Global Journal of Commerce & Management Perspective

OPEN ACCESS Freely available online

Short Communication

Investigation of Fraud Warning in E-commerce

Claudia Colicchia*

Department of Economics, Harvard University, Cambridge Street, Cambridge, USA

DESCRIPTION

Any fraud that exists on an e-commerce platform is referred to as ecommerce fraud. Ecommerce fraud can take many different forms, ranging from using a stolen or phone credit card, assuming a false identity, and affiliate fraud advertising. You as a retailer bear this expense when a customer commits fraud on your online business, which has a detrimental effect on your revenue. Online fraud can be carried out with personal and credit card information, unlike fraud carried out in a specific place where the card must be present during the transaction. Hackers have been known to steal financial and personal data and resell it on the dark web [1]. There are various sorts of customer fraud, such as friendly fraud, when the customer knowingly makes a chargeback to obtain a free product and avoid payment, though this type of criminal fraud is more severe. Due to time and resource limitations, the difficulties of obtaining evidence, and other factors, convictions are infrequent, which contributes to the prevalence of ecommerce fraud today. In order to avoid fraud on your platform and lessen its effect on your business, it is best to integrate a top-notch fraud detection and prevention management system. This is because ecommerce fraud prosecutions are exceptional. Ecommerce fraud is sophisticated and constantly changing as scammers use more sophisticated methods every year. While you must always be correct, malicious actors only need to be correct once. Let's examine the most typical sorts of fraud on an online store before we look at prevention methods [2].

Types of e-commerce frauds

- Identity theft
- Merchant fraud
- Check fraud

Identity theft: Identity theft will always be a serious concern for everyone, especially for online businesses, credit firms, and banks, regardless of the period. Hackers assume the account owner's identity and make transactions, for example, with stolen credit card information. They may effortlessly purchase what they want online at the expense of the credit card owner as long as they have the individual's personal data such as name, address, phone number, and credit card details [3].

Merchant fraud: Merchant fraud is quite frequent, specifically online. It is also the reason why many individuals are suspicious about non-cash-on-delivery transactions. In merchant fraud, an e-commerce shop receives and confirms an order, but no product or service is supplied, and no chargebacks are permitted. Merchant fraud is also known as online fraud [4].

Check fraud: It is fraudulent even to write a check while being aware that there is insufficient money in the account. Another instance of check fraud is when someone uses another person's cheque to make purchases or payments while impersonating them.

CONCLUSION

People should be cautious of phone calls requesting their Social Security numbers and other personal information from the federal government. Some scammers will also approach and offer things in return for money. Mysterious emails that require the recipient to enter their login information in the link could be scamming people. The fraudsters can now utilize the users' login details to steal their accounts after they click the link and provide their information. Another apparent symptom of fraud would be when scammers request money transfers from their victims.

When money is wired, it cannot be undone, and the culprit has almost immediate access to the funds. Almost everybody can become a victim of fraud; it doesn't matter what one's financial situation is. Fraudsters depend on anyone who will fall for their trap; they don't just target the wealthy. So everyone needs to be on guard.

REFERENCES

1. Wang D, Chen B, Chen J. Credit card fraud detection strategies with consumer incentives. Omega. 2019;88: 179-95.
2. Robinson C. Disclosure of personal data in ecommerce: A cross-national comparison of Estonia and the United States. Telemat. Inform. 2017;34(2): 569-82.
3. Lucas Y, Portier PE, Laporte L, He-Guelton L, Caelen O, Granitzer M, et al. Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. Future Gener Comput Syst. 2020;102: 393-402.
4. Shandan Z, Dan F, Yunyun X, Yonghai Z. Influencing factors of credibility in C2C ecommerce web sites. Procedia Eng. 2012;29:509-13.

Correspondence to: Claudia Colicchia, Department of Economics, Harvard University, Cambridge Street, Cambridge, USA, E-mail: claudia.colicchia85@polimi.it

Received: 28-Nov-2022, Manuscript No. GJCMP-22-21064; **Editor assigned:** 02-Dec-2022, PreQC No. GJCMP-22-21064 (PQ); **Reviewed:** 16-Dec-2022, QC No. GJCMP-22-21064; **Revised:** 23-Dec-2022, Manuscript No. GJCMP-22-21064 (R); **Published:** 30-Dec-2022, DOI: 10.35248/ 2319-7285.22.11.018.

Citation: Colicchia C (2022) Investigation of Fraud Warning in E-commerce. Global J Comm Manage Perspect. 11: 018.