INTRODUCTION TO FRAUD DETECTION

A STARTER'S GUIDE TO FRAUD DETECTION AND PLANS FOR PREVENTIONS AND CUSTOMER PROTECTION

formica

Table of Contents

01 /

Introduction

Today, the technology where we run everything from shopping to business life, from banking transactions to many of our hobbies, is developing rapidly day by day to make our lives easier.

In addition to many institutions, also individuals focus to digital-compatible business areas and hobbies at the point of transferring solutions for all areas of life to digital.

This digital transformation also creates new opportunities for scammers.

In this age, where digitally hosted data has become so important, traditional fraud methods are being replaced by new digital fraud methods that used new technologies.

01 /

Introduction

Technologies developed against fraudsters who try to detect the vulnerabilities in the technological infrastructures used by companies or individuals and abuse their digital assets are also developed rapidly day by day to create a defense and protect individuals and institutions.

So what is this concept of digital fraud?

Before planning the precautions you need to take, it is useful to get to know this risk closely.

This e-book has been prepared by Formica so that you can understand the concept of fraud and fraud detection, get to know the risks closely, and plan your precautions.

02 /

What is Fraud & Fraud Detection?

What is Fraud

The concept of fraud includes a criminal and a victim. Unfortunately, it is not possible to put fraud into a clear definition. It can be encountered in many different areas with various methods. So that in addition to separating traditional fraud and digital fraud, even digital fraud activities are also quite diverse in themselves.

Fraud; appears in many different segments, from credit cards to personal data, from promotions to reservations. Any earnings obtained through illegal or unethical ways are classified as fraud.

What is lost as a result of fraud is not have to be money every time.

What is Fraud

As a result of fraud, there may also be losses that cannot be recovered with money, which can lead to more serious consequences in the long term, such as loss of reputation, misinformation, and loss of business opportunities.

The most important point in combating fraud is to be able to detect and prevent fraud before it happens.

When most fraud cases are discovered after they occur, it is almost impossible to recover these losses. Imagine that you are an e-commerce company and your customers' data has been leaked, even if you realize this fraud after it has happened and takes legal action, you cannot recover your company's reputation, the news in the media, and the bad experience of your customers.
At this point, you should plan the steps you need to take before you have a bad experience and be able to commit this trust to your customers.

Fraud detection and prevention tools offered by the latest technology can come into play at this stage and can be a hero for you.

What is Fraud Detection

Fraud detection includes the entire process of institutions to identify fraudulent activities.

These activities can be financial as well as other forms such as fraudulent credit card transactions, data theft, or cyber-attacks.

Fraud detection is usually done with methods to predict abnormal behavior, taking into account predetermined rule flows. Fraud detection methods, such as fraud, are also quite diverse in themselves.

Fraud detection products, which can be customized from the technology used to the workflows defined, to the industry in which they are used, are also developing rapidly to cope with the increasing number of fraud cases as a result of rising digitalization.

What is Fraud Detection

It is very important that the methods developed for fraud detection adapt to the current technology, detect the vulnerabilities before the fraudsters, and do not leave any open doors to the fraudsters.

Many scammers test predetermined patterns and exploit vulnerabilities.

The opportunities provided by the developing technology day by day is the best friend of fraud detection, and it is also the best friend of the fraudsters.

03 /

Why Do You Need Fraud Detection?

Big businesses often have analytics teams that play a significant role in fraud detection, but when considering the working hours, the speed of the human brain, and the multitasking capacity, it's not surprising that no analytics team can be faster than technology. At this point, the most important helper of the analysis team is fraud detection products.

Ideal fraud detection products should be able to provide you real-time transaction data by easily distinguishing your customer, your customers' movements, normal and abnormal behaviors.

Considering the impossibility of analyzing these data one by one, a fraud detection tool that can take actions such as preventing abnormal behaviors, alarm management, limiting the user's behavior will be your greatest helper, apart from providing real-time data.

Benefits of proper fraud detection technology;

- You can prevent losses by detecting fraud attempts in real-time.
- By analyzing your customers' transaction data and behavioral histories, you can create a profile and detect risk situations in advance.
- You can quickly adapt to new fraud techniques by adding new rules to your standard rule flows.
- You can prioritize risk situations and respond to critical situations early
- By reducing manual reviews, you can reduce the workload of your fraud team, enable them to focus on more critical cases, and increase work efficiency.

Benefits of proper fraud detection technology;

- You can increase functionality by better classifying your data.
- You can maintain the relationship of trust between you and your customers by reducing false-positive rates.
- You can adapt your team and company to constantly changing fraud techniques with flexible and easily deployed rules or workflows.
- You can optimize your company's performance and conversion rate by reducing the stressful and inefficient fraud monitoring on your employees and risk teams.

04 /

The Mechanics of Fraud Detection

As a result of increasing digitization, fraud has now entered our lives with many different variations.

Traditional methods developed against traditional frauds have become quite inadequate in detecting and preventing different types of fraud.

Getting to know the mechanics of fraud closely is one of the most significant steps in adapting to proper fraud solutions.

*

Common Types of Fraud

Application Fraud

Application fraud can cause you greater losses than money. The security of your data is crucial to your company's reputation and reliability. Fraudsters use application fraud methods to impersonate synthetic identities or impersonate someone else.

Booking Fraud

Keeping track of your customer activities as the impact of your services expands became more difficult. It is very critical to protect your day-to-day growing business against booking fraudsters and to prevent the abuse of your services.

Promotion Fraud

Promotions are very good tools to keep your customers happy and gain new customers.Promotion abuse is a type of online fraud that involves customers taking advantage of a business's offers. To do not let anyone abuse your promotions and discounts, you can provide specific promotions to user ID and IP..

Debit & Credit Card Fraud

Did you know that you can be exposed to card fraud even if your credit card is not stolen? Credit cards which have security flaws are easily accessible for fraudsters. You have to be faster than fraudsters to detect if your card has a security flaw. You should monitor card transactions in real-time to prevent card fraud.

Internet Fraud

It is one of the most common types of fraud. One of the most effective ways of internet fraud protection is keeping the software on your computer and mobile device up to date. In addition, you should be wary of e-mails from untrusted sources. You should not click on links or download attachments in e-mails from unknown sources.

Mail Fraud

They are frauds to get money or personal information from someone via mail, steal someone's e-mail, and collect money or goods. When checking your e-mails, make sure that they come from corporate e-mail addresses, do not click on links in e-mails that do not come from reliable sources, and do not download attachments.

Learning about the different types of fraud helps you to be aware of the risks and find solutions.

05 /

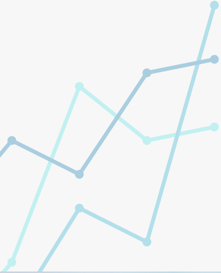
7 Ways To Protect Your Company From Fraud

Fraud Graph

There are many methods of fraud and developing technologies make it difficult to detect fraudsters.

Multiple fraudsters can organize fraud rings with large numbers of users to commit fraudulent transactions.

This organized movement makes it very hard to detect fraudsters. Fraud graphs can find common patterns in customers' data and show the relationships between transactions, actors, and all other data.



Fraud Graph

Using a fraud graph, companies can identify items such as connected users, email accounts, addresses, and common phone numbers in a network.

In this way, you can get an information network that can be visualized, analyzed, and connected to detect fraud. For example, money laundering; there are many ways to money laundering, often these funds are passed through many different organizations, making it hard to trace the source of the money.

Money that cannot be traced becomes laundered.

Graph databases allow you to track transactions, providing you with a clear picture of the entire path money takes from its source to its destination.

Machine Learning

Checking and detecting fraudulent activities is a time-consuming operation for fraud analysts. The speed with which frauds are detected is directly proportional to the time spent by the analysts. However, scammers can perform millions of fraudulent transactions in seconds with developing technological devices.

This loss of time causes the money lost, as a result of this, the laundered money cannot be recovered. Traditionally, businesses used only rules-based systems to prevent fraudulent payments. While rules are still an important part of fraud detection and prevention tools today, their use alone in the past has also caused some problems.

As the data that need to examine increases, the analysis of this data with appropriate methods, the correct classification of the data, and the tracking of user movements revealed the necessity of machine learning systems.

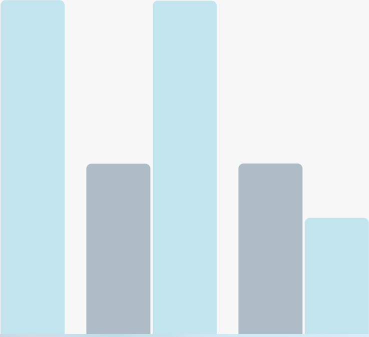
Machine Learning

Fraud detection using machine learning provides many benefits to businesses.

Some of these benefits are;

- Less False-Positive Case

  Deciding whether a transaction is real or suspicious at the point of detecting fraud creates a huge waste of time for analysts. False positives, which seem to be real but are not fraud, slow down the speed of detection of real fraud movements by causing a waste of time due to the workload. Fraud detection using machine learning models applied for this take fast actions at the point of detection and minimize the losses



Machine Learning

- ### Less Employee Need

The more data and experience provided to AI, provide the better the results. At this point, it is important to process the data obtained by companies with machine learning in fraud analysis and to create the right decision-making algorithms with machine learning instead of the workforce. Fraud detection tools using machine learning help quickly detect and recover fraudulent activities and minimize damage to organizations.

- ### Faster Fraud Detection

False-positive transactions are checked by analysts and as a result, it resulted that they are not real frauds. This causes late detection of possible real frauds, and lost funds cannot be recovered. Machine learning provides great support to analysts in detecting false positives. Combined with simple filtering mechanisms and algorithms, machine learning can create the right alert systems.

Machine Learning

- ## Analysing Normal & Abnormal Activities

Machine learning-based anomaly detection algorithms accurately detect abnormal behavior in different data models and apply filters to these anomalies, ensuring you only get alerts on issues that matter to you. One of the key benefits of machine learning is its capacity to process more data than an analyst can and then use the compiled data to identify patterns that are hard for a human to identify. Fraud detection tools using machine learning allow analysts to investigate previously undiscovered suspicious activity. The ability to retrain and tune models and adjust parameters automatically is a powerful tool for risk model management.

Alarm Management

It is necessary to detect fraud cases instantly before they happen, to prevent money laundering.

Using a comprehensive alert management screen to analyze and investigate risky transactions and potential fraud events will be very helpful for your fraud analysis teams.

Especially, organizing your alarms according to urgency, sending notifications to relevant workgroups or individuals through many different channels such as e-mail, SMS, mobile notification will always keep you on the alert.

Thanks to alarm management, you can receive alerts for emergencies instead of spending all day in front of the computer.

In addition, alarm management allows you to easily perform actions such as blocking or changing permissions when necessary.

Alarm Management

Depending on your needs, rules, and workflows, you can approve or reject transactions and control and coordinate all these flows from the alarm management system.

A good fraud tool can take actions for high-risk transactions in line with the rule flows you set, without waiting for the fraud analyst to see the alarm and interfere.

This provides you more convenience and fewer fraud cases.

Real-Time

Real-time fraud detection is the real-time execution of fraud detection algorithms to detect fraudulent activities.

It uses real-time data analysis to determine whether an ongoing transaction is legitimate. Before real-time systems detected the fraud instantly, fraud results were often available weeks or months after the fraud was committed.

It made it hard to trace the fraud activity or allowed the scammer to make a large number of fraudulent purchases.

Real-Time

The best way to stay a few steps ahead of scammers is to detect suspicious transactions in real-time before they happen.

Early detection is the first step in taking action before you suffer any damage. Thus, you can always protect your company against irretrievable damages.

The key to real-time fraud detection is to benefit machine learning tools. It is essential to be proactive in analyzing and detecting potential fraudulent risks.

Undetected frauds can reduce your customers, damage your reputation. You should reduce your customers' security concerns by adapt to new strategies.

The best way to achieve this is to detect fraud in real-time and minimize loss.

Scalability

A scalable approach to fraud detection enables efficient use of big data analytics to improve the ability to handle increasingly complex online frauds.

This approach is applied by supporting machine learning algorithms with big data to increase fraud detection efficiency. With the rapid development of digital payment methods, the importance of big data analytics for fraud detection is increasing.

Scalability allows you to deliver the same security measures millions of times per second for fraud detection. Thus, you can easily provide the high security, that you provide in low-capacity transactions, as well as in higher capacities.

Systems that do not scale efficiently let you at a higher risk of fraud when traffic is busy.

No-Code

Modern technology infrastructures and user-friendly interfaces enable your team to easily adapt to fraud detection and prevention processes.

Fraud products that offer no-code fraud detection will increase your productivity so that lack of technical knowledge does not pose an obstacle to your security measures.

With no-code user intervention, running complex tasks and creating automations without technical knowledge frees you from a very laborious technical workload.

Flexibility – API Integration

The most critical expectation from fraud detection technologies is that always be flexible against developing fraud technologies.

Fraud detection products that offer flexibility use allow you to easily manage many of your workflows by integrating with any service or application your company uses via API gateway.

Thanks to API integrations, you can transfer data of interactions that occur in any channel to your fraud detection platform in real-time.

*

Bonus: Mobile Reporting

Here is a bonus for you.
When you find it, you should never miss it.

Fraud products that offer mobile reporting will make your life much easier so that you can be instantly informed of dangers, improvements, business processes wherever you are.

Mobile reporting applications provide you secure access to your business data and information directly from your mobile phone.

You can check your business reports, KPIs, and dashboards from your mobile phone while you are traveling, in a meeting, or in traffic.

You can also receive notifications and scheduled reports based on user groups and tasks.

06 /

How To Start Your Fraud Detection Operation

Define Goals, Metrics and Resources

No matter what project you start, your first step should be to define your goals.

- What do you aim for with fraud detection?
- What are the types of frauds that hurt you the most?
- What data do you want to measure in fraud detection? How much of this data, if any, do you keep in your systems?
- What types of fraud cases do you want to detect?
- What methods have you used before?
- What are your criteria for measuring the effectiveness of your system?
- What are your needs for your dream fraud detection operation?

Determine Proper Data Sources

After completing your goals regarding the fraud detection operation, you should focus on data sources, which is one of these goals.

Commonly used data in fraud detection systems are;

- billing data
- product usage
- risk profile
- client profile

Other data needed about clients can also be obtained from vendor companies.

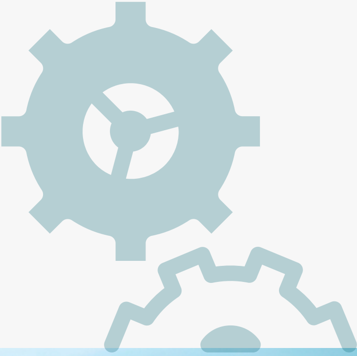
Plan the Fraud Detection System Structure

You should consider many factors when planning your fraud detection system architecture.

Fraud detection frequency determines how often you run your data through your fraud detection model. You should act in real-time in fraud detection.

The fraud detection flows affects the parameters by which you mark different fraud cases as suspicious and how you evaluate and approve these suspicious cases.

The scoring accuracy baseline is important for assessing the adequacy of your fraud scoring model.



Develop the Data Engineering and Modeling Pipelines

For the data engineering pipeline, you need to combine data from different sources, aggregate that data based on business metrics, and set operations.

For the data transformation pipeline, the main goal is to improve the quality of data. Dealing with missing and incorrect data issues and transforming data so that it can be used for machine learning models is critical.

For the machine learning model pipeline, you should focus on building and comparing diversified machine learning models based on key business metrics.

Integrate Your Fraud Detection Model Into The Case Management System

Now you have come to the last step. Now it is time to incorporate your ideal machine learning model into your case management system.

You can rank the risk levels of the cases according to the risk score you have created. You can then send a list of critically suspected cases and forward it to the authorized managers for further investigation through the case management system.

07 /

Conclusion & Next Steps

Digital fraud technologies continue to evolve, even as financial institutions and businesses adopt the latest strategies to make digital payments more secure.

The new generation of scammers is rapidly adapting to innovative technologies to steal your valuable data. To prevent fraud, you should know your vulnerabilities and familiarize yourself with proper technologies to reduce risks.

Misuse of your customer and company data will cause you significant reputational losses as well as financial losses. By adapting quickly to current technologies, you can improve your working processes for your team and your customers by getting to know the technologies with a high degree of accuracy that will not create false alarms, harm your customer experience or leave you vulnerable to fraud.

Be aware of fraud and prevent abuse of your efforts