with Intelligent Anomaly Detection

Table of Contents

Introduction

In today's increasingly digitized economy, financial institutions face significant potential losses from fraudulent transactions. Evolving digital transaction channels such as mobile wallets and apps, ATMs, and remote desktop terminals have translated into less face-to-face time with customers and more opportunities for fraudsters.

Faster payment processing also presents greater fraud risk. KPMG's inaugural Global Banking Fraud Survey noted: "Faster payments processing can pose a challenge with less time available for banks to scrutinize transactions for fraud. Faster payments also pose the risk of reduced fraud loss recovery rates due to the velocity of payments if funds are transferred through multiple accounts in seconds and offshore."

At the same time, the consumers that financial institutions are trying to protect from fraud are increasingly dissatisfied. Poor customer experience results from transactions flagged as potentially fraudulent when they are not. These false positives are a frequent problem.

In 2020, GIR outlined the scope of the false positives problem, stating: “Despite decades and billions of dollars in industry investment, over 95 percent of system-generated alerts are closed as ‘false positives’ in the first phase of review, with approximately 98 percent of alerts never resulting in a suspicious transaction report (STR). Reviewing false positive alerts costs billions of dollars in wasted investigation time each year. The greater the number of false positives, the more expensive it is to onboard customers and process payments. They also expose financial institutions to fines and reputational damage.”

McKinsey recently underscored the financial services enterprise conundrum. Namely, to achieve speed, agility, and flexibility while continuing to manage the scale, security standards, and regulatory requirements. Financial institutions must balance fraud risk mitigation and customer experience, and that balance is difficult to achieve.

Historically, financial institutions have relied on conventional fraud solutions that use rules to flag anomalies for trained fraud teams to review manually. In addition to producing high volumes of false positives, this approach lacks the real-time immediacy needed for fraud detection in a world of near-instantaneous payment processing. In addition, rule-based systems can only respond as programmed, and fraud methods are evolving much faster than new rules can be created.

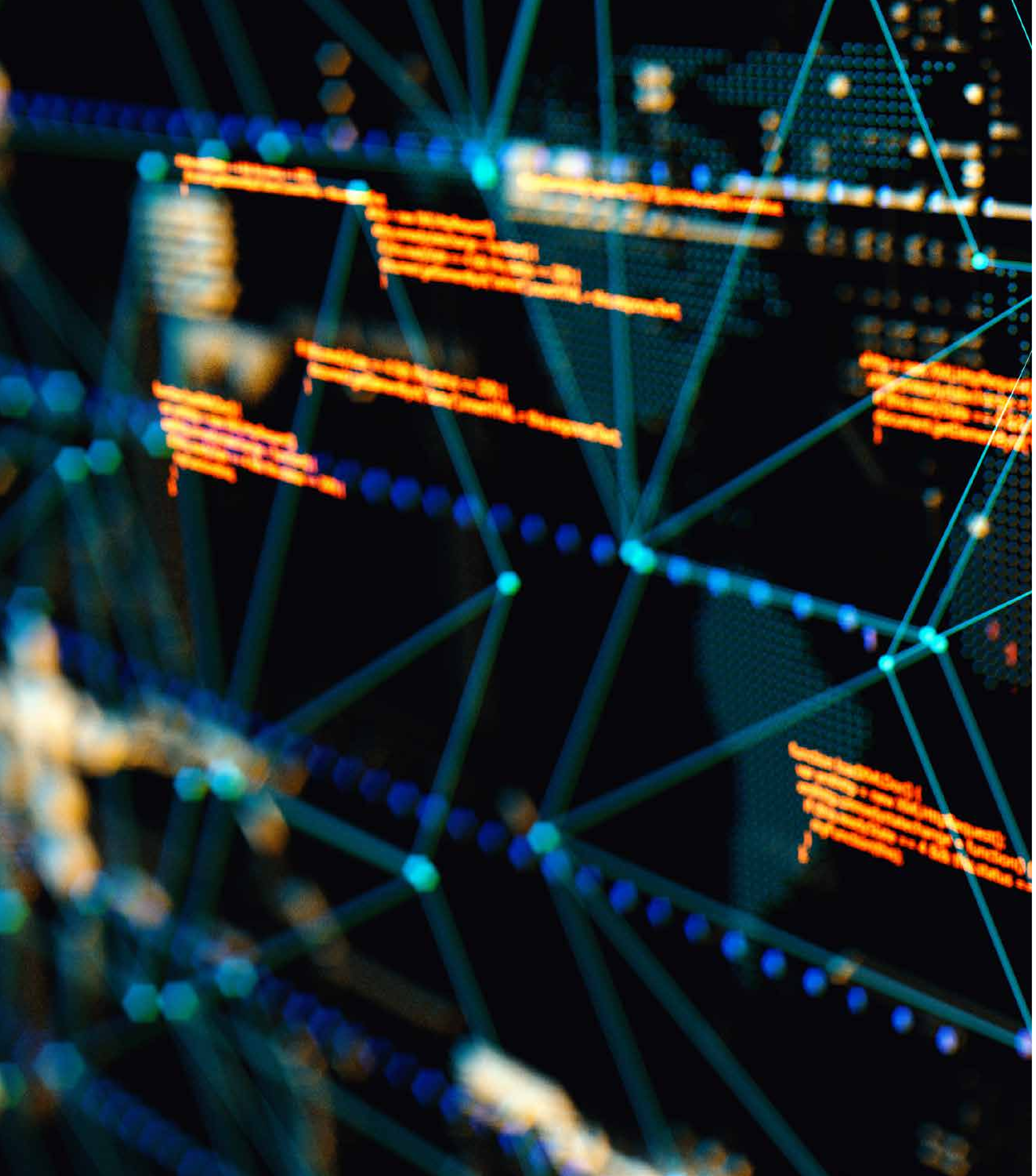
However, according to the GIR report, regulators are increasingly encouraging the use of innovative technologies such as artificial intelligence and machine learning to enhance transaction monitoring capabilities and maximize compliance resources.

To effectively combat fraud, today’s financial institutions need a fraud detection solution that offers:

- Speed, agility, and flexibility combined with the security of a core banking system
- High accuracy and low false positive rates
- Real-time connectivity to all transaction channels
- Hyperconverged analytics powered by advanced artificial intelligence and machine learning

This ebook explores:

- Common anomaly detection methods
- The need for intelligent anomaly detection in financial services
- The vital role of artificial intelligence (AI) and machine learning (ML) in anomaly detection
- Steps to reduce false positives and strengthen a financial institution’s fraud defense mechanism



What Is Anomaly Detection?

An anomaly is an unforeseen variation or deviation from the expected pattern in a particular dataset, which indicates one or more input conditions have changed. Anomaly detection is the practice of identifying anomalies within given data samples. It helps prevent fraud, security breaches, operational performance issues, and other undesirable events by determining when something has deviated from what is considered "normal" and triggering the appropriate response.

Companies that process massive amounts of data, such as financial services institutions, use anomaly detection to flag transactions that break from expected patterns or deviate from previously observed behaviors. Transactions worth trillions of dollars execute every minute in the financial services sector, and identifying anomalies in real time can prevent monumental or catastrophic losses.

Common Anomaly Detection Methods

Financial services organizations have been using technology enabled anomaly detection techniques for decades. Some of the most popular detection approaches today include:

1. Visual Discovery

As the most basic anomaly detection technique, visual discovery employs manual monitoring on dashboards with charts, graphs, plots, and other data visualizations to find data variations. This approach requires extensive industry knowledge and creative thinking to ensure use of the right visualizations to find anomalies. Because most of the analysis is done manually, it is not easy or possible to inspect all the data available in the required timeframe.

2. Supervised Learning

Supervised learning builds on visual discovery by employing qualified people to label datasets as normal or abnormal. A data scientist then uses the labeled data to create machine learning models that can detect anomalies on unlabeled data. This method is effective when analysts have known patterns to use for modeling. The drawback of depending solely on this approach is that fraud is a continuously evolving threat, which means new patterns are constantly emerging.

3. Unsupervised Learning

The need for increased accuracy in anomaly detection has led to the development of unsupervised learning. This approach analyzes unstructured data mined in real time using advanced autoencoders and machine learning algorithms that identify anomalies as they happen without the need for human intervention.

Unsupervised learning is an effective anomaly detection method, especially in cases where patterns are difficult to anticipate or emerge quickly, such as credit card and bank payments or online “instant” credit applications. It detects unknown patterns from massive volumes of data without relying on outdated rules and tribal knowledge, which helps prevent losses from current and new fraudsters and attack vectors.

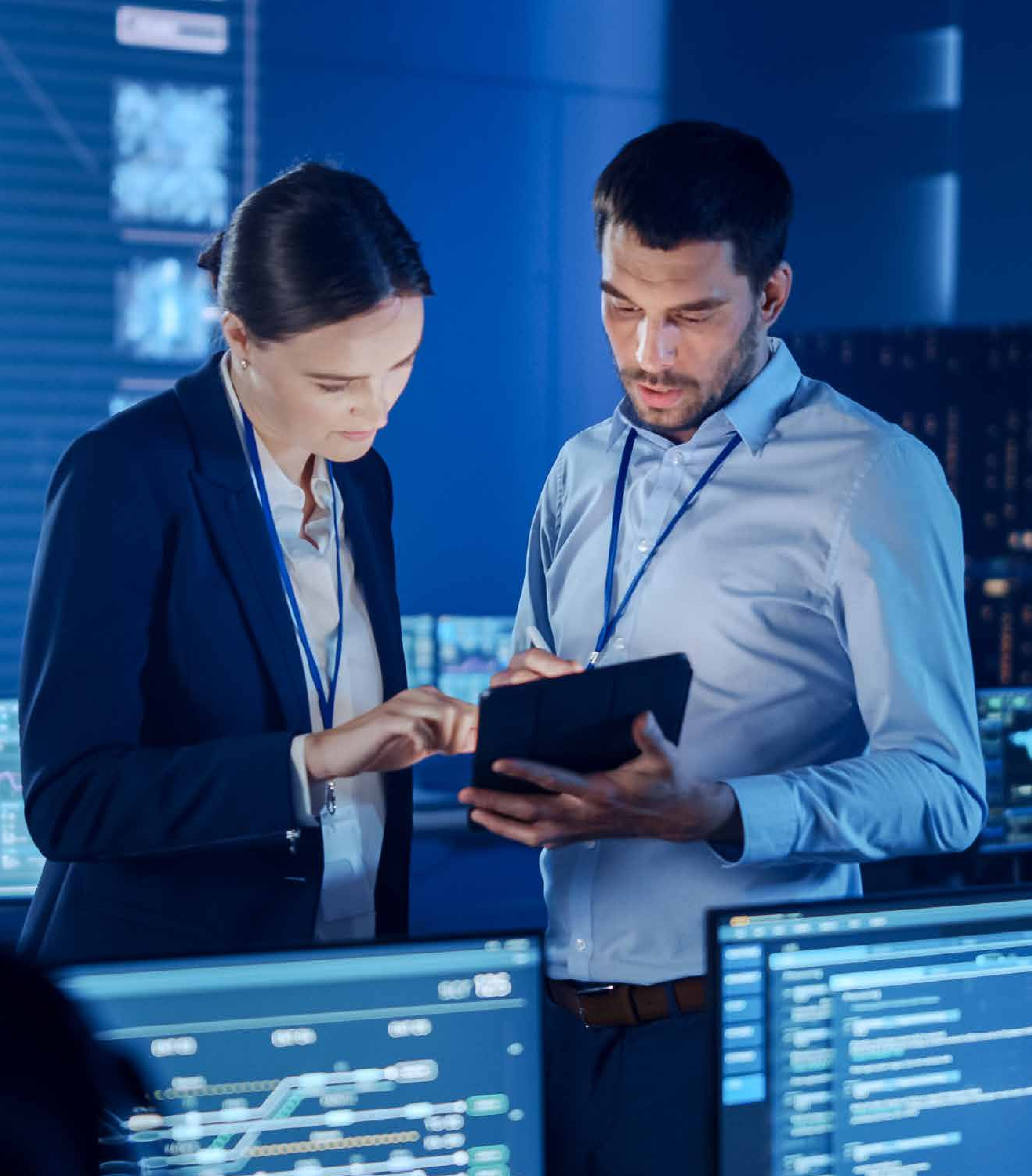
> Delivering only one or two of these methods will prove ineffective. Financial institutions should be using all of them. Here’s why.

The Critical Need for Intelligent Anomaly Detection in Financial Services

Anomaly detection in financial services is more critical than ever before. According to a recent financial crime report, based on 12 billion global transactions between January and March 2021, banking fraud increased by 159 percent between the last quarter of 2020 and the first quarter of 2021. The primary methods of fraud were account takeovers (42 percent), new account fraud (23 percent), and impersonation (21 percent). Unless the industry enhances investment in intelligent anomaly detection, more fraud and massive monetary losses are on the horizon.

In addition to increasingly threatening cyber insecurity, mainstream anomaly detection solutions struggle to balance fraud prevention and customer satisfaction. This is because, more often than not, variations in deposits, withdrawals, payments, and investments do not point to fraudulent activity.

For example, online payments skyrocketed when the COVID-19 pandemic began, and datasets used in training static anomaly detection systems did not have any similar historical patterns. Consequently, countless transactions were inaccurately flagged as fraudulent behavior, leading to numerous abandoned carts, lost sales, and customer alienation; in other words a broken customer journey.



Reinforcing anomaly detection with artificial intelligence, machine learning, event processing, and advanced analytics adds the ability to consider the context of transactions with much greater accuracy and deliver real-time insights into the billions of transactions that run through financial systems every day. With AI, ML, event processing, and advanced analytics, financial institutions can detect emerging fraud patterns, analyze those patterns in the context of overall transactional history, and instantly flag real-time potential fraud indicators for manual review. By combining the security of core banking systems with the flexibility and agility of machine learning, organizations can strengthen their defenses against new attack vectors while protecting customer relationships.

AI/ML: Powering Next-generation Fraud Prevention Solutions

Next-generation anomaly detection solutions rely on AI/ML to build self-learning models. These models are intelligent and can adapt and evolve as new fraud patterns emerge. As a result, organizations can arm employees with accurate, real-time insights into emerging threats, profoundly reducing false positives and reducing friction for customers.

Here's a look at five notable ways AI/ML can improve anomaly detection.

1. Accurate Anomaly Detection

Incorporating AI/ML into anti-fraud systems can dramatically reduce the uncertainty of anomaly detection. AI/ML algorithms can be deployed to analyze data in real time, find even the subtlest events and correlations in user behavior, and generate more accurate alerts than ever before. According to PYMNTS research, 80 percent of fraud prevention specialists surveyed reported that AI reduces payments fraud.

2. Heightened Customer Satisfaction

In recent years, AI/ML has gained commendable traction in fraud prevention, maturing to track and process massive transaction sizes and data simultaneously. ML-enabled anomaly detection can process significantly more financial information faster than rule-based systems. These solutions can reduce false positives and the verification steps that compromise the customer journey.

3. Faster Anomaly Response

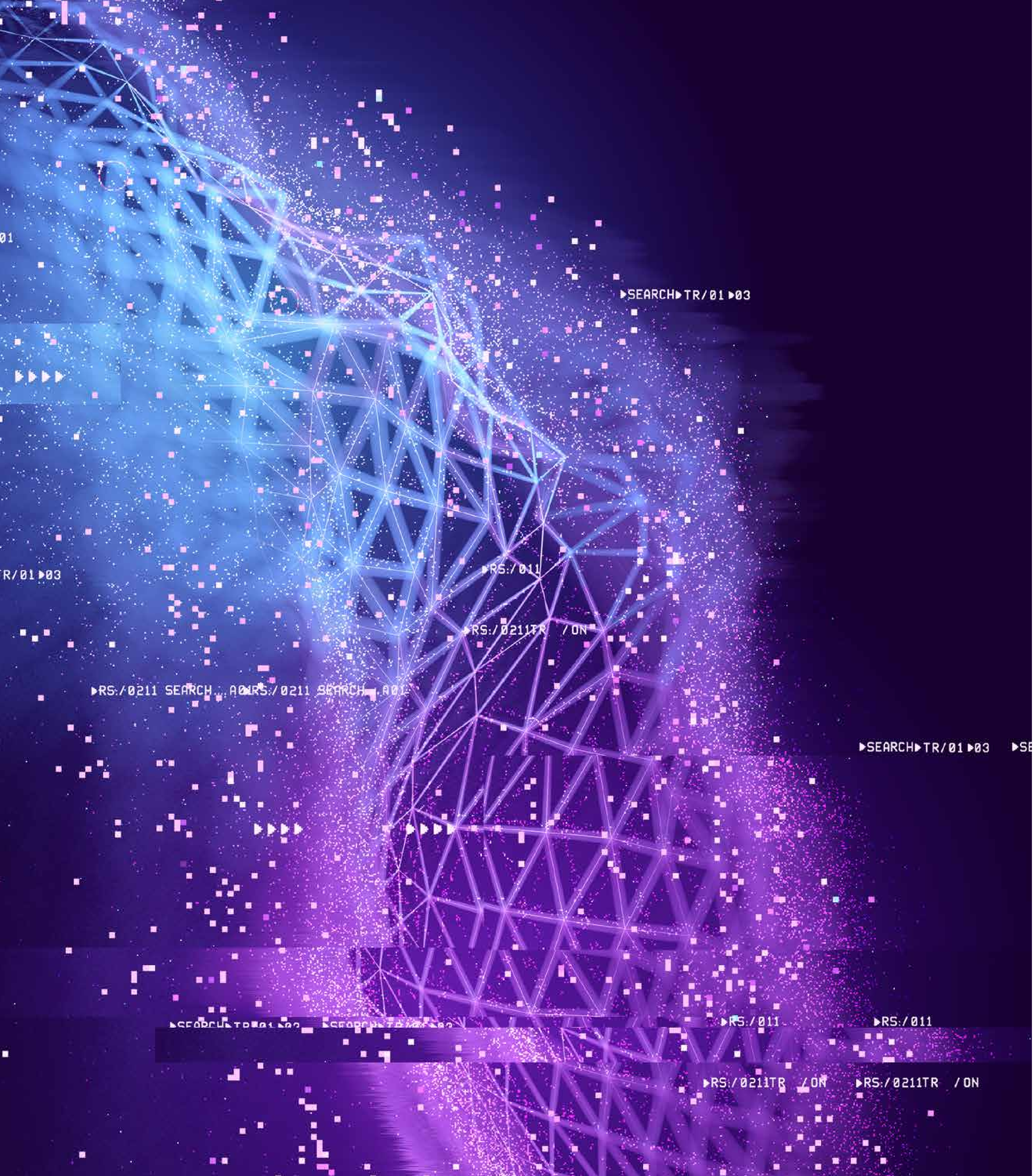
Real-time anomaly detection enables financial services providers to respond quickly to deviations, potentially saving millions in fraud losses. By leveraging AI to eliminate the delay between detection and resolution, payment and financial services providers can maximize the effectiveness of their anti-fraud approaches. In the above-mentioned PYMNTS survey, 63.6 percent of financial institutions reported that AI is a valuable tool for halting fraud before it succeeds.

4. Superior Scalability

Rule-based anomaly detection can deliver acceptable accuracy with several thousands of variables forming mostly static patterns. However, considering the millions of transactions being made every day, maintaining the required accuracy and responsiveness in the real-life financial services sector requires a more sophisticated and scalable anomaly detection solution. ML-powered systems can monitor and correlate multiple complex metrics with different levels of variability to sift through massive datasets every second.

5. Human-in-the-loop AI

AI can reduce the number of cases that must be manually reviewed by humans. For example, leveraging AI, one insurer was able to reduce the need for human intervention in claims processing by 17 percent. For cases in which automated anomaly detection is unable to provide decisive predictions, machine learning models can escalate cases to security professionals for final review and decision. Although the majority of cases can be handled quickly and automatically with AI, new and more challenging cases can be handled by an expert. Combining the machine speed and scale with deep human expertise makes for an optimal and synergistic intelligent system.



Eliminate False Positives with TIBCO's Intelligent Anomaly Detection Solution

With the soaring cost of financial crime and the collateral reputational damage to your financial institution, you cannot afford to adopt a laid-back approach to fraud detection technology. As a financial services provider, you must place investing in a comprehensive, customizable, intelligent anomaly detection system at the top of your priority list.

TIBCO provides a scalable, easy-to-adopt anomaly detection solution that you can deploy immediately to reduce false positives and provide proactive defense against new and emerging fraud strategies. With the necessary adaptability and power of machine learning, TIBCO's anomaly detection solution can do the heavy lifting and deliver superior scalability, accuracy, and responsiveness to help your institution fight financial crime.

Following are three key capabilities that make TIBCO's Intelligent Anomaly Detection the de facto solution for fighting financial crime.

1. Intelligent Fraud Detection

TIBCO uses several technologies, including machine learning, predictive and streaming analytics, and case management to deliver a powerful, cost-effective fraud detection solution. Rather than using one detection approach, TIBCO combines supervised and unsupervised models through AI/ML, event processing, and analytics to provide the most accurate indication of potential fraud.

For example, Asurion, a leading provider of device insurance and warranty and support services, was challenged by multi-channel customer interactions. A customer might start a claim in one channel and finish it in another, requiring the Asurion workforce to look at multiple systems to adjudicate cases.

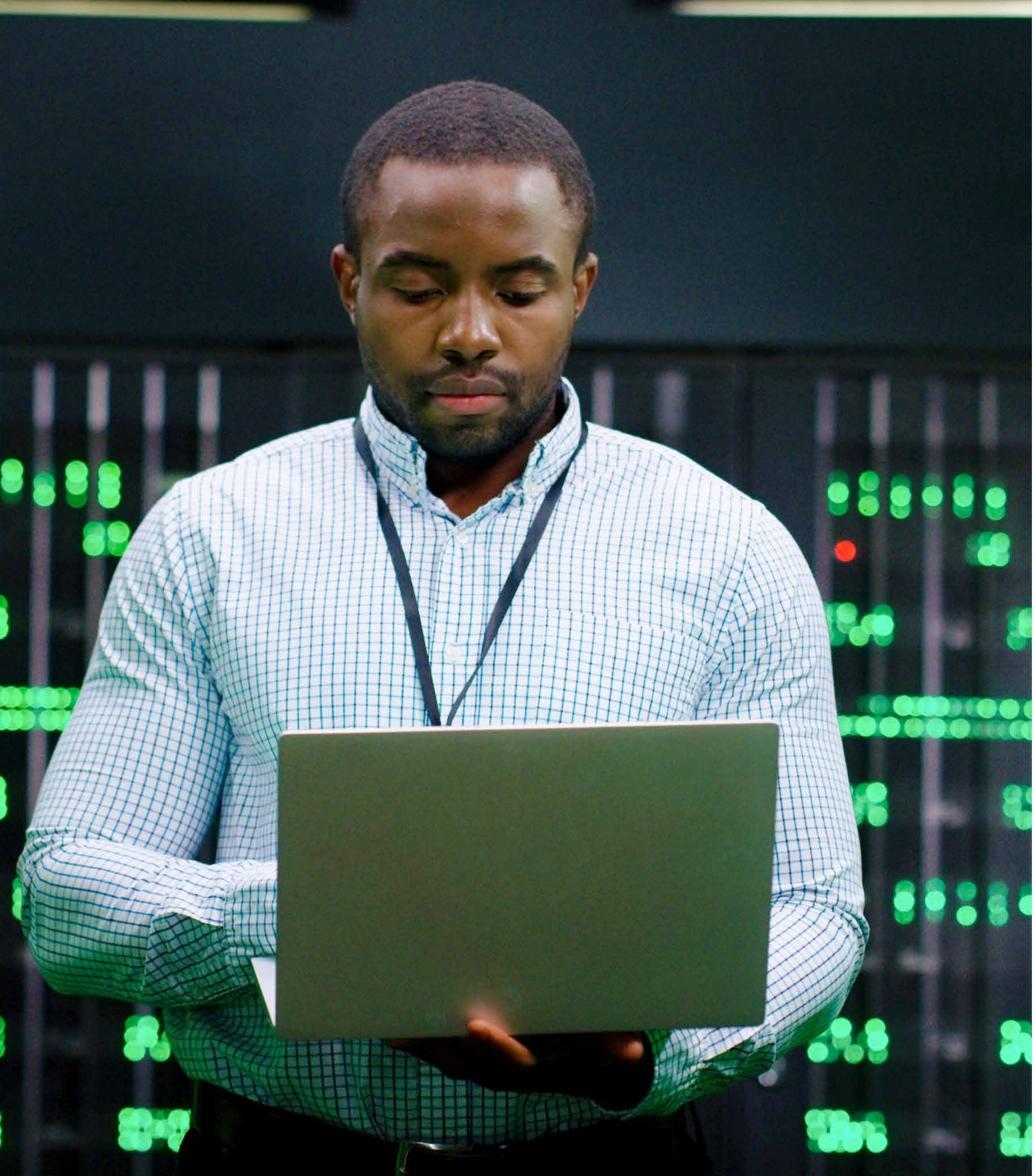
Now, the company's platform presents a quick graphic analysis of claims with baked-in fraud analytics that can help the team red-flag potentially suspicious behavior and analyze claims in real time. Read the full case study.

2. Flexible, Adaptable Platform

TIBCO's solution offers the agility to adapt to as many fraud scenarios as needed. You can modify the framework seamlessly to detect events like money laundering, credit and debit card fraud, insurance fraud, trade surveillance, and e-commerce fraud.

By integrating data discovery and statistical modeling into one solution, you can create visual tools that collect real-time data from multiple sources and transform it in numerous ways to dig as deeply into an alert as possible.

Specializing in home, motor, and travel insurance, AA Ireland relies on the flexibility and adaptability of TIBCO's solution. Colm Carey, chief analytics officer for AA Ireland, observed: "TIBCO was the only provider that could simultaneously optimize pricing, provide a deep understanding of customer types and value, and prevent fraud—so we chose TIBCO solutions. Using TIBCO, data comes in and goes out to models seamlessly without disruption, basically providing real-time predictability. You can understand it all—plus segmentation, fraud modeling, and underwriter profit." (Read the full case study.)



3. Built on Trusted Technology

TIBCO's anomaly detection solution, whether cloud-based or on-premise, connects seamlessly with a myriad of financial solutions, scaling to meet evolving transaction volumes. With real-time data streaming, TIBCO's anomaly detection solution enables financial services organizations to detect and prevent fraud as it happens.

TIBCO's anomaly detection solution can give you the peace of mind you need to focus on your core business needs. Learn about how you can help drive fraud prevention results and minimal false positives with TIBCO's Financial Fraud Detection Accelerator.

©2022, TIBCO Software Inc. All rights reserved. TIBCO, the TIBCO logo, TIBCO Cloud, and WebFOCUS are trademarks or registered trademarks of TIBCO Software Inc. or its subsidiaries in the United States and/or other countries. All other product and company names and marks in this document are the property of their respective owners and mentioned for identification purposes only.