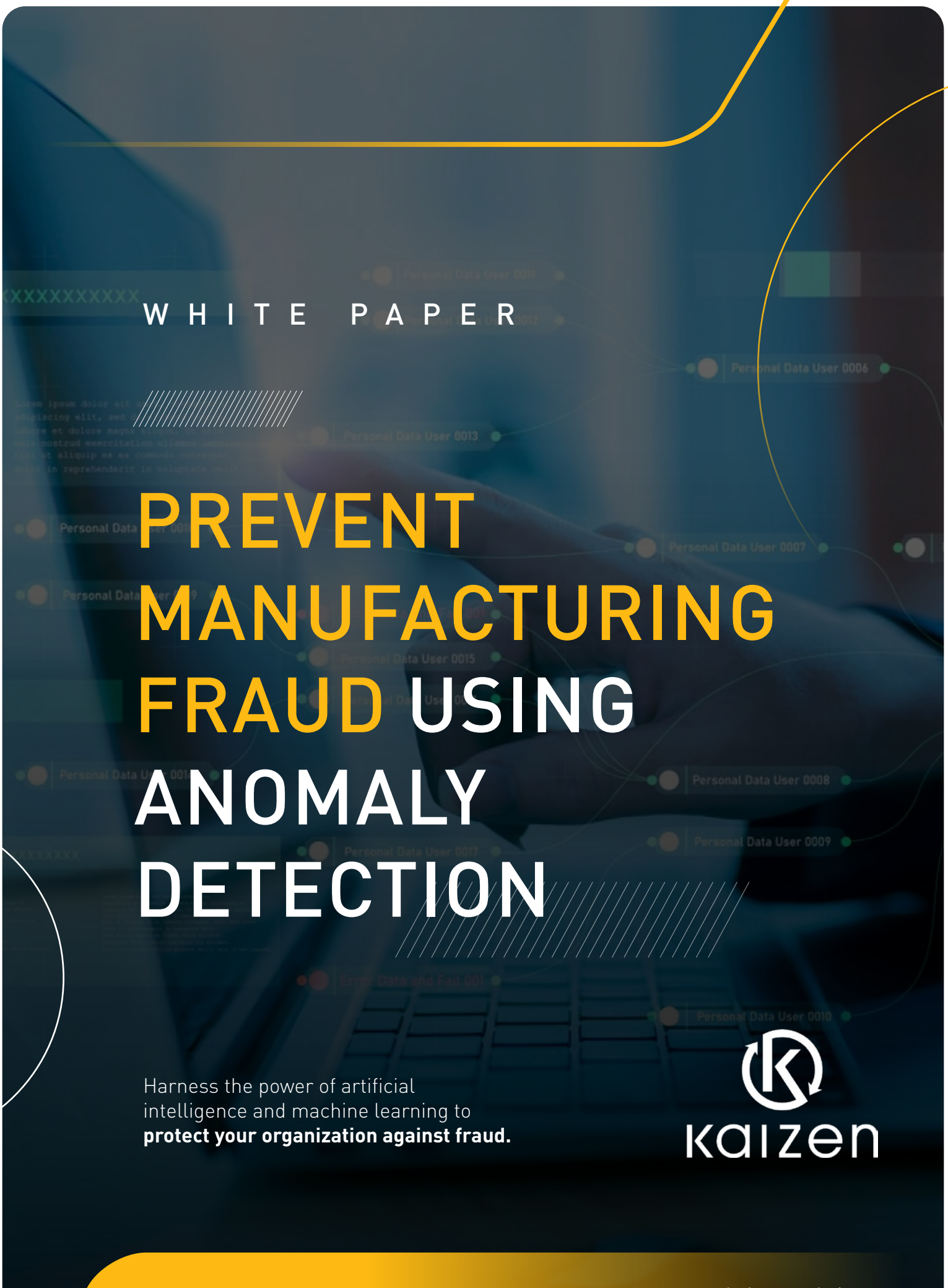

WHITE PAPER

PREVENT MANUFACTURING FRAUD USING ANOMALY DETECTION

Harness the power of artificial intelligence and machine learning to **protect your organization against fraud.**

kaizen

www.kaizenanalytix.com

Harness the power of artificial intelligence and machine learning to protect your organization against fraud.

The unfortunate truth is that the core characteristics of the manufacturing industry – unmonitored supply chains, a host of vendors, underlying assets in the form of inventory, and multiple and frequent transactions – make it a sweet spot for procurement and inventory fraud schemes.

Common vulnerabilities and fraud risks in the manufacturing sector include bid rigging, conflict of interest, warranty claims fraud, IP infringement, theft or misuse of inventory, product counterfeiting, and more. And it's taking a financial toll.

The Association of Certified Fraud Examiners (AFCE) estimates fraud costs

$200,000

per incident

How To Minimize the Risk of Fraud

Fraud is impossible to eliminate entirely, but there are common ways to reduce its probability and more quickly identify red flags:

+ **Assess and actively monitor internal controls.** Existing controls, thresholds and procedures should be regularly reviewed and assessed for relevance, adequacy, and effectiveness.

+ **Develop a robust, well-communicated fraud response plan.** Regularly training teams how to effectively spot, report, and respond to fraud is crucial to limit its impact.

+ **Know your supplier.** Performing background checks and integrity due diligence can ensure that the manufacturers or suppliers are of reputable standing, and it can highlight the manufacturers or suppliers' interests, associations, related parties, and possible conflicts of interest.

+ **Conduct regular checks on quality** such as routine checks for non-deliveries, repeat deliveries for the same order, and discrepancies between purchase orders and delivery.

+ **Optimize the power of data.** Big data is not only useful to provide insights, but organizations can extract real value as data can be analyzed to identify unusual or suspicious behavior.

Putting Data to Work Against Fraud

Utilizing Artificial Intelligence (AI) and Machine Learning (ML) technologies to automate the detection and triage processes allows for faster resolution (with the interconnectivity of data growing like never before, simple univariate anomaly detection techniques frankly do not cut it anymore).

The most advanced companies are leveraging sophisticated anomaly detection techniques to pinpoint the oddities in their data instead of trying to manually find them buried in dashboards and reports.

Using AI to automate fraud detection allows a manufacturer to instantly pick up on red flags such as excessive shrinkage in inventory, an abnormal rise in invoice volumes, split purchase orders, multiple payments made to vendors without any corresponding services rendered, unusually low or high bid price, and a sudden and unexplainable rise in customer complaints.

Companies need algorithms that look across a variety of data sources, metrics, and segments to uncover trends and relationships in order to more confidently assess where the true anomalies lie. Organizations achieve the most significant performance improvements when humans and AI solutions work together. Through such collaborative intelligence, humans and AI actively enhance each other's strengths to realize the best results. **But where do you start?**

5 AI/ML Approaches to Fraud Prevention

Consider these common ways to use artificial intelligence and machine learning to protect your organization against fraud:

1. **Anomaly Detection** is an unsupervised learning technique to automate detection of anomalies and make it more effective, especially utilizing large data sets.

2. **Logistic Regression** is a supervised learning technique that is used when the decision is categorical. This technique can be used to review transactions and flag them either as suspicious, or not suspicious.

3. **Decision Tree algorithms in fraud detection** are used where there is a need for the classification of unusual activities in a transaction from an authorized user. These algorithms consist of constraints that are trained on the dataset for classifying fraud transactions.

4. **Random Forest** uses a combination of decision trees to improve the results. Each decision tree checks for different conditions. They are trained on random datasets and each tree gives the probability of the transaction being 'fraud' and 'non-fraud.' Then, the model predicts the result accordingly.

5. **Neural Networks** is a concept inspired by the working of a human brain, using cognitive computing that helps in building machines capable of using self-learning algorithms that involve the use of data mining, pattern recognition, and natural language processing.

Real World Examples

The following are examples of common procurement fraud issues our customers are currently facing.

Supplier Collusion

Track trends in supplier spend to detect changes in price and volume above expected norms.

Purchase Order Fraud

Assess PO details including invoice frequency, vendor occurrences, and price to detect risk.

Employee Spend

Analyze employee expenses (e.g. travel, materials, business tools) to identify unexpected trends in duplicate, mischaracterized, or fraudulent activities.

The corporate use cases for anomaly detection are practically endless, from spotting fraud to revenue leakage to system outages, you can quickly identify outliers that impact profit. As data has grown along with unpredictability, more attention has been devoted to predicting anomalies as a proactive measure, as opposed to a reactive approach. **The technology is here today to help you take control and minimize profit-cutting fraud.**

About Kaizen

Kaizen is a leading provider of analytics products and business insights solutions that give clients unmatched speed to increased revenues, reduced costs, and maximized margins.

Kaizen combines our pre-built **Kaizen ValueAccelerators™** and data from **KaizenDataLabs™** with our subject matter expertise to rapidly generate actionable insights across the value chain, from Sales and Marketing to Operations and Finance.

Headquartered in Atlanta with offices in New York, Plano Texas and Los Angeles. Kaizen has been recognized as one of America's fastest growing private companies by Gartner, NPR, Forbes, Entrepreneur and Inc. 5000.

Kaizen's Anomaly Detection Engine

Kaizen's new **Anomaly Detection Engine** leverages proprietary machine learning algorithms to identify and quantify business anomalies in a condensed, easy-to-use interface. Waste less time searching for anomalies in your loads of data with a single easy-to-use, interactive interface.

Benefits include:

+ Raise profits by identifying and stopping the factors causing profit leakage
+ Reduce the risk associated with overlooking potential areas of interest
+ Condense your various data sources into one easy-to-use interface
+ Spend more time reviewing the pieces of your data that are most important

kaizen

www.kaizenanalytix.com

Get in Touch

About the Authors

Andy Williamson – Founder and Chief Product Officer, Kaizen

Bobby Falconer – Industry Expert and Business Consultant Lead, Kaizen

678.712.7092

engage@kaizenanalytix.com

Based on an article originally published by **SmartIndustry** on 9/1/2022.