



# MANTIS

## AI Fraud Detection

Wizard Driven  
Anomaly Detection

Let the most advanced eyes in the world help you to identify anomalies, or suspicious transactions in your data, invisible to the human eye.

## Meet Mantis

Mantises are the only invertebrates known to see in 3D.

Our AI solution looks at the data in various dimensions, in ways that the human eye alone is not able to see. AI powered sight will aid you in identifying anomalous, or suspicious, transactions in your data, after analyzing large volumes (millions of records) of historical data.

### Wizard Driven, No-code Solution

Mantis is a wizard driven, no-code software solution that leverages state of art AI models using a simple, guided user interface. This solution abstraction away from coding, enables Citizen Data Scientists in organizations to automate audits with AI.

### Identify Invisible Anomaly Signatures

Mantis flags anomaly that is invisible to human eyes due to the data flood and complex patterns. Stop recurring fraudulent transactions at a batch level and prevent blind spots, guiding users with interpretable, quantified results to further investigation.

### Actor to Actor Flagging

Fraud is usually committed by multiple actors and factors at the same time, and we are not only able to catch a single fraudulent actor, but also the collusion between actors, such as repair billing fraud, inventory return abuse, non-rendered services, duplicate charges, collusion of doctor-patient/doctor pharmacies, fake shops/vendors conspiracy, in addition to identifying anomalous patterns for an actor or transaction level.

### Dynamically Adjusts to Fraud

AI can search for new and unknown patterns to augment or replace the traditional monitor system across industries, such as healthcare fraud waste and abuse, billing invoices fraud, anti-money laundering, insurance, production defect detection, and default rate.



## Human in The Loop

The interpretable real-time reports with visualization generated by AI will guide users through the investigation process, empowering employees with unrevealed insights and taking further actions.

Leverage AI to enhance the quality of process and decision making, stop revenue leakage, and realize benefits.

Employees can easily change the underlying assumption based on different business scenarios and needs after building the model.

## Anomaly Lifecycle Management

Augment quality of decision making process and create a culture of compliance by establishing a complete, robust, and repeatable anomaly life cycle management.

## Portfolio of Algorithms Available

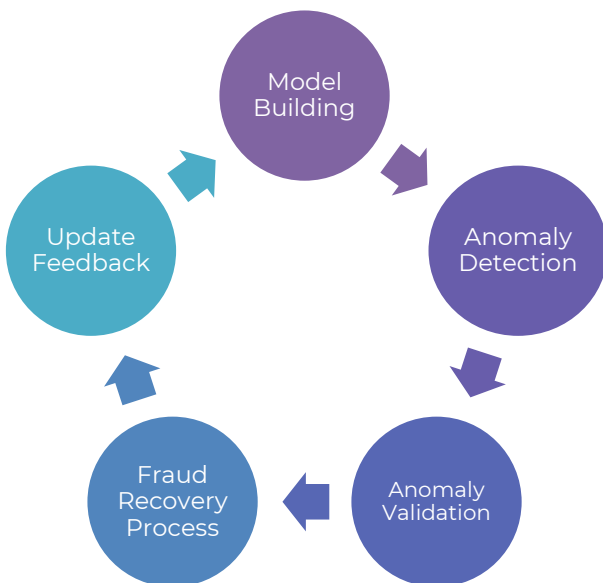
Utilize different algorithms based on various scenarios and assumptions to catch anomaly in different dimensions. Please refer to the next page for the details:

### Enable Citizen Data Scientist:

Whether your business has an audit team or not, Mantis enables users to leverage a wizard driven machine model configurator to guide you in building and visualizing anomalies in a consumable fashion to reduce errors.

## Model Management

Improve the connection and collaboration between data scientists and operations professionals. Orchestrate and manage AI models production, evaluation, application, and governance across the business to ensure that models could be evaluated by business domain experts, thereby supporting the development and deployment of complicated AI models.





Compare the signatures and let the AI try all possible models so you can go with the best!

Signature	What does it do	When to use
<b>Distribution based</b>	Captures cases that substantially deviate from the majority of patterns by identifying data points in the region of low probability	Anomaly detection with one variable only
<b>Clustering</b>	Density-based algorithm that investigates the density of any object and its neighbours and labels it as an outlier if the density is much lower than any of its neighbours.	Anomaly detection with one or more variable
<b>Association Rule</b>	Association rule finds frequent item steps and flags a point as anomalous if the item sets do not occur together frequently	Anomaly detection between two or more variables occurring together.
<b>Sequencing</b>	Extract sequential relationship and features to capture transaction patterns.	Anomaly detection when one event occurs after the other
<b>Historical occurrence</b>	Analyze the frequency and occurrence for historical outliers.	Anomaly detection with only one variable
<b>Custom Rules</b>	Custom solutions based on specific user scenarios and assumptions.	Anomaly detection using thresholds on one variable





## Benefits:

- **Increase Accuracy:**

Due to data flood and the complexity of fraud patterns, checking anomaly manually provokes excessive false positives and overlooks false negatives when . Contextual and Collective anomalies patterns are also very difficult to notice with the human eye.

- **Save Time with Automation:**

If even 10% of 10 million annual expenses are marked problematic, that means a million expense line items would need to be investigated by the compliance team annually. Not to mention to check them one by one and compare with historical files manually.

- **Adapt to New Fraud Signatures:**

While humans usually look for known patterns, AI machine learning can adapt to new changes over time, search for unknown patterns, and keep up with anomalies. Instead of giving binary feedback simply based on a threshold, which may be irrelevant overtime, AI will know the likelihood of fraudulent events.

## Become Proactive, Not Reactive

An ounce of prevention is worth a pound of cure. Don't wait and react until fraud happens. Our AI embedded solutions proactively look for exposures and continuously detect potential fraud before the situation gets worse by catching fraud upstream (during time of estimate) before invoicing. Besides, the actor & actor flagging ability can easily determine the root cause behind the scenes, allowing for the deeper investigation and preventing the recurring revenue leakage.

Without hiring additional data scientists, you can easily leverage AI to continuously improve internal preventive controls, mitigate regulatory risks, enhance the visibility of information, the augment quality of decision making process, and create a culture of compliance.



## About Kavi Global

Headquartered in Barrington IL, US, Kavi Global specializes in Data and Analytics Services Software and Solutions. They have a diverse set of clients in Healthcare, Pharmaceutical, Commercial, Industrial, Financial and Transportation verticals. Kavi Global has been recognized by Gartner in their Market Guides for Data and Analytics for 3 years running.



## Use Cases



### Billing Invoices Fraud

As the global supply chain complexity increases, so does the flow of goods, money, and the information among business entities. Providing visibility to upstream transactions that involve suppliers and logistic providers in a more efficient manner, and managing them in a timely and automated way, has become a challenge for every company. Enhancing the visibility of the flow of goods, money, and the information between business entities, from the shipment to the transaction receipts, is the first step to prevent any potential disruption.

Our AI solution is able to flag fraudulent transactions and conspiracy of fraudulent actors, such as asset repair bill fraud, inventory return abuse, fake shops/vendors collusion, and duplicate charges, efficiently and automatically.

### Pharma & Healthcare Billing Fraud, Waste & Abuse

According to the National Health Care Anti-Fraud Association, 3%-10% health care spending is fraudulent (up to \$300B). In fiscal 2019, the Department of Justice recovered more than US\$2.6 billion claims relating to the healthcare industry out of US\$3 billion from civil cases involving fraud and false claims against the government. There is no precise measure of healthcare fraud waste and abuse, as we will never really know how many we missed out via false negatives, or accidentally classifying fraud and not fraudulent.

Our AI solutions will highlight fraudulent transactions and actors, as well as the collusion of multiple fraudulent actors, such as doctor-pharmacists and doctors-patients conspiracy, instead of simply catching systemic fraud patterns at a batch transaction level and flagging a single actor.



## Use Cases



### Anti-Money Laundering (AML)

Banks in the U.S. spend more than US \$25 billion annually, on average, on anti-money laundering compliance according to Forbes. As the volumes, complexity, availability, and regulations change.

AI will adapt to new changes over time and flag recurring fraudulent actors to augment the traditional rule-based monitor systems. Instead of giving binary feedback simply based on a threshold, which may be irrelevant overtime, AI will know the likelihood of fraudulent events. Compared to other machine learning solutions in the market, the active learning AI methodology we leverage detect the anomaly patterns and flag fraudulent actor collusion with high accuracy.

### Insurance Fraud

The total cost of insurance fraud, excluding health insurance, is estimated to surpass \$40 billion annually, according to the FBI. Insurance Research Council (IRC) also estimated that up to \$7.7 billion of auto injury claims was excessive payments in 2012, accounting for 13%-17% of the total payments of 5 main private passenger auto injury coverages.

Traditional anomaly detection technology in the insurance industry identifies anomalies by fitting them into a preprogrammed template. As transactions get more and more complicated, so does the fraud. A proactive approach is needed to adapt to new fraud patterns and perform dynamic analysis. AI is the only feasible solution that can keep up with anomaly detection and flag recurring fraudulent actors and transactions, when fraud is continuously adapting over time.





## Use Cases



### Supply Chain Sourcing, Production & Quality Defects

The more components and processes in the production line, the greater the remake time and costs. For example, if we require 50% yield rate of the final product, we only need 50% of yield rate of the work-in-progress, if there is only 1 part needed to finish the production. However, if we need 10 parts to assemble the final product, then 93.3% of yield rate is required for each part, to maintain the 50% yield rate for the final product. However, 50% yield is unacceptable to most companies. Revealing the root cause of defects in each manufacturing process to enhance the yield is one of the most inexpensive ways to guarantee the quality, shorten the lead-time, and stabilize the supply chain.

AI can easily detect whether the outliers derive from the nature of process, human factors, machine factors, time factors, or environment factors, enabling stressors to be eliminated or controlled prior to any significant financial impact, and help you to identify improvement opportunities to achieve Six Sigma (3.4 defects per million, 99.99966%). This technology can also be applied to assist in making sourcing decisions. If there is a significant fluctuation in certain material prices in particular time or regions, maybe it is time for the sourcing department to investigate the reason and make a plan B.

### Government

According to McKinsey & Company's estimate, the U.S. government suffers a US\$150 billion dollars loss due to potential fraud annually, half of which goes undetected, and our AI anomaly detection solution enables the government to stop the revenue leakage in many ways. For example, the algorithms can easily identify the concentration of payments based on the geographic and demographic data the government has, thereby capturing the suspicious groups in suspicious regions. For another example, the government can utilize the technology to monitor any significant changes in the financial behaviors/status of tax and debt payers to forecast the possibility of insolvency. Due to data flood and the complexity of anomaly patterns, it is inefficient for humans to reveal these patterns and determine the hidden links between fraudulent actors.