

ENHANCING PAYMENT SECURITY IN UKRAINIAN E-COMMERCE: A MODEL-BASED APPROACH TO CHARGEBACK RISK MANAGEMENT

Kira HORIACHEVA, Yuliia TURCHENKO

Taras Shevchenko National University of Kyiv, Military Institute, Kyiv, Ukraine
yuliiaturchenko@gmail.com, horyachevakira@gmail.com

Abstract: *The rapid expansion of e-commerce has introduced new challenges in transaction risk management, particularly in the domain of chargebacks. These disputes not only disrupt business operations but also represent a growing threat to financial stability in digital markets. This paper presents a model-based approach to analysing chargeback risk in e-commerce, with a specific focus on the Ukrainian context. Using data from two e-commerce enterprises and applying both regression and machine learning methods, the study investigates the influence of key transaction parameters, namely payment amount, security level, and issuing bank characteristics, on the likelihood of chargebacks. The findings confirm that unsecured and high-value transactions are most vulnerable, and that regional banking policies significantly affect dispute rates. In the case of Ukraine, the growing adoption of digital payments, combined with a still-evolving regulatory framework, highlights the urgent need for predictive risk models. Based on the analysis of these three core factors, the paper proposes targeted mitigation strategies that can help businesses reduce financial losses and improve resilience. These insights are especially relevant for enterprises operating in Eastern European and post-Soviet markets, where chargeback dynamics are under-researched but increasingly impactful.*

Keywords: e-commerce, chargeback, machine learning, predictive modelling, Ukraine

1. Introduction

The rapid growth of electronic commerce (e-commerce) has become one of the defining trends of the global economy over the past decade. With increasing internet penetration, mobile device usage, and digital literacy, consumers worldwide have shifted toward online shopping and cashless payments. Electronic Payment Systems (EPS) have played a pivotal role in this transformation, enabling fast, secure, and convenient transactions. However, this shift has also introduced a range of operational and financial risks for merchants – among them, the growing challenge of chargebacks.

A chargeback refers to a payment reversal

initiated by a consumer through their issuing bank, typically as a result of suspected fraud, dissatisfaction with a product or service, or misunderstanding of a transaction. While intended to protect consumers, chargebacks also create significant burdens for businesses, including revenue loss, increased processing costs, and potential reputational damage. In extreme cases, excessive chargeback rates can trigger penalties or account suspensions from payment networks such as VISA and Mastercard.

In Ukraine, the rise of e-commerce has been particularly rapid in recent years, driven by digitalisation reforms and the resilience of the payment infrastructure during crisis

conditions, including wartime. According to national and international reports, over 60% of consumer payments in Ukraine are now conducted via non-cash methods. The adoption of digital wallets, card payments, and mobile payment platforms has accelerated, yet regulatory protections and consumer awareness regarding transaction disputes remain less developed compared to Western markets. This imbalance creates a need for advanced risk management tools that reflect local realities.

This paper addresses the growing issue of chargebacks in Ukrainian and regional e-commerce by modelling the impact of key transaction parameters, such as payment amount, security level, and issuing bank, on chargeback likelihood. By applying machine learning models to real-world transaction data, the study offers insights into the predictive factors of chargebacks and proposes data-driven strategies to mitigate them. The findings contribute to improving payment system resilience and risk prevention practices across Eastern Europe and similar emerging markets.

2. Analysis of recent researches and publications

The phenomenon of chargebacks has attracted growing academic and industry attention due to its impact on the financial stability of e-commerce enterprises. Research by Caldeira et al. (2014) and Guo et al. (2018) has highlighted the increasing complexity of fraud patterns in digital commerce and the urgent need for predictive models capable of identifying high-risk transactions [1; 3]. These studies emphasise the importance of transaction parameters, particularly payment amount, security features, and banking institution characteristics, in determining chargeback probability.

Machine learning and data mining have emerged as critical tools in fraud detection, enabling the analysis of large transaction datasets and the recognition of non-obvious patterns. Liu and Lee (2022) proposed

integrating machine learning with blockchain to improve fraud traceability and transparency, offering a comprehensive approach to digital risk management [2].

In the Ukrainian context, Mints et al. (2022) examined the growth of cashless payments and the limited institutional awareness of chargeback procedures [4]. Despite the rapid adoption of digital payments, Ukrainian businesses often lack access to advanced risk mitigation frameworks.

Thus, the existing literature underscores both global trends and local gaps in understanding chargeback dynamics. This study builds on prior work by introducing a regionally focused, data-driven approach to predictive modelling in e-commerce risk analysis.

3. Methods of investigation and sources

This study employs a mixed-method approach that combines quantitative modelling with qualitative interpretation to examine the relationship between transaction parameters and the occurrence of chargebacks in e-commerce. The research is grounded in transaction risk theory and applies predictive modelling techniques to real-world data obtained from two Ukrainian e-commerce enterprises operating in different market segments.

The primary methods used include multiple linear regression, logistic regression, and ensemble machine learning techniques such as Random Forest and Gradient Boosting. These methods enable the identification of significant predictors among variables such as transaction amount, security level, and issuing bank. Python was used for data processing, model training, and diagnostics, including tests for multicollinearity, heteroscedasticity, and model adequacy.

The data were collected over a four-month period (November 2023 to February 2024) and included more than 110,000 transactions. The dataset contains detailed information such as payment method, amount, security status, and chargeback outcomes. Special attention was given to

identifying trends specific to the Ukrainian digital payment environment, taking into account regional practices and institutional settings.

By combining robust statistical methods with real operational data, the study offers practical insights for developing risk mitigation strategies tailored to the e-commerce landscape of Ukraine and similar emerging markets.

4. Investigation results

To explore how key transaction parameters influence chargeback likelihood in Ukrainian e-commerce, the study formulated three core hypotheses:

H1: Payment amount has a positive effect on chargeback likelihood.

H2: Transactions with higher levels of security are less likely to result in chargebacks.

H3: The characteristics of the issuing bank influence the likelihood of a chargeback. These covered the expected influence of payment amount, transaction security level, and issuing bank characteristics on chargeback frequency. The investigation below tests these hypotheses using real transaction data from two Ukrainian e-commerce enterprises and applies both statistical and machine learning models to assess their validity.

The empirical investigation was based on transaction data collected from two Ukrainian e-commerce enterprises operating in distinct market sectors: one in fast-moving consumer goods (FMCG), and the other in household electronics retail. The dataset includes over 110,000 transactions conducted over a four-month period (November 2023 to February 2024), with full transaction metadata and chargeback indicators. The purpose of this section is to analyse the chargeback patterns in these enterprises and validate the previously proposed hypotheses through statistical and machine learning models.

4.1. Descriptive statistics and regional patterns

In the first enterprise (FMCG), a total of 14,732 transactions were recorded, of which 847 (5.75%) resulted in chargebacks. As shown in Figure 1, the majority of transactions originated in Europe, particularly in France, Australia, and the United Kingdom, with France alone accounting for over 5,300 transactions.

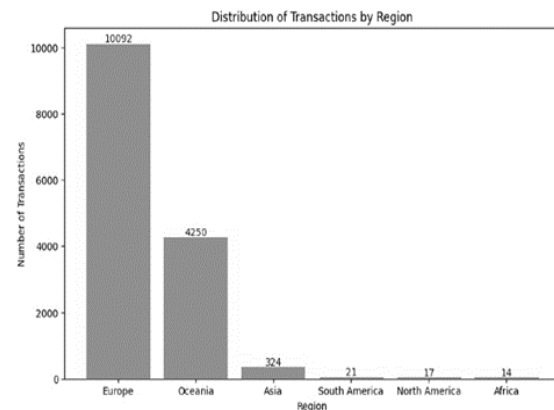


Figure 1: Number of transactions by region for the First Enterprise

Source: author's own research

Chargebacks by region mirrored transaction volumes, with Europe again dominating (686 chargebacks, see Figure 2). This suggests a correlation between market size and dispute incidence. However, further analysis revealed that chargeback rates varied depending on issuing banks and payment characteristics.

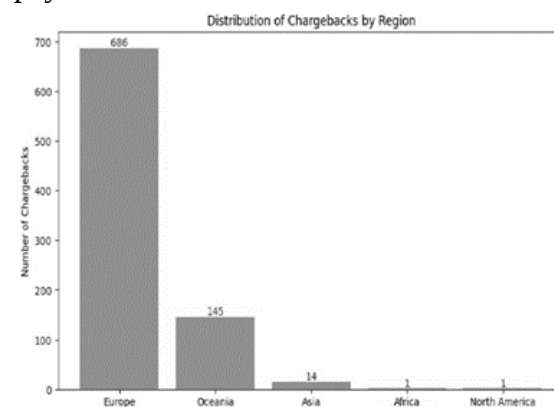


Figure 2: Number of chargebacks by region for the First Enterprise

Source: author's own research

In the second enterprise (electronics retail), 96,295 transactions were analysed, with 2,427 resulting in chargebacks (2.52%). Figure 3 illustrates that Chile accounted for 62% of all transactions, while Figure 4 shows that the same country contributed over 85% of chargebacks. This suggests that high transaction volumes in specific regions may reflect underlying differences in banking practices or consumer behaviour, even if geography itself is not the primary risk factor.

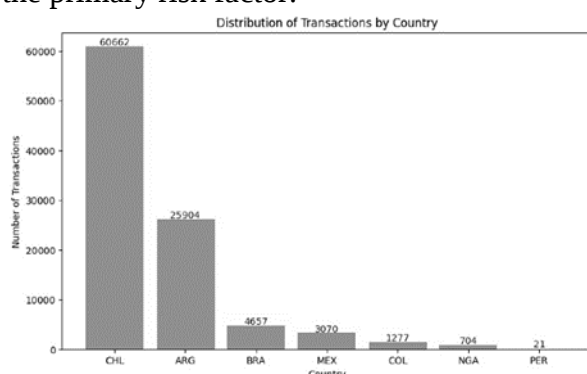


Figure 3: Distribution of transactions by country for the Second Enterprise
Source: author's own research

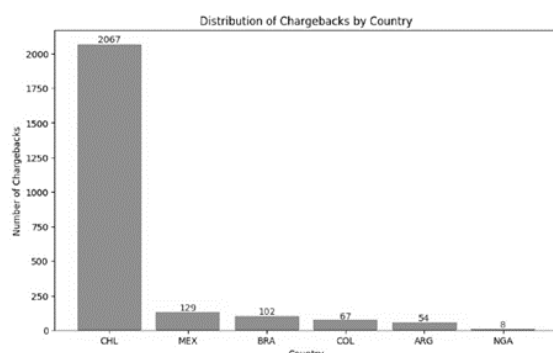


Figure 4: Distribution of chargebacks by country for the Second Enterprise
Source: author's own research

4.2. Transaction value and chargeback frequency

Transaction amount was found to significantly influence the probability of chargebacks in both enterprises. In the FMCG company, the majority of transactions were low in value (under USD 10), while chargebacks predominantly occurred in higher-value ranges, especially above USD 40.

Similarly, in the second enterprise, higher-value transactions were positively correlated with chargeback incidence, confirming the hypothesis H1. This is consistent with earlier findings by Saputra et al. (2019), who reported that consumers are more likely to initiate chargebacks on higher-value purchases due to increased loss aversion and scrutiny [5].

Regression models further validated this relationship. In the linear regression for the second enterprise, the 'amount_usd' coefficient was 0.0017 ($p < 0.001$), confirming statistical significance. The logistic regression also yielded a significant coefficient of 0.0232 ($p < 0.001$) for transaction amount.

4.3. Role of transaction security

The variable 'is_secured' was a critical factor in both enterprises. In the first enterprise, 83% of transactions were conducted without additional authentication (e.g., 3D Secure), as shown in Figure 3. The logistic regression model confirmed that secured transactions had a significantly lower probability of chargebacks, with a coefficient of -2.3023 ($p < 0.001$). This supports H2.

Distribution of Transactions by Security (is_secured)

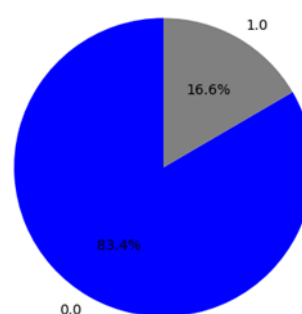


Figure 3: Distribution of transactions by payment security level for the First Enterprise
Source: author's own research

These findings align with Ray (2022), who emphasised that enhanced authentication reduces fraud risk [6]. The importance of adopting such protocols is especially urgent in Ukraine, where 3D Secure adoption is still in progress across banks and Payment

Service Providers (PSPs), such as LiqPay, WayForPay, Fondy, and Monobank, which play a key role in securing online transactions and managing risk.

4.4. Regional variations in chargeback activity

In the electronics retail enterprise, Chilean transactions were less likely to result in chargebacks (coefficient = -0.018; coefficient = -0.5607).

In contrast, in the FMCG enterprise, transactions from France and the UK were associated with high chargeback counts, especially when involving La Banque Postale. These patterns reflect not only consumer behaviour but also regional regulatory differences. As Mints et al. (2022) note, Ukraine's legal and procedural framework for chargebacks remains underdeveloped compared to Western Europe, impacting both consumer action and merchant protection [4].

4.5. Transaction type and tokenisation

Tokenised payments used in repeat transactions, comprised 68.5% of payments in the first enterprise. Interestingly, the logistic model found a positive coefficient for 'redefined_transaction_type_token' (2.1702, $p < 0.001$), indicating that tokenised payments were more likely to lead to chargebacks.

This observation suggests that tokenised transactions in Ukraine may carry unique risk patterns that require further investigation. Possible factors include insufficient communication during recurring billing, low transparency, or consumer unfamiliarity with stored payment authorisation.

4.6. Issuing bank and card brand impact

In both enterprises, the issuing bank was a strong predictor of chargeback activity. In the FMCG enterprise, transactions involving La Banque Postale were significantly more likely to lead to chargebacks, as shown in the final linear regression model (coefficient = 0.1111, $p < 0.001$) and logistic regression (coefficient = 0.6143, $p < 0.001$).

Similarly, in the electronics retail enterprise, Banco del Estado de Chile was positively associated with chargebacks. This confirms H3.

In terms of card brands, VISA was found to be more chargeback-prone in both enterprises. This may reflect higher usage volumes or simplified dispute processes for VISA users. Caldeira et al. (2014) similarly observed that certain card networks are more vulnerable to friendly fraud due to their consumer-friendly dispute resolution protocols [3].

4.7. Strategic insights for Ukraine

The results of this investigation offer actionable guidance for Ukrainian e-commerce enterprises. First, risk mitigation should prioritise the implementation of transaction-level security, particularly on tokenised and high-value payments. Second, monitoring of specific issuing banks and card networks is crucial, especially those associated with high dispute rates.

Third, the adoption of predictive models can assist Ukrainian merchants in proactively identifying high-risk transactions. Given the evolving regulatory environment in Ukraine, as highlighted by Mints et al. (2022), data-driven models may serve as an interim safeguard against financial and reputational losses [4].

Lastly, region-specific differences suggest that global fraud prevention strategies must be adapted to local conditions. Ukrainian businesses require chargeback prevention strategies tailored to their unique transaction structures, customer base, and institutional constraints.

The evidence presented confirms the three proposed hypotheses regarding transaction amount, security level, and bank-specific policies, offering a foundation for targeted risk mitigation and policy adaptation in Ukraine's digital commerce landscape.

5. Conclusions

This study examined the relationship between key transaction parameters and the

likelihood of chargebacks in Ukrainian e-commerce, using real-world data from two local enterprises and applying both statistical and machine learning techniques. The analysis confirmed three central hypotheses: that higher payment amounts increase chargeback risk, that enhanced transaction security reduces this risk, and that issuing bank characteristics significantly influence the outcome of payment disputes.

The findings show that most chargebacks occurred in high-value and unsecured transactions, underscoring the importance of robust authentication mechanisms such as 3D Secure. Moreover, the type of issuing bank and its regional policies emerged as a critical risk factor, particularly in countries with consumer-friendly chargeback regulations. This was especially evident in transactions involving La Banque Postale and Banco del Estado de Chile, which showed consistently high chargeback rates. Additionally, the study highlighted the risks associated with tokenised and recurring transactions, especially when consumer consent and transparency are insufficient. While tokenisation is often regarded as a security feature, its implementation in Ukraine requires further development and clearer user communication.

The results offer practical recommendations for Ukrainian businesses, including prioritising secure transaction channels, monitoring chargeback-prone banks, and implementing data-driven screening tools for high-risk transactions. Given the ongoing evolution of Ukraine's digital payment ecosystem, these insights contribute to the formation of adaptive and locally-relevant risk mitigation strategies.

Finally, the observed regional variations in chargeback dynamics reinforce the need to tailor global fraud prevention frameworks to national contexts. By integrating predictive analytics into their transaction monitoring systems, Ukrainian enterprises can enhance their operational resilience and better protect themselves from financial and reputational losses in the digital economy.

6. Limitations

While this study provides valuable insights into the influence of transaction parameters on chargeback risks in Ukrainian e-commerce, several limitations should be acknowledged. First, the analysis is based on data from only two enterprises, which, although diverse in their market segments, may not fully represent the entire Ukrainian e-commerce landscape. Second, the time frame of the data (four months) limits the ability to assess seasonal effects or long-term behavioural trends.

Furthermore, the study focuses on quantitative transaction attributes and does not include qualitative factors such as customer satisfaction, dispute resolution processes, or merchant-side policies, which may also influence chargeback outcomes. Lastly, due to the limited availability of publicly accessible chargeback datasets in Ukraine, the model may require recalibration when applied in different institutional or regulatory environments.

Future research should aim to expand the dataset, include more diverse business types, and integrate behavioural and regulatory variables for a more comprehensive analysis of chargeback dynamics.

References

- [1] Guo R., Wang S., Zhang H. A Payment Fraud Detection Model Based on Behavior Features and Transaction Patterns. *IEEE Access*. 2018;6:77114-77123.
- [2] Liu D., Lee J. Blockchain and Machine Learning Integration for Fraud Detection in Financial Systems. *Journal of Financial Innovation*. 2022;8(2):134–147.

- [3] Caldeira J.F., Moura G.V., Santos M.A. Fraud Detection in E-Commerce Using Neural Networks and Decision Trees. In: Silva A., ed. Proceedings of the 12th International Conference on E-Business. Lisbon: IADIS Press; 2014. 89–95.
- [4] Mints A., Pavliuk D., Shlapak V. Challenges of Chargeback Management in Ukrainian Online Retail: Legal and Operational Perspective. *Ukrainian Journal of E-Commerce*. 5(1): 2022, 12–21.
- [5] Saputra A., Suharjito. Fraud Detection using Machine Learning in e-Commerce. *International Journal of Advanced Computer Science and Applications*. 10(9): 2019, 332–339.
- [6] Ray S. Fraud Detection in E-Commerce Using Machine Learning. *BOHR International Journal of Advances in Management Research*. 1(1): 2022, 7–14.