Telecom Bank Card Fraud Analysis Based on Statistical Measures

Yang Zhao, Guangshuo Liu, Ziqing Liu*

Qinghai Normal University, Qinghai, 810000, China

Received: 3 Jun 2025
Revised: 4 Jun 2025
Accepted: 6 Jun 2025
Published: 8 Jun 2025

Abstract: In recent years, telecommunication network fraud has become increasingly severe, posing significant threats to financial security and social stability. This study aims to investigate the correlation between fraud occurrence and key indicators, including bank card usage and PIN authentication, to identify risk factors and protective measures. Statistical analyses were conducted on a comprehensive dataset of reported fraud cases, incorporating Kolmogorov-Smirnov (K-S) tests to examine the distribution characteristics of "Fraud," "Card," and "PIN" variables, followed by Spearman correlation analysis to assess their interdependencies. Visualization through pie charts revealed the proportional distribution of fraud types, with particular emphasis on differentiating telecom-related bank card fraud from non-telecom cases. The results indicate that bank card transactions conducted via digital devices exhibit a higher susceptibility to fraudulent activities, whereas the implementation of PIN verification significantly mitigates fraud risk. These findings provide empirical insights for enhancing anti-fraud strategies, emphasizing the importance of secure authentication mechanisms in digital financial transactions.

Keywords: Telecom Fraud; Spearman; K-S Test; Normal Distribution; Pie Chart

1 INTRODUCTION

Telecom fraud has emerged as a pervasive threat in the digital age, leveraging communication technologies such as phone calls, internet platforms, and text messages to deceive victims through fabricated information, ultimately coercing them into unauthorized fund transfers. This form of financial crime has evolved in sophistication, exploiting vulnerabilities in both technological systems and human psychology. In response, public security departments have intensified efforts by implementing specialized measures under the framework of "four specializations and two joint efforts," which have contributed to curbing the rapid escalation of telecom fraud cases [1-5]. Despite these interventions, the overall landscape remains concerning, with fraudsters continually adapting their tactics to bypass security measures.

Among the prevalent fraud schemes, ten major categories—including rebate scams and fake online investment platforms—account for nearly 80% of reported incidents. Rebate fraud exhibits the highest occurrence rate, while fraudulent investment and wealth management schemes inflict the most substantial financial losses on victims [6]. The persistence of these scams underscores the need for a deeper understanding of the mechanisms that facilitate telecom fraud, particularly in transactions involving bank cards.

This study seeks to analyze the key factors influencing telecom-related bank card fraud by addressing two critical questions. First, it examines whether the act of conducting transfer

transactions via digital devices using a bank card increases susceptibility to fraud. Second, it evaluates whether the additional security layer of entering a bank card PIN during transactions reduces the likelihood of fraudulent exploitation [7]. By investigating these aspects, the research aims to provide actionable insights that can enhance fraud prevention strategies and safeguard financial transactions in an increasingly digitalized economy.

2 MODEL ASSUMPTION AND BUILDING

In this study, we built an analytical framework based on the following assumptions:

(1) It is assumed that all statistical cases are true and valid data.

(2) It is assumed that the method of transfer transactions will not be changed in all the cases counted.

First of all, the "Fraud" column, the Pin column and the "Card" column are preprocessed with data, since the "Fraud" column, the Pin column and the "Card" column are all 0 and 1, we only need to complete the missing values, and through data screening, we find that the "Fraud" column, Pin column and "Card" column have no missing values [8].

We first remove the number of rows with the "Fraud" column as 0, and the data left behind is the data of telecom fraud. Then, the proportion of transfer transactions using and not using a bank card on the device and Pin number is calculated separately as follows:

$$\begin{cases} FR(C) = \dfrac{\sum_{i=1}^{N}(F_i \times C_i)}{\sum_{i=1}^{N} C_i} \\ FR(P) = \dfrac{\sum_{i=1}^{N}(F_i \times P_i)}{\sum_{i=1}^{N} P_i} \end{cases} \tag{1}$$

The above equation calculates that the proportion of transfer transactions made on the device is summed up with and unused, and the proportion of transfer transactions made with and without numbers is summed respectively [9]. Next, we draw a pie chart of the proportional data and visualize it as follows:

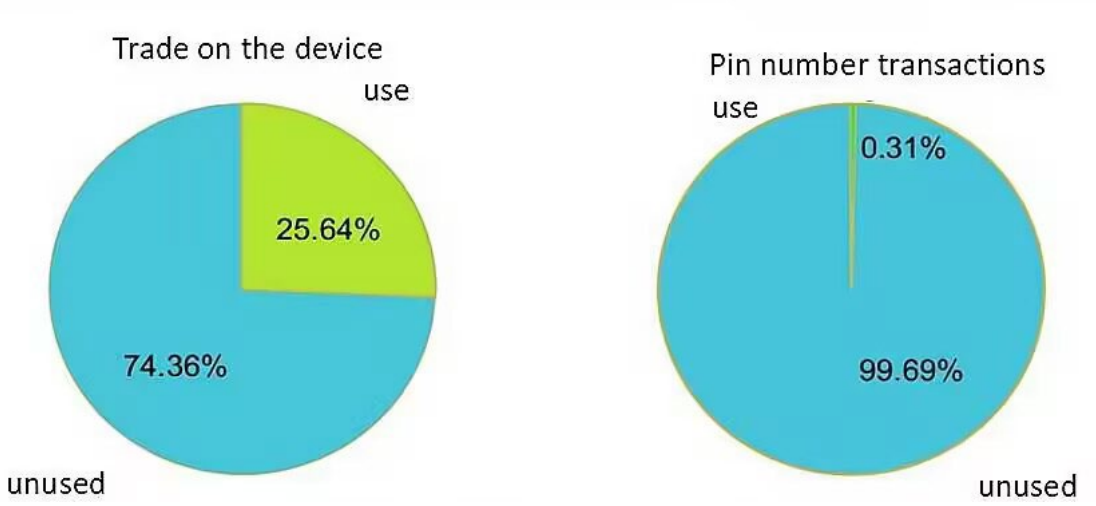

Fig. 1: Pie chart of device and number transactions using the ratio to unused.

As can be seen from the figure above, the proportion of transactions that are defrauded using an on-number number is lower than the proportion of transactions that are scammed when using a device. Therefore, using a bank card to transfer money on a device is more likely to cause fraud.

To investigate the relationship between "whether to use a bank card to transfer money on a device" and "whether to use a bank card PIN number to transfer a transaction" and the occurrence of telecom fraud, statistical models can be used for computational modeling.

The Kolmogorov–Smirnov test is a nonparametric statistical method of testing distributions, with the null hypothesis that the data conform to a given distribution [10]. We used the K-S test to test the normality of the raw data, and the results are shown in Table 1. All the P-values in Table 1 are much less than 0.05, and we need to reject the null hypothesis that the raw data given in the question do not conform to the normal distribution.

Table 1: K-S test results of indicators.

Index	K-S value	P-value
Card	0.4186	0.0000
Pin	0.5304	0.0000
Fraud	0.5341	0.0000

Through the above analysis, we know that the sample data does not meet the normal distribution. when the sample does not meet the normal distribution, the Spearman correlation coefficient is usually used for correlation analysis.

$$\rho = \frac{\sum_i (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_i (xi - \bar{x})^2 \sum_i (y_i - \bar{y})^2}} \tag{2}$$

The closer to 1 is the linear correlation between the two samples. At the same time, in order to visually represent the magnitude of the degree of correlation. we draw the Spearman correlation coefficient heat map as follows:

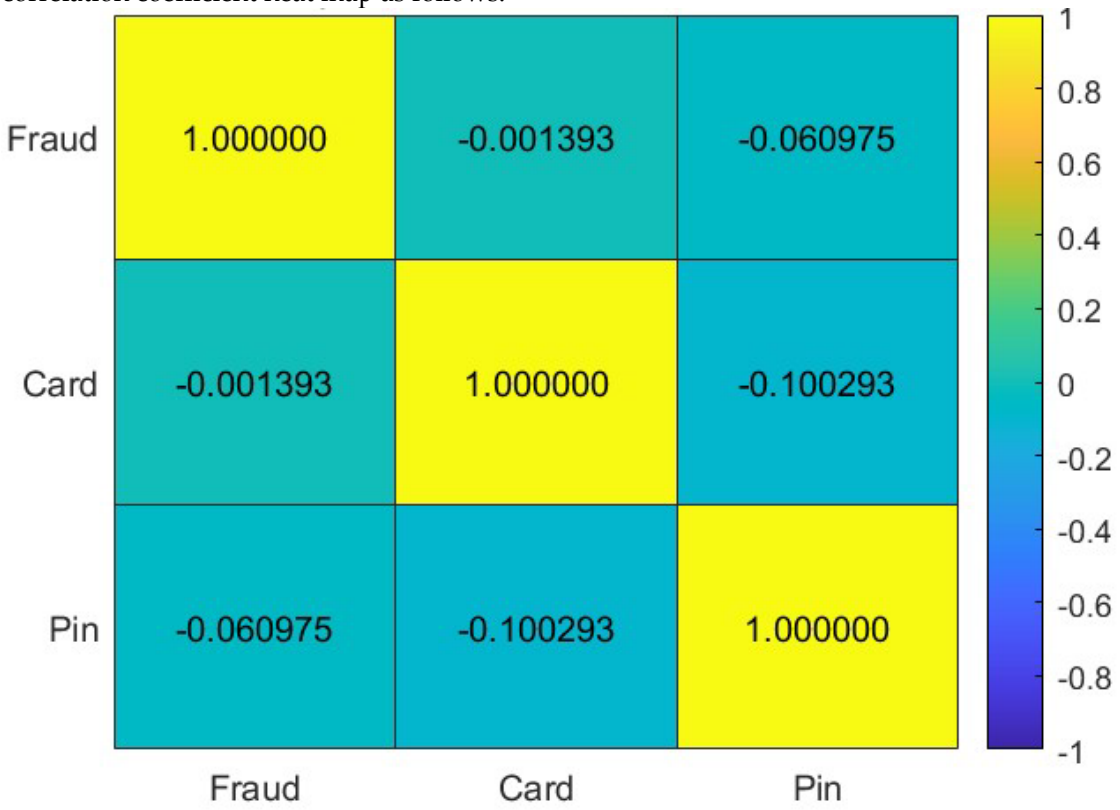

Fig. 2: Correlation analysis heat map.

As can be seen from the above figure, the correlation coefficient between "whether to use a bank card to make a transfer transaction on the device" and the occurrence of telecommunication fraud is -0,001393, and the correlation coefficient between "whether to use a bank card number to make a transfer transaction" and the occurrence of telecommunication

fraud is -0.060975. Because -0,001393> -0.060975, using a bank card to transfer money on a device is more likely to scam.

We first divide the data in column "Pin" into two parts by the 0 and 1 of column "Fraud", and then calculate the proportion of telecom card fraud in the two parts and the proportion of non-occurrence of telecom card fraud, which is calculated as follows:

$$\begin{cases} FR(P) = \dfrac{\sum_{i=1}^{N}(F_i * P_i)}{\sum_{i=1}^{N} P_i} & Use\ a\ PIN \\ FR(UP) = \dfrac{\sum_{i=1}^{N}\left(F_i * P_{ui_i}\right)}{\sum_{i=1}^{N} P_{ui}} & The\ PIN\ is\ not\ used \end{cases} \tag{3}$$

The proportions of being deceived and not being deceived by using Pin number transactions are 0.27% and 99.73%, and the proportions of being deceived and not being deceived by using Pin number transactions are 9.69% and 90.31% respectively. Next, we draw a pie chart of the proportional data and visualize it as follows:

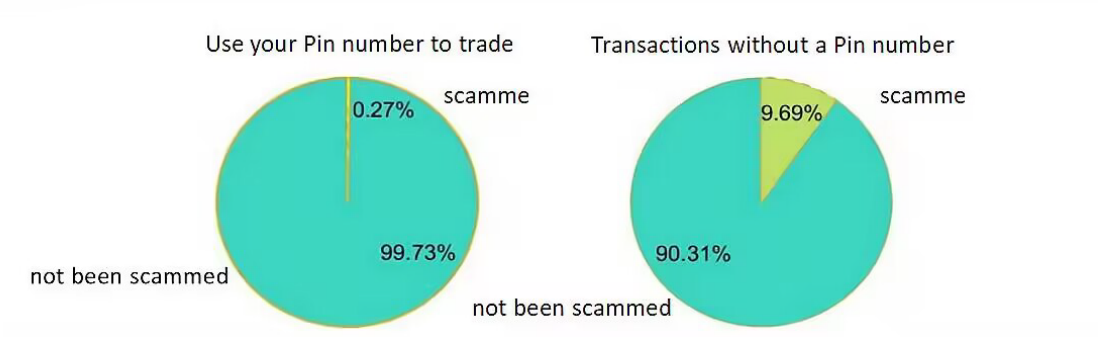

Fig. 3: A pie chart of the percentage of people who have been scammed.

As can be seen from the above figure, the proportion of people who are defrauded by using PIN numbers is lower than the proportion of people who are defrauded by not using PIN numbers, so using the PIN number of a bank card can reduce the probability of being defrauded by telecommunications.

3 CONCLUSION

This study provides empirical evidence on the risk factors associated with telecom fraud in bank card transactions through statistical and correlation analyses. Visualization of fraud patterns via pie charts revealed a significant trend: transactions conducted using bank cards on digital devices exhibit a substantially higher susceptibility to fraudulent activities. This finding underscores the vulnerabilities inherent in device-based financial operations, where security measures may be circumvented by sophisticated fraud techniques. The prevalence of such cases highlights the need for enhanced protective mechanisms in digital payment ecosystems to mitigate fraud risks.

Further investigation using Spearman correlation analysis, a robust method for non-normally distributed data, confirmed that device-based bank card transactions are strongly associated with increased fraud incidence. The non-parametric nature of this approach ensured reliable results despite deviations from normal distribution in the sample data. Additionally, the study quantified the impact of PIN authentication on fraud reduction. By analyzing the proportion of telecom-related fraud cases, it was demonstrated that requiring a bank card PIN

during transactions significantly lowers the probability of fraudulent exploitation. This reinforces the importance of multi-factor authentication in securing financial transactions against unauthorized access.

The findings of this research carry important implications for both financial institutions and policymakers. Strengthening transaction security protocols, particularly by mandating PIN verification for device-based transfers, could serve as an effective deterrent against telecom fraud. Future studies could expand on these insights by exploring additional authentication methods or examining fraud trends across different demographic groups. Ultimately, fostering collaboration between technology developers, banks, and regulatory bodies will be essential in developing comprehensive strategies to combat the evolving threat of telecom fraud.

REFERENCES

[1] Wang, M., Xie, J., Chen, Z., Liu, M., Zhang, S., & Li, J. (2024). Enhancing Telecom Fr aud Prediction Accuracy Using a Combined CNN-LSTM Model with Bahdanau Attention Mechanism. Journal of Globe Scientific Reports, 6(2), 56-73.

[2] Wahid, A., Msahli, M., Bifet, A., & Memmi, G. (2024). NFA: A neural factorization aut oencoder based online telephony fraud detection. *Digital Communications and Networks*, *10* (1), 158-167.

[3] Liu, G. (2024). Leveraging Machine Learning for Telecom Banking Card Fraud Detection: A Comparative Analysis of Logistic Regression, Random Forest, and XGBoost Models. *C omputers and Artificial Intelligence*, *1*(1), 13-27.

[4] Shao, L., Chen, Q., & He, M. (2025). Telecom Fraud Money Laundering Account Recog nition Case: Multiple Machine Learning Techniques. In *AI in Banking: Practical Applicatio ns and Case Studies* (pp. 159-197). Singapore: Springer Nature Singapore.

[5] Hapase, D. S., & Patil, L. V. (2024). Telecommunication fraud resilient framework for eff icient and accurate detection of SMS phishing using artificial intelligence techniques. *Multi media Tools and Applications*, 1-23.

[6] Alshawi, B. (2024). Comparison of SVM kernels in Credit Card Fraud Detection using G ANs. *International Journal of Advanced Computer Science & Applications*, *15*(1).

[7] Du, H., Lv, L., Wang, H., & Guo, A. (2024). A novel method for detecting credit card f raud problems. *PloS one*, *19*(3), e0294537.

[8] Li, F., & Chen, Z. (2025). Dynamic quantification anti-fraud machine learning model for real-time transaction fraud detection in banking. *Discover Computing*, *28*(1), 59.

[9] Charizanos, G., Demirhan, H., & İçen, D. (2024). An online fuzzy fraud detection framew ork for credit card transactions. *Expert Systems with Applications*, *252*, 124127.

[10] Sizan, M. M. H., Chouksey, A., Tannier, N. R., Al, M. A., Jobaer, J. A., Roy, A., ... & Aminul, D. (2025). Advanced Machine Learning Approaches for Credit Card Fraud Detect ion in the USA: A Comprehensive Analysis. *Journal of Ecohumanism*, *4*(2), 883-905.