International Journal of Management, IT & Engineering
Vol. 15 Issue 01, January 2025,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Trust on eCommerce Platforms

Kshitij Sharma

Abstract

eCommerce Platforms face multiple types of fraud and causing revenue loss, and it has become a critical aspect to solve for them. Adoption and Implementation of Artificial Intelligence and Machine Learning based systems to make predictive decisioning is key to solving these challenges.

Keywords:

eCommerce;
Trust;
Machine Learning;
Payment Fraud;
Marketplace.

Author correspondence:

Kshitij Sharma,
Product Manager (Staff/Lead), eBay Inc, California, USA
Email: Sharma868717@gmail.com

1. Introduction

eCommerce industry has grown at a rapid pace in the last few years. A lot of trust in these online marketplaces stem from the use of fraud detection and prevention solutions. Marketplace platforms are typically two sided, eg. Amazon, eBay, but nowadays there are a lot of three-sided platforms bringing in the third side through gig economy, eg. Doordash, Uber. Ensuring that the customer feels safe and trusted is one of the key areas to drive recurring purchases and build a long term relationship. Trust can be evaluated based on the amount of fraud and the different types of fraud that happen in eCommerce Marketplaces.

2. Types of eCommerce Fraud

Fraud in online marketplaces can be categorized into four major areas:

1. Account Fraud: Common example of this is 'Account Takeover'. This is characterized when a malicious entity is able to login to the user's account.
2. Payment Fraud: Payment fraud is characterized when a bad actor uses stolen payment information to make purchases.
3. Seller Fraud: This happens when the Seller intends to use fraudulent items for selling.
4. Buyer Fraud: Buyers drive this behavior by doing fraudulent returns or chargebacks.

These fraud components build negative pressure on growth of the company, both from a consumer (buyer/seller) and operational cost of the company.

3. Payment Fraud Categories

Payment fraud is one of the biggest challenges that financial institutions and banking companies face. It is estimated that more than ~$40 Billion are lost because of fraud every year.
Payment fraud can be segmented in three key areas:

· Card Fraud (Credit/Debit): It is the unauthorized use of a Credit or Debit card to make a purchase.
· Account Fraud/Takeover: This is when a fraudster takes over the bank or identity and makes fraudulent transactions (transfers, withdrawals, purchases etc.)
· 3rd Party Apps Fraud: This is associated with fraud that happens on third party applications such as Venmo, Zelle, Cash App etc on which customer's bank account or card information was associated.

There are other areas of financial fraud as well, such as check fraud, and compliance/regulatory fraud, such as money laundering etc. Solving these frauds is a key aspect for a successful payment focused company. Focusing on Card Fraud, the responsibility of stopping this resides on both the financial institution and the retailer at the point of purchase. From a customer perspective, the customer will eventually ask for a chargeback (aka return of the money) as this was a fraudulent transaction. Now the financial institution will work with the retailer to determine the fraud and if the chargeback is valid. Depending on how fraud is determined, either the retailer or the financial institution will take a loss of the chargeback and return the money to the customer. Thus, the need for both the retailers and financial institutions to have payment specific fraud detection systems. Financial institutions or payment providers develop their own solutions or can partner with another company for this functionality.

4. Fraud Detection Flow

Understanding the flow for web payment processing fraud detection, the Financial Institution will make decisions based on the data and model evaluation of the decision system. As a request is made through an API for payment, the merchant will do initial analysis by running risk models and then send a response to the Financial Institution. The Financial Institution will then make a further assessment on the payment request through its own risk assessment model and send a feedback to the merchant with a final assessment of success or decline. The whole process can take from a few milliseconds to a few seconds depending on the capabilities of the merchant and the financial institution.

One of the big challenges that happen during the flow is the time taken by these systems to make the evaluation. As the evaluation time becomes longer, the good customers feel frustrated, and could thus abandon the payment or checkout. This creates a dual challenge of managing customer expectations with a frictionless experience and reducing fraud.

SLA improvements can be done by deploying faster API's and SDK's, and enabling these to improve data signals that improve the performance of the fraud detection models. For example, Stripe has called out performance SLA's of 100ms for its fraud detection product 'Radar' and specifically calls out '36%' improvement in fraud detection if Stripe's SDK's are adopted, thus confirming the success of this strategic approach.

4. AI & ML Models

One key initiative that has enabled these marketplaces to fight back against fraud is through the adoption of strong machine learning and artificial intelligence technologies. Specifically, the key outcome is predictive decisioning, which can be defined as being able to predict the next action based on the existing data that is fed into the models. From a buyer/shopper journey, the buyer logs into the account, identifies the item, and then completes the purchase. If the buyer is unhappy, then can decide to return the product.

As organizations are in early stages, they tend to focus on specific areas to reduce fraud and move fast, e.g Account Takeover at Login, Payment Fraud at Checkout. The fraud detection systems tend to function excellently at solving their specific usecases. As these system's use ML modeling to stop fraud, the models are evaluated based on F scores, Precision, Recall, Accuracy etc.

Precision: True Positives / (True Positives + False Positives)
Recall: True Positives / (True Positives + False Negatives)

Recall is defined as positive observations are not missed, a fraud detection system that is trying to ensure that all good users pass through. Precision focuses on ensuring what is being predicted is correct, a fraud detection system that is allowing fewer fraud users to pass through.

4. Balance for Recall and Precision

As organizations grow, they start using specialized fraud systems to manage each use case. For each fraud system, when organizations tend to focus more on Recall, they are focusing on minimal friction for good users, but run the risk of allowing fraudsters to succeed. If the focus is more on Precision, then the system could have higher friction for good users even if it is tougher for fraudsters to pass through. Each organization manages these decisions on what's the focus area and how to manage the outcome of these. As these shopping platforms grow larger, these multiple focused systems tend to be overly complex, thus the need for a more end-to-end fraud system that connects these individual fraud detection systems.

In an ideal state, both the Precision and Recall are equal to 1, as this would be the perfect state. There is typically a push and pull challenge between Precision and Recall, as the company tries to perfect one, the other metric degrades, and this is not a great experience for the good customers. To maximize the outcome, the best approach is to evaluate a Precision-Recall Curve. This curve can be built by using the Precision and Recall on the two axes, and evaluate the impact (customer feedback, fraud costs, fraud reduction etc.) as we try to find the most optimal state for the fraud system on the curve. Another metric is ROC (Receiver Operator Characteristic), as this is the balance between the True Positive Rate and False Positive Rate, and can be measured by the AOC (Area under the Curve), which is another way to maximize outcome from these evaluation models.

4. Conclusion (10pt)

The criticality of a more end to end fraud detection has become evident as fraud has also evolved into the social behavior inside the marketplace. Some examples where fraud can possibly be found is seller and item review system system, inappropriate messaging behavior, or even fraudulent complaints against a user. These types of social fraud in ecommerce can be restricted by building an end to end fraud management system that evaluates customer behavior from all areas: account, payment, shopping, and usage. The success of this system again depends on how well it can predict behavioral patterns, thus again the need for strong machine learning models that connect all individual evaluation systems.

References(10pt)

1. US online retail sales to reach $1.2 trillion this year: report
2. Payment fraud 101: What businesses need to know | Stripe
3. PayPal to Acquire Simility to Expand Global Merchant Offerings Visa to Acquire Featurespace
4. Prevent Retail Payment Fraud | Mastercard Developers
5. Send complete fraud signals | Stripe Documentation
6. Ecommerce fraud trends and statistics merchants need to know in 2024
7. What Are Machine Learning Performance Metrics? | Pure Storage