LEVERAGING ARTIFICIAL INTELLIGENCE FOR FRAUD RISK PREVENTION IN THE GROWING E-COMMERCE SECTOR

Mykhailo Pyrkh[1]

DOI: https://doi.org/10.30525/978-9934-26-498-6-37

The rapid expansion of e-commerce has transformed global markets, with most money now existing as electronic data. Israeli historian Yuval Noah Harari estimates that of the $60 trillion global money supply, less than $6 trillion is in physical form, with over 90% (more than $50 trillion) existing only as digital records [1].

Global e-commerce revenues are expected to reach $4,117 billion by 2024, with a 9.49% annual growth rate (CAGR) from 2024 to 2029, resulting in a market value of $6,478 billion by 2029. China is forecasted to lead, with revenues of $1,469 billion in 2024. User penetration is anticipated to increase from 40.5% in 2024 to 49.1% by 2029, with an average revenue per user (ARPU) of approximately $1,620 [2].

While e-commerce expands, it also exposes businesses to significant fraud risks, posing substantial challenges for online merchants. In 2021, global payment card fraud reached $22.8 billion, a 4.4% increase from 2020, with the United States representing 38.7% of incidents [3]. U.S. fraud losses alone reached $8.45 billion in 2021, with potential losses projected to exceed $28 billion by 2030 [4]. Effective fraud risk management is essential to maintain transaction integrity and consumer trust.

In e-commerce, fraud risks can be divided into universal and industry-specific categories, enhancing merchants' understanding and management of complex fraud risk. Strategic risks involve inadequacies in fraud prevention strategies and the inability to adapt to evolving fraud tactics, underscoring the need for a resilient fraud risk management plan. Market risks arise from regulatory changes, shifts in consumer behavior, and competitive pressures, which affect the types and frequency of fraud encountered. Credit risks in e-commerce include fraudulent credit transactions, such as chargebacks, which directly impact revenue. Fraud can also disrupt cash flow, leading to liquidity risks, especially through mechanisms like refund fraud. Financial risks encompass direct losses from unauthorized transactions, chargebacks, and account takeovers.

[1] Zaporizhzhya National University, Ukraine

Technological vulnerabilities present industry-specific risks, including the use of insecure payment gateways, weak website security, and susceptibility to cyber-attacks such as phishing and hacking. Operational risks arise from inefficiencies in fraud prevention processes, such as inadequate personnel training and the absence of automated detection tools, leading to delayed responses.

Informational risks, particularly data integrity and security breaches, are critical in the e-commerce sector due to the dependency on sensitive customer data. Breaches can expose merchants to substantial reputational and financial damage, as compromised data often fuels further fraudulent activity [8].

The rise in e-commerce fraud has necessitated sophisticated defense mechanisms. Artificial Intelligence (AI) and Machine Learning (ML) play a transformative role in managing e-commerce fraud risk, enabling businesses to analyze vast datasets, including customer and transaction data, to identify patterns and anomalies indicative of fraud [5].

AI fraud detection systems establish baseline behavior patterns and continuously monitor data for deviations. As data diversity increases, AI models fine-tune their parameters, enhancing accuracy in fraud detection. Key mechanisms in AI fraud detection include data collection, feature engineering, model training, anomaly detection, continuous learning, and alerting and reporting. Aggregating large transactional data volumes and identifying indicators of fraud enable AI systems to detect potential threats effectively. With the ability to adapt to evolving fraud tactics, AI systems provide robust security [6].

AI can detect multiple types of e-commerce fraud. Payment fraud includes unauthorized transactions using stolen data. Chargebacks, when a cardholder disputes a transaction, often lead to losses for merchants. Account takeover (ATO) involves unauthorized access to user accounts, often through phishing or stolen credentials. Fake account creation involves the use of false or stolen information for identity theft or promotional abuse. Content scams and spam consist of deceptive or unsolicited content that targets users to extract information [7].

AI is essential in managing e-commerce fraud risks, enabling precise and adaptive fraud detection. Machine learning algorithms allow businesses to respond proactively to evolving fraud tactics, reducing financial losses and maintaining consumer trust. Integrating AI in fraud risk management strengthens the security framework necessary for sustainable growth in digital commerce.

References:

1. Harari Y. N. (2023) *Sapiens: A Brief History of Humankind* / Trans. from English by O. Demianchuk. Kyiv: Bookchef, 230 p. [In Ukrainian]

2. *Credit card ownership (% age 15+)*. URL: https://genderdata.worldbank.org/en/indicator/fin7-t-a?view=trend&geos=WLD&gender=total&gender=female&gender=male

3. *E-commerce fraud – statistics & facts*. URL: https://www.statista.com/topics/9240/e-commerce-fraud/#dossierKeyfigures

4. Drimer S., Murdoch S. J., Anderson R. (2009) *Optimized to Fail: Card Readers for Online Banking*. In: Dingledine, R., Golle, P. (eds). *Financial Cryptography and Data Security. FC 2009*.

5. *Ecommerce Fraud Prevention: How AI Detects & Blocks Fraudulent Activity (The Ultimate Guide)*, Charter Global, June 14, 2024. [Online]. URL: https://www.charterglobal.com/ai-for-ecommerce-fraud-detection/

6. *Understanding AI Fraud Detection and Prevention Strategies*, Digital Ocean, 2021. [Online]. URL: https://www.digitalocean.com/resources/articles/ai-fraud-detection

7. *How to Use AI in Fraud Detection*, Sift Trust and Safety Team. URL: https://sift.com/blog/what-is-an-otp-bot

8. Savchuk V. (2024) *Risk Management*. Kyiv: Laboratory. P. 89. [In Ukrainian]