International Journal of Engineering & Scientific Research
Vol.13 Issue 01, January 2025
ISSN: 2347-6532 Impact Factor: 8.076
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-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Risk Systems and Remediation

Kshitij Sharma

Abstract

Online shopping platforms face multivariate levels of risk, and thus need dedicated systems to detect and mitigate them. Additionally, remediation paths are needed for improved customer experience.

Keywords:

eCommerce;
Risk Modeling;
Risk Remediation;
Marketplace.

Author correspondence:

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

1. Introduction

Leveraging Risk Models to stop bad actors is now a standard system that is adopted across the eCommerce Industry. Risk Systems not only stop consumer fraud use cases, but also focus on stopping targeted hacks or virus attacks. As these systems focus more on safeguarding the customer information, they also have Know Your Customer (KYC) or Remediation path for customers who get locked because of Risk evaluations.

2. Understanding Risk Categories

Risk at eCommerce platforms can be divided in the three key categories:

1. Cybersecurity: Cybersecurity is protecting the systems, networks, and data from software or online attacks (virus, malware etc.).
2. Compliance: Ensuring compliance and adherence to Regulatory, Financial, and Retail Standards
3. Consumer Fraud.: Consumer fraud includes Chargeback Fraud, Card Fraud, Return Fraud, Fake Item fraud etc.

There are categories eg. Strategy, Company Financials etc, which are outside the preview of Risk and Fraud Detection systems and their remediation methods.

3. Cybersecurity

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These attacks can be broadly segmented into two areas: gain data or information; and second to disrupt a service. The first type of digital attacks focus on sensitive information with the goal of accessing them. The entry point for these attacks are virus, malware, phishing attacks etc. Companies solve these challenges by adopting specific solutions such as antivirus, systems security applications etc.

DDoS (Distributed Denial of Service) is another type of Cybersecurity attack in which fraudsters send high traffic to website servers, thus causing the service to become nonfunctional, and make the website unreachable.

Setting up a clear solution for DDoS has become a basis for a successful operation of an eCommerce Shopping Platform. Most solutions for DDoS now provide three step strategy:

1. Detection: Identify and differentiate a DDoS attack against regular traffic.
2. Mitigate & Respond: Respond with mitigation strategies, such as managing load at Application and Network levels.
3. Adapt: Evolve existing Detection and Mitigation to improve as newer fraud types are identified.

Deployment of Cybersecurtiy solutions that execute on all three levels are critical for online and web businesses.

4. Compliance & Regulatory

eCommerce companies need to follow set forth compliance and regulatory requirements to fulfill legal requirements and customer trust. Compliance and Regulatory can come from government driven entities or industry self-regulated committees as well. The goal of these remains the same: ensure a safe and trusted environment for buyers and sellers. Some key areas of Regulation and Compliance are:

1. Data: Data Privacy Standards, such as GDPR for the European Union focuses on Data Protection Rights.
2. Payment: Focus specifically on Payment specific data regulations such as PCI.
3. Product: Focuses on legal requirements, item categories, environmental impact, and safety of customers and employees.
4. Taxation: Ensuring compliance for taxation as per the requirements of local and regional governmental laws.

As a shopper on ecommerce marketplaces, consumers expect all compliance, and regulatory requirements are being implemented and followed. For any non-compliance, businesses can face regulatory implications. More importantly, because of any non-compliance, consumers lose trust, and the ecommerce company could see decline in customer engagement and growth.

4. Consumer Fraud

Buyer side frauds are primarily Chargebacks, Returns Fraud, and Item Not Received fraud. Chargeback fraud is when the user knowingly makes a purchase, and then decides to file a chargeback with the Card/Payment, claiming that this purchase was not made by them. Return fraud is when the buyer decides to return a fraudulent item instead of the real purchase item, thus keeping the original item and also getting the money back. Item not received fraud is when the buyer marks the item as not received and asks for the money back, even though it was delivered. All these frauds cause operational losses and create pain for Sellers, impacting Seller sentiment for the eCommerce company.

4. Remediation for Customers

Remediation can be defined as the process of identifying and fixing any challenges or problems. For businesses, remediation focuses on getting systems back to work, which is defined as part of the risk strategy planning.

Cybersecurity mitigation for different types of attacks is key to business continuity. For example, for an DDoS attack, mitigation strategies include redirecting internet traffic and managing and monitoring different traffic from different data center's; thus, evaluating and redistributing traffic accordingly. Payment Multi-Acquirer Strategy defines the approach to integrate with more than one payment processor or a gateway that is then connected to more than one acquirer. This enables businesses to reduce operational costs, manage payment processing volume, and manage payment traffic across processors as a remediation strategy for any processor outage.

Cybersecurity and Payment Processor strategy are key functional aspects for businesses but are not something that the end shopper sees or feels on day-to-day experience. Remediations for Account/Login and Payment Instrument need end customer or shopper intervention. As the Risk model evaluates a threat, one strategy includes to restrict access to the account and ask the customer to complete an authentication or remediation step to provide access back to the account. Account and Login remediation has a lot of options, such as reentering password, PIN, or OTP. All these options fall under the MFA (Multi-Factor Authentication) umbrella. From a Payment threat perspective, a remediation that is widely used is reentering the AVS (Address

Verification Service) and CVV (Card Verification Value) for that Credit/Debit card. Typically, AVS is evaluated first if the risk or threat models term the transaction as risky for cards that are on file. Once the risk model returns the possibility of fraud, the risk strategy can define re-entering both the Address and the CVV details for the payment instrument.

References(10pt)

1. https://azure.microsoft.com/en-us/products/ddos-protection/
2. https://aws.amazon.com/compliance/gdpr-center/
3. https://stripe.com/en-pl/guides/pci-compliance
4. https://www.ey.com/en_us/services/tax-compliance
5. https://www.cloudflare.com/learning/ddos/ddos-mitigation/
6. https://www.mastercard.com/gateway/expertise/insights/monoline-vs-acquirer-agnostic.html
7. https://www.okta.com/blog/2024/10/okta-identity-security-posture-management-and-workflows-automated-detection-and/