FRAUD GLOSSARY

Learn the language of fraud"

by formica.ai

Anomaly Detection

In data mining, anomaly detection is the identification of data points, items, observations, or cases that diverge from an expected pattern or the majority of data.

These anomalies may signal a warning, such as fraud, cyber attack, or faults in texts.

Accounting Fraud

It is the situation in which financial data is presented by changing it so that it does not reflect the real value or financial activities of the organization.

This may include accounting misconduct, fraudulent borrowings, providing financing, fraudulent applications, and illegal transactions.

Anti-competitive/ Anti-trust

Violation of laws that encourage market competition is the regulation of anti-competitive and unfair practices carried out by organizations.

For example; fixing prices, discriminatory pricing, providing unfair trading conditions.

Artificial Intelligence (AI)

Artificial intelligence is the technology that a computer program or machine has thought skills and the ability to learn.

It is a technology that learns by analyzing data and adapts itself by what it learns through data.

Bank Identification Number

The first 6 digits of credit cards are the bank identification number (BIN). This set of numbers identifies the financial institution that issued the card.

BINs are used to verify the geographic region where cardholders are located.

Binary Classification

It is the classification of elements belonging to a group into two groups with a classification rule. It typically includes a class that represents the normal state and one that represents the abnormal state. It is frequently used in credit card fraudulent transaction detection methods.

Biometric Authentication

It is a verification or security process based on people's biological characteristics.

Facial scanning, fingerprint verification, eye scanning can be given as examples.

Bot Attacks

A bot attack is automated web requests used to trick, defraud, or embarrass a website, application, API, or end-user.

Bot attacks started as simple spam attacks and then grew day by day into complex structures with their economies and infrastructures.

Call Center Scams

It is when scammers phones call centers and impersonate real customers to seize a real customer's account or obtain their personal information.

CNP Fraud

A card-not-present transaction happens when the customer makes a purchase by mail, phone, or online, where the credit card is not physically present at the time of purchase. This payment method is easy for customers but vulnerable to fraud.

Credential Stuffing

Credential stuffing attacks are a type of fraud in which fraudsters use stolen credentials to break into user accounts.

In this process, fraudsters take advantage of a large number of leaked legitimate user credential data.

Customer Fraud

Fraudulent practices against the companies through the illegal access and tricky practices of products or services by customers or others.

CVV

CVVs are three- or four-digit numbers that provide an extra layer of security for cardholders and merchants.

In e-commerce, retailers ask customers for the CVV value to verify whether they own the card they used to purchase.

Cybercrime

It is used to refer to any crime committed by a computer and computer network.

The computer can be used as a crime tool or be a victim of a crime. Cybercrime can harm individuals' data and financial security.

Data Augmentation

Data augmentation is the process of generating new data points to increase the amount of data by changing the original data, in data analysis.

It creates artificial copies by making some changes to the existing training data. These copies create larger training data set by being added to the existing training data set.

Data Breaches

Data breach is the illegal accessing or disclosing of sensitive, confidential, or protected data.

Many reasons such as hackers, weak passwords, phishing attacks, software errors can result in a data breach.

Data Mining

It is the process of finding anomalies and patterns within large datasets to predict outcomes.

Data mining allows you to understand related data and evaluate outcomes, enabling you to make informed decisions.

Data Insights

It refers to the understanding of a specific business phenomenon that you can achieve by using machine learning and artificial intelligence technology to analyze a set of data.

Deep Learning

Deep Learning, a sub-category of machine learning, is a type of artificial intelligence that allows machines to learn to solve complex tasks without the need for programming.

The more data input, the more successful the deep learning processes will be.

Denial of Service Attack (DDoS)

It is a category of attack in which authentic users are prevented from receiving services by hackers. In these attacks, the hacker sends multiple messages asking the network or server to verify requirements with unacceptable arrival addresses.
This overloads the system and may prevent authentic users from accessing this service.

False-Positive

Transactions that are described as suspicious but have not yet been verified are considered false-positive in fraud detection.

False positives can cause huge financial and reputational losses to companies in both the short and long term.

Fraud

Fraud is intentional acts or failures that cause the perpetrator's gain or victim's harm by deceiving others. It is carried out in unethical ways. Depriving a person or institution of the benefits it deserves is also defined as fraud.

Fraud Graph

Traditional relational databases lack the efficiency to store and analyse information between different entities. For explore and visualise the relationships within the data and overcome the poor performance of relational databases, you need to use graph databases.

You can identify common phone numbers or email addresses between connected users and create a network of similar information that can be analysed to detect fraud.

Fictitious Refunds

In a fictitious refund scheme, an employee treats as the customer is returning the merchandise, even though there is no actual return.

Because the transaction is not genuine, there are no actual returns and company inventory is overstated.

Machine Learning

A type of artificial intelligence that analyzes data to learn automatically through experience.

Machine learning algorithms create a model using sample data to make predictions and decisions without the need for programming.

Manual Review

It is the process of examining transactions in fraud detection manually by risk teams without the help of any software.

In some cases, it can be done in addition to the investigations performed by fraud detection tools.

Money Laundering

It is the process of hiding the source of money obtained by fraud or any illegal way.

There are often large sums of money and detection involves longer monitoring and analysis processes than a typical fraud case.

Monitoring

It is the process of observing the progress of a transaction, customer, or anything else over a period of time.

It is often done for suspicious transactions and customers in fraud detection process.

Predictive Analytics

Predictive analytics predicts user behaviours based on existing data.

With the data, it evaluates the potential possibilities and predicts and analyzes the possible behavior of the users.

Point-to-Point Encryption (P2PE)

P2PE is a standard established to improve the security of credit card transactions. According to these standards, transaction data is securely encrypted when entering the merchant's point of sale, and this encryption continues until the end of the transactions made with the credit card. This layer of protection is used in addition to SSL encryption.

Procurement Fraud

It is illegal actions that negatively affect the bidding or tender processes in the procurement processes of the services, goods, or assets of the suppliers.

Phishing Attacks

The process by which a fraudster tries to obtain private information from a victim by impersonating a legitimate person.

E-mail is one of the most common tools fraudsters use to phishing attacks.

Real-Time Fraud Analysis

Analiysing all tnsactions in real time and alerts fraud analysts of potentially fraudulent activity. Traditional fraud detection systems might take hours to convert and analyze the data to identify anomalous activity.

AI-powered fraud detection services provide efficient results for real-time fraud detection

Risk Assessment

It is the process of evaluating the potential risks that may occur for a foreseen activity. Different systems and methods may be required to carry out risk assessment.

This evaluation process also includes determining the possibilities of risks that may threaten systems in the future.

Rule-Based Fraud Detection

Rules-based fraud detection systems use correlation, statistics and logical comparison of data to identify potential fraud actions based on insights from previous fraud cases.

They often use traditional data analysis methods and require time-consuming research.

Ransomware

It is malware that blackmails the user. It blocks access to a computer with encryption unless a specified fee is paid.

Scammers often threaten victims with say they can delete important data.

Scalable AI

It is defined as the ability of algorithms, data, models, and infrastructure to operate at the size, speed, and complexity required for the given mission.

Synthetic Identity Theft

It is known as a technique mainly used for application fraud.

It is the process by which a malicious person creates an identity that contains personal data belonging to more than one person, or creates an identity that uses a combination of real and fake personal data.

Streaming Data

It is the process of receiving, sending, and processing data obtained in real-time. The ability to process and analyse information with the support of artificial intelligence ensures that the process is sustainable.

Online games, stock markets, processing facilities, retail management systems, and location sharing applications are examples of data flow applications.

Sniffing

It is the process of monitoring and capturing all data packets passing through the given network. It is illegal to do it by an unauthorized party. Stolen information runs the risk of being used for fraud and blackmail.

They are used by network administrators to monitor network traffic and troubleshoot problems.

Tax Fraud

It's the illegal methods that an organization or individual deliberately uses to avoid paying their tax liability.

Transaction Monitoring

The process of analyzing and reviewing a transaction operated on an information system or business application to evaluate its compliance with regulations or policies.

Two-Factor Authentication

It is a tool used to secure online accounts. It is created by adding a layer of security to the user and password.

But with advanced fraud technologies, even two-factor authentication can be overcome.

Transaction Authentication Number (TAN)

It is a disposable code used to process online transactions. It offers an additional layer of security to the password for logging into or transacting an account.

It is used to reduce the possibility of fraud in transactions.

URL Shortener Spam

It is the masking of malicious links through URL shortening services.

The purpose of this technique is to make spam links seem as safe and trick victims into clicking on links.

Unsupervised Machine Learning

It is often used to discover patterns in large amounts of unlabeled data. It is especially effective in discovering new and unknown patterns.

It focuses on examining the relationships between input data in anomaly detection techniques.

Utility Fraud

Fraudulent use of someone else's name or identity to take advantage of any service.

The most common form is making phone calls to impersonate public officials for fraudulent purposes.

Unauthorized Withdrawals

It is the withdrawal of money from a person's bank account or any transfer transaction without the authorization or approval of a person.

Validation

It is the verification of the completion of a transaction in the way it should be and by the person who needs to do it. There are many verification methods for security purposes in fraud prevention.

Velocity

It means that the volume of transactions carried out from a particular source higher than the average volume of users too much. For example, making a large number of transactions at once from an account that has not been used for a long time is an example of Velocity. It can also be defined as measuring the speed of multiple transactions of a user.

Vishing

It is the fraudsters' access to areas that they can reach by creating synthetic voices or imitating someone.

It is generally intended to intimidate the other party with the method of using someone else's voice.

Voice Authorization

It is a security protection used to ensure that a certain transaction can be performed by a authenticated person.

It is usually done by ensuring that the authorized person continues the transaction with the defined voice during the purchasing stages.