VIEW POINT

ADDRESSING FALSE POSITIVES IN THE BATTLE TO PREVENT RETAIL FRAUD

Abstract

According to a leading global organisation in payment authentication and monitoring solutions, the third quarter of 2021 witnessed alarming statistics with regards to cybercrime. About 68% of digital banking fraud originated from mobile channels. There has been a 274% increase in brand abuse attacks and a total of 1,56,000+ online attacks have been detected.

Infosys®
Navigate your next

Another report by a leading global accounting firm states that 67% of companies have experienced external fraud in the past 12 months, and 38% expect the risk of fraud committed by external perpetrators to somewhat increase this year. Yet another study predicted merchant losses to online payment fraud will exceed $206 billion cumulatively for the period between 2021 and 2025. This makes retailers scramble for security systems to detect and prevent fraudsters in the retail space. But sometimes the cure can be more deadly than the problem. [1]

Take for instance the issue of false positives. False positives are scenarios where legitimate customers get flagged as fraudsters. The customers either get blocked from the system or have to undergo unnecessary lengthy verification processes. Could technologies such as artificial intelligence (AI) and machine learning (ML) come to the rescue and efficiently minimise false positives? Yes, and this could save retailers billions of dollars in revenue and improve brand image in this already cut-throat business.

Examining a retail customer's digital journey [8]

Today's customers are spoilt for choice. Therefore, tracking their retail journey helps retailers align their strategies and provide better customer experience. Though mapping the customers' journey can be complex, it can be construed in the following stages:

- **Awareness:** This is the initial stage where customers become aware of your product or service.
- **Consideration:** At this stage, customers find your offering valuable and consider it worthy of purchase by looking at the reviews or comparing it with the offerings of other service providers in the market.
- **Acquisition:** This is the stage where customers decide to purchase and either create new accounts or log in to an existing one. The probability of false positive is at the highest during this stage when customers place the product in their shopping carts and prepare to checkout.
- **Service:** In this stage, customers place their order and the service provider fulfils the order.
- **Loyalty:** If customers are happy with the product or the service, they are likely to repeat the order or recommend the business to their family and friends, thus creating brand loyalty and repeat business.

The key to a flawless digital journey is to realise and predict false positives before they cause damage. As most millennials prefer to use a smartphone to complete a purchase, it is essential that retailers and vendors have a false positive prediction and prevention system that is platform agnostic.

The actual cost of false positives is more than the revenue loss [2]

Revenue loss is just the tip of the iceberg, but the real damage lies under the surface. Some of the major impacts of false positives are:

- **Cart abandonment:** Most rule-based fraud detection systems are based on a simple 'yes' or 'no' logic. For example, multiple orders from the same IP address are declined because of fraud suspicion. But these could actually be legitimate orders. According to a study, 42% of customers abandon their carts if the system declines their payment method.
- **Opting to buy from a competitor:** The same study found that 40% of the customers facing false positives would rather buy from a competitor. Losing such customers could be devastating for a business. [4]
- **Negative online reviews:** It is also worth noting that about 57% of shoppers who are the victims of false positives are repeat clients. This is an alarming number and could even result in customers posting negative reviews online. These reviews generated from a false positive experience could reach thousands of existing and new customers within minutes.
- **Impact on the business metrics — CAC and LTV:** Customer acquisition cost (CAC) is the cost that the business pays to convince customers to purchase a product or a service. This includes advertising, research, and interaction time with the customers. False declines raise the cost of acquiring new customers. For example, a business that spends $100 in acquiring a new customer loses this amount in case of a false positive. Lifetime value (LTV) is the profit that the business anticipates from customer loyalty and any future purchases. Customers who are victims of false positives may stop buying from the merchant altogether, resulting in long-term revenue loss. [1]

According to a survey, about 19% of the lost customers are in the income bracket of $800,000–900,000 per annum, while 32% are in the bracket of $1+ million per annum. This causes savvy retailers to place more emphasis on preventing false positives than actual frauds.

Using technology to reduce false positives [3] [5]

AI and ML use deep learning algorithms from structured and unstructured data to build a baseline mathematical model, which helps make predictions about false positives without explicit programming. The more data (both historical and real time) becomes available, the more accurate are its predictions, resulting in identifying normal consumer spending and differentiating it from suspicious and fraudulent activities.* [6]

Here are some ways in which technology helps in detecting false positives:

- **Embracing real-time data:** Continuous learning and improvement ensures dynamic fraud scoring. Since this process is not stagnant, it helps banks and e-commerce companies identify high-risk activities before it is too late and segregate legitimate transactions from fraudulent ones. The real-time data produced should also be valid and reliable to make accurate and conclusive decisions. Using complex and highly varying functions, AI and ML systems investigate and flag frauds in real time, thus preventing any system downtime and false positives. This partnership of real-time data and continuous system uptime saves e-commerce businesses from any chargebacks and lost sales.
- **Rule-based fraud detection versus behavioural data:** Rule-based fraud detection systems are manual processes designed to detect illegitimate activities. But these systems cannot keep up with the pace at which technology is evolving. With millions of valid transactions processed every second, it is easy for fraudulent activities to sneak in undetected. Rule-based systems are also not flexible enough to keep up with the changing customer behaviour and new types of frauds globally. This often creates a large number of false positives and lost revenue that takes over 40 days to get detected. Customers now have various ways to access their financial and payment information, making rule-based systems obsolete. Traditional systems can get overwhelmed quickly as they cannot handle large volumes of data from different channels such as omnichannel e-commerce, mobile payments, IoT payments, and contactless payments. [7]

  Behavioural data, as the name suggests, learns from customers' behaviour during online transactions. This includes how they typically spend money, time, dates, spending medium, frequency, and various other metrics. This is a rich source of data to train machines on customers' buying patterns and detect fraudulent transactions.
- **Supervised versus unsupervised models:** AI can learn from data and train machines using algorithms as a set of instructions. This teaches the machines to cluster the information and identify patterns, detect irregular actions, and draw conclusions from the overall dataset. Two types of algorithms that train machines are 'supervised' and 'unsupervised.'
  - **Supervised model:** This model feeds the machine with labelled or tagged transaction details. Machines digest a vast amount of tagged information and create customer patterns that reflect legitimate transactions. As the information fed into the machine increases, the more accurate the baseline model becomes.
  - **Unsupervised model:** This process creates a baseline model without using the tags because it is difficult to identify the details that lead to a desired output. Instead, it uses a form of self-learning to reveal patterns that are invisible to other analytics models. This model identifies new fraudulent activities that were previously unknown. [6]

Some of the other benefits of ML include smarter alert triage, faster due diligence, and lower operational costs. [7]

Types of data needed to reduce false positives [7]

It is crucial to have cross-channel customer data for better fraud detection and analytics. Rather than having individual payment channels and customer segments, it is better to aggregate from cardholders' portfolio and feed it into the analytics system. The technology also helps you aggregate additional data stashed in other systems.

- **General customer data:** This is data collected as a part of the KYC process and additional information, such as account age, direct debit frequency, and existing economic relationship with other account holders within the family or with the employer.
- **Transaction data:** This data provides regular insights about the frequency, volumes, transaction types (automated clearing house [ACH], card not present [CNP], and direct debit), and the location.
- **Non-transaction-based activities:** This could be an updated email or a password with unusually high spending, indicating suspicious activity.
- **Location data:** High-volume and high-value transactions from a new IP address not associated with the account could indicate fraud, which could prevent false positives.
- **Social and mobile data:** Social and mobile data provides insights about customers' activities and monetary transactions with the people they know.

By feeding such information into an ML system, you can create high-performance analytical models. This prevents false positives and corresponding declines.

Conclusion

There is no one-stop shop to select the right AI-based algorithm. The first step in vetting an AI-based fraud prevention system is to identify your fraud prevention goals. Some of the most important questions to ask are:

- Can the solution react quickly and detect frauds in real time?
- Can the system scale up as the network of customers grows?
- Is the AI-based fraud detection system data agnostic?
- How does the system handle false positives?
- What benefits and risk analytics do the system provide?

Most e-commerce businesses and associated banks have inconsistent data stashed in multiple places. This can cause unwanted and bloated alerts, lack of customer visibility, and high cost of security screening across a large customer base. Before adopting an AI- and ML-based model, one must build a strong base for aggregating, storing, and operationalising the data.

With e-commerce transactions on the rise, especially after COVID-19, retailers cannot afford to conform to the status quo of outdated fraud detection systems. Adopting AI and ML in retail will significantly reduce false positives, leading to higher customer satisfaction and loyalty.

*For organisations on the digital transformation journey, agility is key in responding to a rapidly changing technology and business landscape. Now more than ever, it is crucial to deliver and exceed organisational expectations with a robust digital mindset backed by innovation. Enabling businesses to sense, learn, respond, and evolve like a living organism, will be imperative for business excellence going forward. A comprehensive yet modular suite of services is doing exactly that. Equipping organisations with intuitive decision-making automatically at scale, actionable insights based on real-time solutions, anytime/anywhere experience, and in-depth data visibility across functions leading to hyper- productivity, Live Enterprise is building connected organisations that are innovating collaboratively for the future.

References

1. Reducing the Risk of False Positives | PYMNTS.com
2. By the numbers: How False Declines Cost Merchants Now and in the Future
3. A major challenge: False positives
4. Why understanding your fraud false positive rate is key to growing your business
5. How AI Can Help Prevent Fraud and Save Retailers Millions
6. AI False Positives: How Machine Learning Can Improve Fraud Detection
7. How to Reduce False Positives and Improve AML with Machine Learning
8. How False Positives Disrupt the Digital Customer's Journey

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next