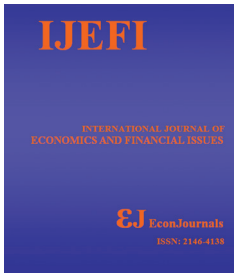

International Journal of Economics and Financial Issues

ISSN: 2146-4138

available at http: www.econjournals.com

International Journal of Economics and Financial Issues, 2025, 15(1), 17-23.

Predicting Credit Card Frauds in India: An Empirical Investigation

Lokendra Puri[1], Ranjit Singh[1], Rafiqul Bhuyan[2]*

[1]Department of Management Studies, Indian Institute of Information Technology Allahabad Prayagraj, India, [2]Department of Accounting and Finance, Alabama A&M University, AL, USA. *Email: rafiqul.bhuyan@aamu.edu

Received: 26 August 2024 **Accepted:** 07 November 2024 **DOI:** https://doi.org/10.32479/ijefi.17666

ABSTRACT

This study attempts to predict credit card fraud and to know the factors responsible for credit card fraud. Using primary data of 7,500 credit card holders, collected using a questionnaire, this study conducts statistical analysis using discriminant analysis method. It is observed that variables, such as distance from home, distance from the last transaction, ratio to the median purchase price, used chip, used PIN for the transaction, and online order are significant factors in contributing to credit card fraud.

Keywords: Bank Customers, Credit Card Fraud, Digital Transaction, Discriminant Analysis, Machine Learning
JEL Classifications: C58, G21, G29, N25

1. INTRODUCTION

Thanks to the adoption of digitalization in every country, the banking sector has adopted digitalization to offer a smooth and safe environment to customers to conduct banking transactions (Kültür and Çağlayan, 2017). In the advent of internet technology, customers' preferences have changed from physical payment to digital payment due to minimal surcharges and small transaction time (Chakravorti and To, 2007). Society, in the context of greater India, has witnessed the complete implementation of technologies emergence of the Green Revolution, eChoupal call centres during Yellow Revolution and Unified Payment Interface (UPI) based payments during post-demonitization (Heeks, 2008; Tassabehji et al., 2019). Digitalization, like western nations, has strengthen the banking sector in India as banks are able to inter and intra-connect branches to offer different kinds of online products and services such as cheque, credit card, debit card, electronic money transfer, mobile transfer, and wallets (Joshi, 2017; Kumar et al., 2022). Credit cards, as a method of carrying money and making payment for transaction, has emerged as one alternative and effective payment option due to its associated initiatives like rewards, safety, short-term free credit, soft cash etc (Uddin, 2020). A credit card is a kind of money card offered by the bank which allows the holder to perform transactions on demand and settle the amount after some time as per the policy of the card provider (Coskun et al., 2022) and it is widely used in both developed and underdeveloped nation. Although credit card offers many benefits to users, it also carryes significant risk of fraud as hackers can steal credit card information and carry out transaction without the authorization of credit card holders. Just like in any other country, credit card fraud is also one of the top frauds happening in India (Barker et al., 2008). Credit card fraud can be classified into two parts i.e., application fraud and behavioural fraud (Sael et al., 2018). Application fraud represents the kind of fraud under which a fraudster provides false information to the card-issuing company to receive the card. On the other hand, behavioural fraud takes place when the fraudster takes the card's authentic information fraudulently (Bolton and Hand, 2002a; Linda, et. al., 2009). Behavioural fraud is further classified into 4 parts i.e., mail theft fraud, lost/stolen card fraud, counterfeit card fraud,

and cardholder not present fraud (Chaudhary and Mallick, 2012; Sael et al., 2018). Some studies criticize the use of credit cards on the grounds that it promotes procrastination (Barboza et al., 2017; Wray, 2014). Regulators of many countries are taking all possible steps such as campaigning, tele-messaging, emails etc to generate awareness and activeness among the customers to deter fraudulent activities. However, it is still a serious concern as frauds are happening and cases are registered daily in India (Sood and Bhushan, 2022). In order to promote smooth financial system, there is a need to understand more of those reasons for the fraud and the factors responsible for it, so that financial institutions and government can implement better security and protection system for consumers to allow fraud free financial system. This study attempts to identify the condition as well as the factors that are responsible for credit card fraud. Thus, the present study attempts to answer the following questions:

- RQ1: What are the factors responsible for credit card fraud?
- RQ2: How accurately fraud prediction can be done in the case of credit cards using the relevant personal information of the holder?

The rest of the paper is structured as follows: Section 2 considers the theoretical background and the literature review; Section 3 explains the methodology; Section 4 illustrates the result; Section 5 deals with the discussion; Section 6 explains the implications and in last section 7 presents the conclusion of the study.

2. THEORETICAL BACKGROUND AND LITERATURE REVIEW

With the increase in digital offerings by banks, the cases of digital fraud are also increasing (Gawer, 2021). There are many theories related to fraud. A few relevant theories are discussed below:

I. The fraud triangle theory: It explains the conditions which result in the mishandling of assets and something wrong with the financial statements (D'onza and Lamboglia, 2014; Hayati et al., 2011; Misra et al., 2020). This theory consists of the 3 major components which are explained below:
   i. Opportunity: This condition happens due to trust beyond the limit, selection of not-competent authority, weak control and regulations, and improper running (Lin et al., 2003).
   ii. Pressure: It encourages someone to do fraud just because of the demands, not sounding financial status, not satisfied with the ongoing job, and an attempt to stand against the system (Persons, 1995).
   iii. Rationalization: It also contains four acts named a bad attitude, dishonesty in the character, deficiency of self-integrity, and self-justification (Huang et al., 2017).

II. Fraud diamond theory: Wolfe and Hermanson (2004) expanded the fraud triangle theory. Authors remarked that fraud triangle theory lacks one most important element i.e., Capability. Further, added that the person acts after covering many things and (s)he is having full capacity to cheat and not uncover (Munawer and Siti-Nabiha, 2012).

III. Fraud scale theory: This theory is also the continuation of the fraud triangle theory. It explains that the occurrence of fraud can be measured by evaluating the capacity of personal integrity, opportunity and pressure (Tsaih et al., 2009). The main highlight of this theory is living beyond their means, a desire for profit, and a higher amount of personal debt (Wyrobek, 2020; Zager et al., 2016). According to the mentioned theory, a higher amount of trust in the employees and weak coordination from the superiors are also playing a role of catalyst in the case of fraud (Munawer and Siti-Nabiha, 2012; Nizamani et al., 2014).

IV. Fraud Pentagon Theory: This theory adds two more elements to the existing version of the triangle theory. Two more elements i.e., arrogance and opportunity added to the existing components of the fraud triangle theory (Rezaee, 2005). Under this theory, arrogance is indicating the arrogant kind of attitude that makes herself/himself fully capable of cheating, although the opportunity is representing the availability of the space to commit fraud. Authors also concluded that rising of such situations is just because of weak control (D'onza and Lamboglia, 2014; Summers and Sweeney, 1998).

V. Neutralization theory: Neutralization theory explains that willpower to perform a crime/fraud with the rational decision is supreme to doing the offence although rational reason must happen before the crime/fraud is taking place. The neutralization theory identifies five major methods of neutralization that are: denial of injury, denial of responsibility, denial of victim, appealing to the higher loyalties, and condemnation of the condemners. Further, a model PICOIR is created using the above-mentioned theory. Under that thread, PICOIR stands for Pressure, Integrity, Capabilities, Opportunity, Integrity, and Rationalization (Sorunke, 2016).

Based on existing literature, the present study has highlighted several factors which were found significant in various studies done by different authors. Table 1 considers the significant variables and the name of the study which found such variables significant.

Likewise, Distance from home indicates the distance between the transaction place (where the transaction occurred) to the home of the cardholder. Although, Distance from the last transaction states the distance from the last transaction to the home of the cardholder. Distance from home and distance from the last transaction become opportunities from the perspective of the cardholder and fraudsters. It becomes an opportunity for the cardholder to choose the shortest distance to do the transaction. Also, it becomes an opportunity for

Table 1: Factors found significant in the existing literature

Aspect of fraud	Studies
Distance from home	(Pulina and Paba, 2010)
Distance from last transaction	(Aihua et al., 2007; Pulina and Paba, 2010)
Ratio to purchase median price	(Burnes et al., 2020; Yu et al., 2020)
Repeat retailer	(Pawar et al., 2014; Sriyalatha, 2016)
Used chip	(Sun and Davidson, 2015)
Used pin number	(Gadi et al., 2008)
Online order/online transaction	(Khan et al., 2014)

the fraudster too as they can easily track the holder's activities to do fraud. Based on existing literature, the proposed model for the current study will be as shown in Figure 1.

3. METHODOLOGY

This study is descriptive in nature. A sample of people from India, with credit cards, are selected for the study. Primary data is used for the analysis. A well-structured questionnaire is designed to gather the data. Initially, several bank branches are selected to collect the data in person as well as via mail. Then, personal meetings are also arranged with the cardholders which is a time-consuming task. Further, a Google form consisting of the questionnaire is circulated on various social media platforms such as Facebook, LinkedIn, and WhatsApp and later on shared with friends, colleagues, batch mates, businessmen, and students etc to get accurate data. This process takes a significantly long periods, about 22 months i.e., August 2021 to May 2023 to gather the data. There are lot of incomplete responses by the respondents which are screened and discarded from the data set. After numerous rounds of screening and filtering, duly filled responses are taken for further analysis. Finally, the data consists of 7500 cardholders. The dataset contains 7500 random cardholders with different variables like distance from home (Pulina and Paba, 2010), distance from the last transaction (Pulina and Paba, 2010), ratio to the median purchase price (Burnes et al., 2020; Yu et al., 2020), repeat retailer (Pawar et al., 2014; Sriyalatha, 2016), used chip (Sun and Davidson, 2015), used PIN for the transaction (Gadi et al., 2008), and online order (Khan et al., 2014). The data also contains information about occurance of fraud. If fraud takes place then the respondent is asked to fill in 1 otherwise 0 (Benchaji et al., 2021). Many studies have recently used different techniques to identify or predict fraud in the case of credit cards. Studies find that logistic regression can highlight the presence or absence of fraud if several important characteristics are given and the predictor is fully capable of giving the result carefully (Altman et al., 1994; Flitman, 1997). Many authors tried to detect credit card fraud using the neural network which is a node-connected network just like the brain and provides its findings after analyzing the algorithm (Quah andf Sriganesh, 2008; Zaslavsky and Strizhak, 2006). After the entry of deep learning, several studies supported the decision tree systems to predict fraud. The purpose to use a decision tree system is to build a decision tree with greater precision and small scale (Quinlan, 1994; Quinlan and Cameron-Jones, 1993). An algorithm i.e., a Genetic algorithm (previously used for the insurance sector) is also taken to detect fraud which is made of different algorithms like best match algorithms, density selection algorithms, diagnostic algorithms, diagnostic resolution strategies, negative selection algorithms, and probabilistic curve algorithms etc (Wheeler and Aitken, 2000). Two more techniques i.e., clustering technique and outlier detection have been already used by the authors in different sectors to identify fraud including the credit card industry (Bolton and Hand, 2002a). The study is funded by the Scientific and Technological Research Council of Turkey (TÜB_ITAK) detected credit card fraud using the fisher discriminant coefficient and found a very significant result (Mahmoudi and Duman, 2015). Discriminant analysis is used to find the more accurate and reliable result that will help to diagnose the discrimination between fraud and not fraud as found in the case of telecom sector (Oghojafor et al., 2012).

4. RESULTS

The dataset is classified into two (2) different groups i.e., Fraud and Not fraud, to run and validate our model. Likewise, we trained our model with the training dataset i.e., 5000 and left the rest as a holdout sample to find out the efficiency and fitness of our model. Firstly, the test of equality of group means is conducted on training sample whose result is shown in Table 2.

It is observed that, except for repeat retailer, all variables are significant. The next step is to calculate the Eigenvalues that are shown in Table 3.

Table 3 presents the value of canonical correlation i.e., 0.573 which also helps to calculate the value of $(R)^2 = (0.573)^2 = 0.328$which implies that approximately 33% of the variation in the grouping is explained. The next step is to proceed towards the value of Wilk's lambda.

Wilk's Lambda is used to know the status of the significance of the discriminant function. In Table 4, it is visible that the discriminant

Figure 1: Proposed research model to predict the fraud

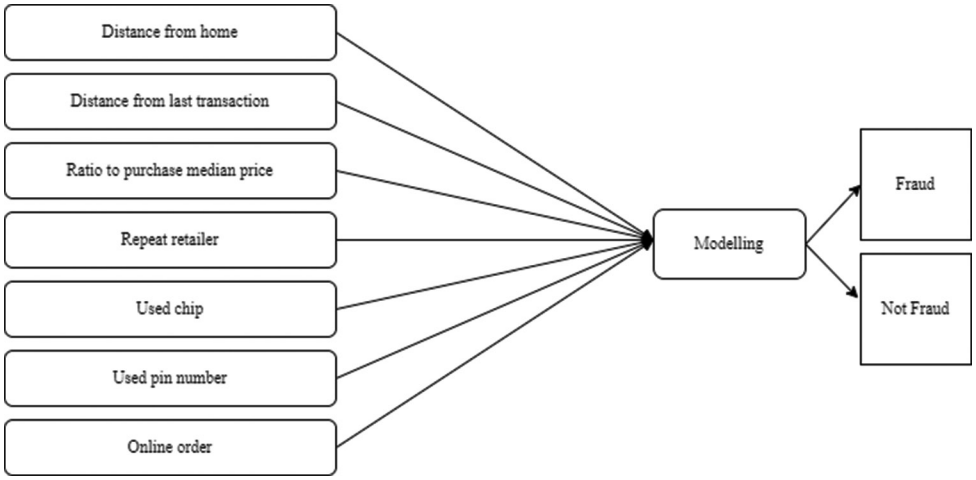

Table 2: Value of group means equality

Tests of equality of group means					
Choice Variable	**Wilks' Lambda**	**F**	**df1**	**df2**	**Sig.**
Distance from home	0.956	227.570	1	4998	0.000
Distance from last transaction	0.988	61.150	1	4998	0.000
Ratio to median purchase price	0.782	1391.405	1	4998	0.000
Repeat retailer	1.000	1.965	1	4998	0.161
Used chip	0.994	29.819	1	4998	0.000
Used pin number	0.990	52.049	1	4998	0.000
Online order	0.958	219.644	1	4998	0.000

Table 3: Eigenvalues

Eigenvalues				
Function	**Eigenvalue**	**% of Variance**	**Cumulative %**	**Canonical correlation**
1	0.488[a]	100.0	100.0	0.573

[a]First 1 canonical discriminant function was used in the analysis

Table 4: Value of Wilk's Lambda

Wilks' Lambda				
Test of Function (s)	**Wilks' Lambda**	**Chi-square**	**df**	**Sig.**
1	0.672	1983.991	7	0.000

Table 5: Discriminant function coefficient

Standardized canonical discriminant function coefficients	
Choice Variables	**Function**
	1
Distance from home	0.440
Distance from last transaction	0.209
Ratio to median purchase price	0.873
Used chip	−0.176
Used pin number	−0.206
Online order	0.406

Table 6: Value of classification function coefficient

Classification function coefficients		
Choice Variables	**Fraud**	
	0	**1**
Distance from home	0.008	0.025
Distance from last transaction	0.008	0.027
Ratio to median purchase price	0.327	1.269
Used chip	1.449	0.524
Used pin number	1.080	−0.612
Online order	3.016	5.175
(Constant)	−2.276	−7.975

Fisher's linear discriminant functions

function is highly significant which is less than the P-value i.e., 0.05. The function also can discriminate the cases with 67.2% strength correctly. Moving further, the next step is to know the discriminant function coefficient.

Table 5 shows the value of the standardized discriminant coefficient should help determine the importance of the function and its direction. As can be seen in Table 5, the ratio to the median purchase price (0.873) is the top discriminator. It is followed by the distance from home (0.440), online order (0.406), distance from the last transaction (0.209), used pin number (−0.206), and last used chip (−0.176). Based on table 5, the discriminant function

Table 7: Classification result

Classification Results[a]					
Groups		**Fraud**	**Predicted group membership**		**Total**
			0	**1**	
Original					
	Count	0	4368	200	4568
		1	56	376	432
	%	0	95.6	4.4	100.0
		1	13.0	87.0	100.0

[a]94.9% of original grouped cases are correctly classified

Table 8: Classification result of the holdout sample

Classification Results[a]					
Groups		**fraud**	**Predicted Group Membership**		**Total**
			0	**1**	
Original					
	Count	0	2160	130	2290
		1	20	190	210
	%	0	94.3	5.7	100.0
		1	9.5	90.5	100.0

[a]94.0% of original grouped cases are correctly classified

is given as follows:

D = 0.873 ratio to median purchase price + 0.440 distance from home + 0.406 online order + 0.209 distance from last transaction + (-0.206) used pin number + (-0.176) used chip

As can be seen in Table 6, the value of online orders has the highest value among all variables. That is followed by the used chip, used pin number, ratio to the median purchase price, distance from the last transaction, and last distance from home.

Table 7 demonstrates that out of 5000 samples, our model can predict approximately 94.9% (accurate 94.88%) of customers correctly that is 4744 customers in case of fraud.

Moreover, we ran the discriminant analysis using the holdout sample i.e., 2500 samples to validate and test the efficiency of our model. Table 8 shows the result of our findings that our model is capable to predict 94% of cases correctly. That means out of 2500, our model has the strength to predict the 2350

customers correctly which is also a very big achievement for our model.

5. CONCLUDING REMARKS

This study is an attempt to predict the probability of fraud and identify the factors responsible for credit card fraud in India. The study considered the seven variables namely distance from home, distance from the last transaction, ratio to the median purchase price, repeat retailer, used chip, used PIN for the transaction, and online order. This study uses discriminant analysis to propose a model that should work to predict the probable rate of credit card fraud.

After analyzing the data with discriminant analysis, the study finds that repeat retailer is the only variable that is insignificant while all remaining variables are found significant in the case of fraud. Ignoring the insignificant variable, further analysis took place that provided a model whose predictability strength is approximately 94.88% and 94% for the trained and holdout samples respectively. Predicting credit card fraud at this big rate is the beauty of the model designed which is a very big achievement indeed. Kassem and Higson (2012) also supported the track of the model used in the study. Few more studies support the findings of the current study, Studies stated that it does not mean people will not do fraud if their level of integrity is down/low, there are other factors too that encourage the person to do fraud (Kakati and Goswami, 2019). The study covered various variables which are having detailed information about the cardholder's personal experience that provides a stronger base to the study as compared to the existing studies (Khare and Singh, 2012; Świecka et al., 2021). Mahmoudi and Duman (2015) concluded that the fisher discriminant analysis performed much better, especially in the case of credit card fraud. Although, the authors gave a hint to use discriminant analysis in future research because it would be helpful in minimization of the time cost and maximization of the total profit. The study answers the first question by marking the factors that are responsible to make fraud in the context of credit cards. Next to that, the study answers the second and last research question which is about fraud prediction in the case of credit cards. The study has the capability to predict credit card fraud with the strength of 94% accuracy which sounds much prettier as visible in Table 8.

5.1. Managerial Implications

The present study provides a model to identify and predict credit card fraud. Managers can take the advantage of findings of the study to minimize credit card fraud. Managers can categorize the customers based on the probability of fraud occurrence. Categorization of the customers will help the managers to take the action accordingly. That means the level of predicted fraud, attention, and support from the management is directly proportional to each other i.e., the level of attention and the support from the managerial end will move along with the predicted rate of fraud. If the manager knows the highlighted person (with whom credit card fraud chances are high) then (s) he can take all the precautionary steps to mitigate or reduce the rate of fraud. Likewise, findings will be more beneficial to the card society i.e., card holders and the card issuers. Stopping credit card fraud will also generate a feeling of faith in the cardholders towards their banks.

5.2. Policy Implications

The findings of the study are very much helpful to policymakers too. Policymakers can take advantage of findings of the study to make remedial policies accordingly. Likewise, at the time of issuing the card to the holder, banks will be able to know the chances of fraud with that particular person. With the highlighted factors, policies can be made to mitigate fraud. Policymakers can use the variables like distance from home, distance from last transaction, and ratio to the median purchase price, repeat retailer, used chip, used PIN for the transaction, and online order in their home etc. to make the credit card environment more safe and secure. That will be much sounder to all the cardholders and card issuers.

5.3. Scope of the Future Research

This study is done with primary data. From the lens of future studies, the future researcher can extend the light of data collection widely to cover the wide region of society. The researcher can also add a blend of demographical, geographical and psychological factors to go more accurate and reliable which will be much more beneficial to society.

REFERENCES

Aihua, S., Rencheng, T., Yaochen, D. (2007), Application of Classification Models on Credit Card Fraud Detection. In: Proceedings - ICSSSM'07: 2007 International Conference on Service Systems and Service Management, p2-5.

Altman, E., Varetto, F., Di Torino, P., Altman, E. I., Marco, G., Varetto, F. (1994), Corporate distress diagnosis: Comparisons using linear discriminant analysis and neural networks (the Italian experience), Journal of Banking and Finance, 18, 505-529.

Barboza, F., Kimura, H., Altman, E. (2017), Machine learning models and bankruptcy prediction. Expert Systems with Applications, 83, 405-417.

Barker, K.J., D'Amato, J.D., Sheridon, P. (2008), Credit card fraud: Awareness and prevention. Journal of Financial Crime, 15(4), 398-410.

Benchaji, I., Douzi, S., El Ouahidi, B. (2021), Credit card fraud detection model based on LSTM recurrent neural networks. Journal of Advances in Information Technology, 12(2), 113-118.

Bolton, R., Hand, D. (2002a), Statistical fraud detection: A review. Statistical Science, 17(3), 235-255.

Burnes, D., Marguerite, D., Lynn, L. (2020), Risk and protective factors of identity theft victimization in the United States. Preventive Medicine Reports, 17, 101058.

Chakravorti, S., To, T. (2007), A theory of credit cards. International Journal of Industrial Organization, 25(3), 583-595.

Chaudhary, K., Mallick, B. (2012), Credit card fraud: Bang in E-commerce. International Journal Of Computational Engineering Research, 2(3), 935-941.

Coskun, M., Saygili, E., Karahan, M.O. (2022), Exploring online payment system adoption factors in the age of COVID-19-Evidence from the Turkish Banking Industry. International Journal of Financial Studies, 10(2), 39.

D'onza, G., Lamboglia, R. (2014), The Relation between the

Corporate Governance Characteristics and Financial Statement Frauds: An Empirical Analysis of Italian Listed Companies. In: 10th European Academic Conference on Internal Auditing and Corporate Governance. Available from: http://www.iacmaster.it/iacgconference2012/wp-content/uploads/2012/04/D-Onza.pdf

Flitman, A.M. (1997), Towards analysing student failures: Neural networks compared with regression analysis and multiple discriminant analysis. Computers and Operations Research, 24(4), 367-377.

Gadi, M., Wang, X., Lago, A. (2008), Credit card fraud detection with artificial immune system. ICARIS, 8, 119-131.

Gawer, A. (2021), Digital platforms and ecosystems: Remarks on the dominant organizational forms of the digital age. Innovation, 24(1), 110-124.

Hayati, S.N., Zawawi, M., Idris, K.M., Rahman, R.A. (2011), Determinants of behavioral intention of fraudulent financial reporting: Using the theory of reasoned action. Malaysian Accounting Review, 10(1), 43-62.

Heeks, R. (2008), ICT4D 2.0: The next phase of applying ICT for international development. Computer, 41(6), 26-31.

Huang, S.Y., Lin, C.C., Chiu, A.A., Yen, D.C. (2017), Customer churn prediction in telecommunications. Information Systems Frontiers, 19, 1343-1356.

Joshi, M.C. (2017), Digital payment system: A feat forward of India. Research Dimension, 1(1), 1-12.

Kakati, S., Goswami, C. (2019), Factors and motivation of fraud in the corporate sector: A literature review. Journal of Commerce and Accounting Research, 8(3), 86-96.

Kassem, R., Higson, A. W. (2012), The new fraud triangle model. Journal of Emerging Trends in Economics and Management Sciences, 3(3), 191-195.

Khan, A.U.S., Akhtar, N., Qureshi, M.N. (2014), Real-Time Credit-Card Fraud Detection Using Artificial Neural Network Tuned By Simulated Annealing Algorithm. In: Proceedings of International Conference on Recent Trends in Information, Telecommunication and Computing, ITC (ACEEE), p113-121.

Khare, A., Singh, S. (2012), Factors affecting credit card use in India. Asia Pacific Journal of Marketing, 24(2), 236-256.

Kültür, Y., Çağlayan, M.U. (2017), Hybrid approaches for detecting credit card fraud. Expert Systems, 34(2), 1-13.

Kumar, A., Choudhary, R.K., Mishra, S.K., Kar, S.K., Bansal, R. (2022), The growth trajectory of UPI based mobile payments in India: Enablers and inhibitors. Indian Journal of Finance and Banking, 11(1), 45-59.

Lin, J.W., Hwang, M., Becker, J.D. (2003), A fuzzy neural network for assessing the risk of fraudulent financial reporting. Managerial Auditing Journal, 18(8), 657-665.

Linda, D., Abdou, H., John, P. (2009), Credit card fraud and detection techniques: A review. Banks and Bank Systems, 4(2), 57-68.

Mahmoudi, N., Duman, E. (2015), Detecting credit card fraud by modified Fisher discriminant analysis. Expert Systems with Applications, 42(5), 2510-2516.

Misra, S., Thakur, S., Ghosh, M., Saha, S.K.S. (2020), An autoencoder based model for detecting fraudulent credit card transaction. Procedia Computer Science, 167, 254-262.

Munawer, Z., Siti-Nabiha, Y.S.A.K. (2012), Sell-side security analysts: Re-reporting of Enron corporation fraudulent financial data. Procedia - Social and Behavioral Sciences, 62(24), 749-760.

Nizamani, S., Memon, N., Glasdam, M., Nguyen, D.D. (2014), Detection of fraudulent emails by employing advanced feature abundance. Egyptian Informatics Journal, 15(3), 169-174.

Oghojafor, B., Mesike, G., Bakarea, R., Omoera, C., Adeleke, I. (2012), Discriminant analysis of factors affecting telecoms customer churn. International Journal of Business Administration, 3(2), 59-67.

Pawar, A.D., Kalavadekar, P.N., Tambe, S.N. (2014), A Survey on outlier detection techniques for credit card fraud detection. IOSR Journal of Computer Engineering, 16(2), 44-48.

Persons, O.S. (1995), Using financial statement data to identify factors associated with fraudulent financial reporting. Journal of Applied Business Research, 11(3), 38-46.

Pulina, M., Paba, A. (2010), A Discrete Choice Approach to Model Credit Card Fraud. Munich Personal RePEc Archive. Available from: https://mpra.ub.uni-muenchen.de/20019

Quah, J., Sriganesh, M. (2008), Real-time credit card fraud detection using computational intelligence. Expert Systems with Applications, 35(4), 1721-1732.

Quinlan, J.R. (1994), C4.5: Programs for Machine Learning by J. Ross Quinlan. Morgan Kaufmann Publishers, Inc., 1993 (A. Segre (ed.); Vol. 16). Boston: Kluwer Academic Publishers. Available from: http://server3.eca.ir/isi/forum/programs for machine learning.pdf

Quinlan, J.R., Cameron-Jones, R.M. (1993), FOIL: A midterm report. In: Lecture Notes in Computer Science No 667 (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). LNAI, p3-20.

Rezaee, Z. (2005), Causes, consequences, and deterence of financial statement fraud. Critical Perspectives on Accounting, 16(3), 277-298.

Sael, N., Benabbou, F., Sadgali, I. (2018), Detection of credit card fraud: State of art. International Journal of Computer Network and Information Security, 18(11), 76-83.

Schüpfer, G., Hein, J., Casutt, M., Steiner, L., Konrad, C. (2012), Vom Finanz- zum Wissenschaftsbetrug: Methode, den Irrungen in der medizinischen Literatur beizukommen. Anaesthesist, 61(6), 537-542.

Sood, P., Bhushan, P. (2022), Factors impacting banking frauds in India: A conceptual framework. International Journal of Business and Globalisation, 31(4), 500-519.

Sorunke, O.A. (2016), Personal ethics and fraudster motivation: The missing link in fraud triangle and fraud diamond theories. International Journal of Academic Research in Business and Social Science, 6(2), 159-165.

Sriyalatha, M. (2016), Determinants of customers' attitude towards credit card usage: lessons learned from academics in Sri Lanka. Case Studies in Business and Management, Macrothink Institute, 3(2), 19-37.

Summers, S., Sweeney, J. (1998), Fraudulently misstated financial statements and insider trading: An empirical analysis. The Accounting Review, 73(1), 131-146.

Sun, Y., Davidson, I. (2015), Influential factors of online fraud occurrence in retailing banking sectors from a global prospective An empirical study of individual customers in the UK and China. Information and Computer Security, 23(1), 3-19.

Świecka, B., Terefenko, P., Paprotny, D. (2021), Transaction factors' influence on the choice of payment by Polish consumers. Journal of Retailing and Consumer Services, 58, 102264.

Tassabehji, R., Hackney, R., School, M. (2019), Evaluating digital public services A contingency value approach within three exemplar developing countries Takao Maruyama Evaluating digital public services. Information Technology and People, 32(4), 1021-1043.

Tsaih, R.H., Lin, W.Y., Huang, S.Y. (2009), Exploring fraudulent financial reporting with GHSOM. In: Intelligence and Security Informatics: Pacific Asia Workshop 5477. PAISI, p31-41.

Uddin, M.A. (2020), A study on literacy and usage behaviour of credit cards users in India. Humanities and Social Sciences Reviews, 8(1), 60-68.

Wheeler, R., Aitken, S. (2000), Multiple algorithms for fraud detection. Applications and Innovations in Intelligent Systems VII. Germany: Springer, p219-231.

Wolfe, D.T., Hermanson, D.R. (2004), The fraud diamond: Considering the four elements of fraud. CPA Journal, 74(12), 38-42.

Wray, R. (2014), Loanable funds, liquidity preference, and endogenous money: Do credit cards make a difference? Journal of Post Keynesian Economics, 26(2), 309-323.

Wyrobek, J. (2020), Application of machine learning models and artificial intelligence to analyze annual financial statements to identify companies with unfair corporate culture. Procedia Computer Science, 176, 3037-3046.

Yu, X., Li, X., Dong, Y., Zheng, R. (2020), A deep neural network algorithm for detecting credit card fraud. In: 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), p181-183.

Zager, L., Malis, S., Novak, A. (2016), The role and responsibility of auditors in prevention and detection of fraudulent financial reporting. Procedia Economics and Finance, 39, 693-700.

Zaslavsky, V., Strizhak, A. (2006), Credit card fraud detection using self-organizing maps. Information and Security, 18, 48-63.