THE ROLE OF DEVICE FINGERPRINTING, USER BEHAVIOR, AND SHIPPING ADDRESS IN PREVENTING PROMOTION ABUSE IN INDONESIAN E-COMMERCE PLATFORMS

Eric Fo Candra[1]
Universitas Kristen Indonesia, Jakarta, Indonesia
fochandra@gmail.com

Lis Sintha[2]
Universitas Kristen Indonesia, Jakarta, Indonesia
lis.shinta@uki.ac.id

Denny Tewu[3]
Universitas Kristen Indonesia, Jakarta, Indonesia
denny.tewu@uki.ac.id

Abstract

This research investigates the utilization of device data to identify user behaviors associated with promotion abuse on Indonesian e-commerce platforms. Promotion abuse refers to fraudulent activities where individuals exploit promotional systems, often by creating multiple fake accounts or using the same device for claims repeatedly. The purpose of this study is to examine the relationship between device fingerprinting, user behavior patterns, shipping address data, and the effectiveness of fraud prevention systems. Using a quantitative approach, data were collected from fraud reports made between June 2018 and May 2019. Multiple regression was applied to test the proposed hypotheses. The findings show that device fingerprinting, user behavior, and suspicious delivery address variables significantly affect fraud detection effectiveness. This study highlights the importance of integrating behavioral analysis and device-based data into fraud detection systems to proactively minimize promotional abuse. These insights provide practical implications for e-commerce companies looking to improve their digital security measures and maintain consumer trust.

Keywords: Promotion Abuse, Fraud Prevention, Device Fingerprinting, User Behavior, E-Commerce

INTRODUCTION

The rapid development of digital technology has transformed the way people conduct financial transactions, particularly through the growing use of e-commerce platforms. In response to the competitive market landscape, many e-commerce companies offer various promotional programs, such as discounts, cashback, and loyalty rewards, to attract and retain customers. However, these promotional efforts have given rise to a significant challenge known as promotion abuse, where users exploit system vulnerabilities for personal gain. This fraudulent behavior often involves creating fake accounts, manipulating system algorithms, or repeatedly using the same device to claim benefits illegitimately. According to recent global fraud assessments, promotion abuse contributes significantly to financial losses in the digital commerce sector.

Previous research has identified the effectiveness of device data particularly device fingerprinting in detecting repeated patterns of misuse across multiple accounts. While studies such as Gupta and Sharma (2020) and Zhou et al. (2021) have highlighted the technical potential of such approaches, most existing literature has focused on global or regional contexts and lacks depth in examining the behavioral aspect of fraud in Indonesia unique digital landscape.

This study offers a novel contribution by examining the combined influence of device fingerprinting, user behavior patterns, and shipping address data on fraud detection systems within the Indonesian e-commerce environment. The research addresses the gap in localized fraud detection strategies by leveraging behavioral analytics in conjunction with device data to enhance the accuracy and responsiveness of fraud prevention mechanisms.

The objective of this research is to analyze how device fingerprinting, user behavior patterns, and shipping addresses affect the effectiveness of fraud prevention systems. The findings are expected to offer practical implications for e-commerce companies in developing more robust fraud detection frameworks, while also enriching the academic discourse on digital fraud prevention.

LITERATURE REVIEW

Theory

The study of fraud prevention in digital ecosystems has evolved significantly, particularly with the introduction of data-driven technologies in e-commerce platforms. A foundational framework for understanding fraudulent behavior is the *Fraud Triangle Theory* proposed by Cressey (1953), which identifies three elements pressure, opportunity, and rationalization as key factors influencing fraudulent behavior. These dimensions explain why individuals commit fraud when given a perceived necessity, access, and justification.

Complementing this, the *Attribution Theory* (Heider, 1958; Robbins & Judge, 2017) posits that behavior can be attributed to internal or external causes. In fraud contexts, internal factors such as personal pressure or rationalization combine with external system vulnerabilities to produce misconduct. Applying this framework, promotion abuse in e-commerce, such as exploiting promotional loopholes through multiple fake accounts or repeated device use, can be viewed as a product of these interacting factors.

Moreover, *Risk Management Theory* (Fayol, 1916; Gallagher, 1956) provides the rationale for institutional responses to fraud by emphasizing systematic identification, assessment, and control of risks. Integrating these theories offers a holistic view of fraud in e-commerce, especially as platforms struggle to balance user incentives with risk controls.

Empirical research has increasingly focused on device-based fraud detection. Gupta and Sharma (2020) demonstrated that device fingerprinting allows the detection of fraudulent patterns across multiple user accounts. Zhou et al. (2021) confirmed that repeated promotional claims from the same device are strong indicators of abuse. More recently, Byrapu Reddy et al. (2024) highlighted that combining device characteristics, user behavior patterns, and geographic data enhances fraud detection. Tan and Wong (2021) further stressed that fraud detection systems improve not only technical detection but also user trust in the platform.

However, most of these studies have been conducted in global contexts with limited exploration of localized behavioral patterns. Additionally, few have examined the effect of shipping address data as a predictor in fraud detection, which may reveal patterns in fraudulent clusters or reinforce legitimacy in user transactions.

This study fills that gap by analyzing the direct influence of Device Fingerprinting (X_1), User Behavior Patterns (X_2) and Shipping Address Data (X3) on fraud detection effectiveness (Y). This model extends the fraud triangle by integrating digital identity markers and behavioral analytics into the risk assessment process, focusing solely on direct effects without testing moderating or interaction relationships.

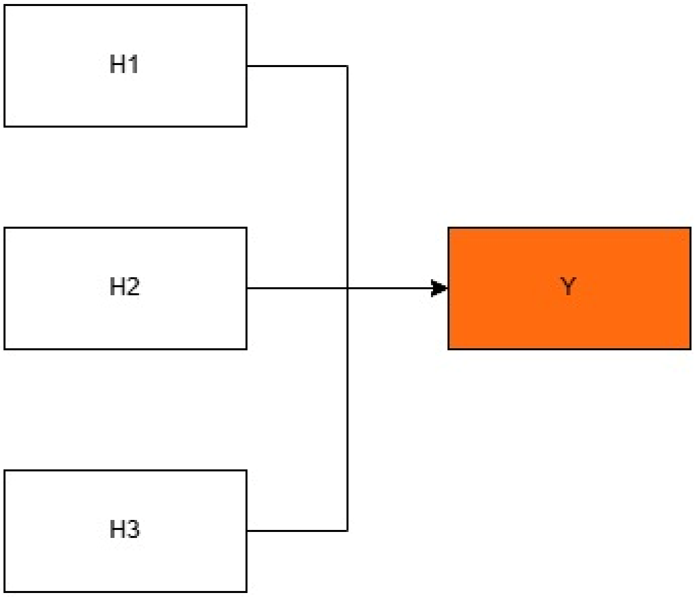

Figure 1.
Conceptual Framework

Hypotheses

Based on the theoretical and empirical foundations above, the following hypotheses are proposed:

H1: Device Fingerprinting (X1) has a significant effect on fraud detection effectiveness (Y).
H2: User Behavior Patterns (X2) have a significant effect on fraud detection effectiveness (Y).

H3: Shipping Address Data (X3) has a significant effect on fraud detection effectiveness (Y). The conceptual model representing these relationships is shown in Figure 1.

RESEARCH METHOD

This study employed a quantitative research design using a descriptive-associative approach to examine the relationship between device fingerprinting (X1), user behavior patterns (X2), and shipping address data (X3) on fraud detection effectiveness (Y). The research utilized secondary data derived from internal fraud monitoring reports of a leading Indonesian e-commerce company, covering transaction records flagged for suspected promotion abuse between June 2018 and May 2019.

The population comprised all user transactions that occurred on the platform during the specified timeframe. Samples were selected using purposive sampling techniques, focusing on transactions identified by the anti-fraud system as having indications of repeated device usage, abnormal behavioral patterns, and overlapping shipping addresses.

The independent variable X_1 (device fingerprinting) is measured through the identification of unique device characteristics and the frequency with which a device is associated with multiple user accounts. The second independent variable, X_2 (user behavior patterns), is assessed by analyzing the frequency and timing of transactions, as well as the similarity of repeated behaviors across user profiles. The third independent variable, X3 (shipping address), reflects address repetition, postal code overlap, and the presence of the same shipping details used across multiple accounts. The dependent variable, Y (fraud detection effectiveness), is operationalized using the level of fraud identified per rule or pattern as reported by the fraud detection system.

All variables were measured using interval scales, expressed in percentages and frequencies corresponding to fraud incident rates associated with each detection category. Data collection was conducted through the extraction of anonymized transaction logs and fraud detection flags from the company's rule-based system.

The statistical analysis was performed using SPSS version 27. Prior to hypothesis testing, classical assumption tests were conducted to ensure model validity, including tests for normality, multicollinearity, heteroskedasticity, and autocorrelation. Hypothesis testing was carried out through multiple linear regression analysis to examine the direct effects of X_1, X_2, X3 on Y. The structural model tested in this study was formulated as follows:

Model 1 – Direct Effects:

$$Y=\beta 0+\beta 1X1+\beta 2X2+\beta 3X3+\epsilon$$

The study was conducted in Jakarta, Indonesia, with data processing and analysis taking place between March and April 2025. The research strictly adhered to ethical standards and data protection regulations by exclusively utilizing anonymized datasets to ensure participant confidentiality.

RESULTS AND DISCUSSION

This study aimed to analyze the influence of device fingerprinting (X_1) and user behavior patterns (X_2) on fraud detection effectiveness (Y), while also evaluating the role of shipping address data (X3). The analysis was conducted using multiple linear regression testing through SPSS version 27.

Table 1.
Results of Hypothesis-testing

Hypothesis	Relationship	Coefficient (Beta)	T-stat	P-value	Conclusion
H1	Device Fingerprinting (X1) → Fraud (Y)	0.646	5.318	<0.001	Supported
H2	User Behavior Patterns (X2) → Fraud (Y)	0.440	3.016	0.017	Supported
H3	Shipping Address (X3) → Fraud (Y)	0.406	2.707	0.027	Supported

$$\mathbf{Y= -1{,}658 + 1{,}315\ X1 + 0{,}839\ X2 + 1{,}553\ X3 + e}$$

The results show that device fingerprinting has a statistically significant and positive effect on fraud detection effectiveness (H1 supported), with a beta coefficient of 0.646 and a p-value < 0.001. This indicates that devices reused across multiple accounts are strongly associated with fraudulent activity, particularly promotion abuse. This finding supports the Fraud Triangle Theory, where opportunity in this case, access via shared devices facilitates fraud. It also confirms the relevance of technical indicators in fraud prevention, as previously highlighted by Gupta and Sharma (2020).

Likewise, user behavior patterns (H2) demonstrated a significant and positive effect on fraud detection outcomes, with a beta of 0.440 and p-value of 0.017. Behavioral traits such as high-frequency transactions, repeated use of promotional codes, and short-interval activities are predictive of exploitation intent. These findings are aligned with Zhou et al. (2021), who showed that behavioral clustering is a common signal in fraud networks.

The regression also showed that shipping address (X3) has a significant direct effect on fraud detection effectiveness (H3 supported, p = 0.027). Addresses used repeatedly across accounts or those with postal code overlaps are red flags in fraud detection. This supports the importance of incorporating contextual data into fraud monitoring systems

CONCLUSION

This study concludes that device fingerprinting, user behavior patterns, and shipping address data each have a significant and direct influence on fraud detection effectiveness in e-commerce platforms. The use of the same device across multiple accounts and patterns of repeated suspicious behavior are strong indicators of promotion abuse. These findings support the effectiveness of combining technical device identification with behavior-based analysis in identifying fraudulent activities.

The analysis also demonstrates that shipping address data independently contributes to fraud detection. The study is limited by its use of data from a single e-commerce platform over a specific time period. The use of anonymized data also limits the ability to perform deeper user-level segmentation or real-time tracking. These limitations suggest caution when generalizing the findings across broader contexts.

Based on the findings, it is recommended that e-commerce platforms implement fraud detection systems that integrate device-level fingerprinting with user behavior analytics and shipping address verification. Attention should be given to tailoring fraud detection rules that distinguish between technical indicators and behavioral markers. For future research, expanding the model to include variables such as payment methods, account linkage networks, and geolocation metadata may further enhance fraud detection accuracy and adaptability.

REFERENCES

Byrapu Reddy, S., Kumar, R., & Tan, Y. (2024). Leveraging device data for fraud detection in e-commerce. *International Journal of E-Business Research, 20*(1), 56–70.

Cressey, D. R. (1953). *Other peoples money: A study in the social psychology of embezzlement*. Free Press.

Fayol, H. (1916). *General and industrial management*. (Reprinted 1949). Pitman Publishing.

Gallagher, R. S. (1956). The case for risk management. *Harvard Business Review, 34*(5), 45–52.

Gupta, S., & Sharma, P. (2020). Fingerprinting technologies for fraud detection in e-commerce systems. *Journal of Cybersecurity and Digital Forensics, 7*(1), 33–45.

Heider, F. (1958). *The psychology of interpersonal relations*. Wiley.

Robbins, S. P., & Judge, T. A. (2017). *Organizational behavior* (17th ed.). Pearson Education.

Tan, L., & Wong, Y. (2021). Data-driven approaches to combatting e-commerce fraud. *Asia Pacific Journal of Information Systems, 31*(2), 142–160.

Zhou, H., Li, J., & Wang, T. (2021). Behavioral patterns in fraudulent activities: A case study on promotion abuse. *Journal of Electronic Commerce Research, 22*(2), 67–81.