

FAQ

1. What is this Product?

"Fraud Analytics" is an AI-driven solution designed to detect and prevent fraudulent activities. It's specifically tailored for the credit card and insurance sectors, which are highly susceptible to fraud.

2. What does it do?

The product uses AI algorithms to automatically detect patterns in claims data that may indicate fraud. It classifies transactions or claims into three categories: reasonable suspicion, strong suspicion, and no suspicion. This helps in prioritizing cases for further investigation.

3. Where can it be applied?

The solution is applicable in the credit card and insurance industries, where fraud is a significant concern. It can be used by:

- Insurance providers to detect fraudulent claims.
- Credit card companies to identify suspicious transactions.

4. What problems does it solve?

"Fraud Analytics" addresses the challenges posed by fraudulent activities, such as:

- Financial losses for businesses and customers.
- Time-consuming manual fraud detection processes.
- The need for accurate and efficient fraud detection in the face of evolving fraud tactics.

5. Dataset used for training

The model can be trained on the past years of data, which implies a substantial volume of historical data is utilized.

6. Model used to train

The product leverages an ensemble model, which combines multiple AI techniques. It includes:

- Feature Engineering using NLP (Natural Language Processing) and other methods.
- Both rules-based and black-box models.
 - **Rules-based models:** These models rely on predefined rules and conditions set by experts. For example, a rule might be "If a transaction exceeds \$10,000 and occurs in a foreign country, flag it as potentially fraudulent." These rules are based on known patterns and expert knowledge of fraud.
 - **Black-box models:** These models, often based on machine learning algorithms, analyze vast amounts of data to identify complex patterns of fraud that may not be apparent to humans. The term "black box" implies that the decision-making process is not always transparent or easily interpretable. However, these models can uncover hidden relationships and adapt to new fraud tactics.
 -

- **What Attributes ?**

The basic model uses 100-200 attributes/data sources and is applicable in the BFSI sector, including mortgage, loan, and insurance sub-domains. The model selection and results help in decision-making.

7. How many use cases have been done so far?

The document highlights two primary use cases:

- Insurance fraud detection
- Credit card fraud detection.
- Raising a Claim in the System

9. Does it follow HIPAA compliance?

There is no explicit details of HIPAA compliance

10. Average cost/timeline of implementation

Defining exact "average timeline" for fraud analytics implementation is challenging because it varies greatly depending on several factors like:

- **Data Volume and Complexity:**
 - The "Fraud Analytics" product uses historical data. The sheer volume of this data, its cleanliness, and its organization significantly impact the preprocessing time.
 - Data from various sources (claims, claimants, payments, vendors) adds complexity.
- **Integration:**
 - Integrating the model with existing systems (Salesforce, cloud environments, third-party applications)
- **Testing and Validation:**
 - Thorough testing and validation are crucial, especially in fraud detection, where accuracy is paramount.

11. Does it also provide a detailed report of the reason for marking fraud?

The model that product uses doesnot explicitly provide report but the model uses a combination of rules-based and black-box approaches:

- **Rules-based:** The system is trained on historical data and predefined rules set by experts. So, if a particular rule is triggered (e.g., a transaction exceeding a certain amount), that could be a reason for flagging fraud.
- **Black box:** The AI also identifies complex patterns that might not be obvious to humans. If the AI detects a pattern strongly associated with fraud, that would contribute to the decision.

12. Is there any manual check also required?

The system is designed for end-to-end automation, but it classifies suspicions, implying that further investigation (possibly manual) might be needed for cases with reasonable or strong suspicion.

13. What's the accuracy?

The model gives a 74% accuracy rate.

Additionally, it a 90% reduction in conversion time and \$1.5 million in potential savings.

- What are the benefits of the product? The product increases accuracy by 75%, increases revenue by 20%, improves operational efficiency by 60%, and reduces human bias by 95%. It also helps in real-time verification, automated data retrieval, risk scoring and prioritization, anomaly detection, and real-time alerts.
- What data is used for the model? The model uses demographic data, claim data, payment data, and incident data.
- What is the process flow for the model? The process flow includes data cleaning, data preprocessing, feature engineering, model training, and model evaluation.
- What features are used in the model? The features used include demographic information, claim details, payment information, and incident specifics.
- Where does this fit in? This solution fits in the Banking, Financial Services, and Insurance (BFSI) sector, specifically in loan and mortgage processes.
- What additional services can be provided? The solution can help in identifying potential customers for additional services through segmentation analysis, dashboard alerts, real-time analytics, and cross-selling strategies.

- What is the architecture of the solution? The architecture involves database, data cleaning, data preprocessing, feature engineering, model training, and model evaluation.
- What are the implementation details for fraud detection? The implementation involves advanced data analytics, machine learning algorithms, behavioral analysis, and collaboration with industry partners.
- What are the objectives and challenges of the solution? The objectives are to detect and prevent fraudulent activities and identify potential customers for targeted sales. The challenges include rising incidents of financial fraud, the need for real-time detection and response, and balancing security with customer convenience.
- What are the differentiators of the solution? The differentiators include dashboard alerts, real-time analytics, prediction over revenue generation, and cross-selling strategies.
- What are the advantages of using the solution? The advantages include reduced fraud losses, increased revenue, and enhanced customer satisfaction.
- What is the solution layer? The solution layer includes Sales Cloud, Finance Cloud, AppExchange, and the Fraud Model.