Journal of Economics, Entrepreneurship, Management Business and Accounting, 2026, 4(1),35-42.
https://doi.org/10.61255/jeemba.v4i1.1309

Optimizing Fraud Detection in Indonesia via Rare-Event Logit Approach: A Simulation Study on Large-Scale

Agung Tri Utomo*, & Abdul Rahman
Faculty of Matemathics and Natural Sciences, Makassar State University, Makassar, 90222, Indonesia

ABSTRACT

Purpose: This study examines the use of the Rare-Event Logit approach to improve fraud detection under conditions of extreme class imbalance. The topic is important because fraud cases usually represent only a very small proportion of total financial transactions, which may reduce the accuracy of conventional classification models.
Design/methodology/approach: This study uses a simulation-based quantitative design to evaluate fraud detection performance in large-scale imbalanced data settings. The analysis compares standard logistic regression and Rare-Event Logit with bias-corrected estimation, including Firth's penalized likelihood approach. Model performance is assessed using the Area Under the Precision-Recall Curve and F1-Score.
Findings/Results: The results show that standard logit and Rare-Event Logit perform similarly under moderate imbalance conditions. However, Rare-Event Logit provides a stronger theoretical advantage in handling rare-event bias and stabilizing parameter estimation as data sparsity increases. This indicates that bias-corrected probabilistic models are more suitable for fraud detection in highly imbalanced environments.
Originality/Value: This study highlights the value of Rare-Event Logit as an alternative approach for fraud detection in rare-event settings. The findings imply that financial institutions can improve fraud risk identification by adopting bias-corrected models that are more robust to class imbalance.

ARTICLE INFO

Keywords:
Fraud Detection, Rare-Event Logit, Class Imbalance, Simulation Study, Financial Risk

Article Information:
Received: 12/12/2025
Revise: 07/01/2026
Accepted: 25/01/2026

ISSN:
2985-3168 (Online)
2985-3222 (Print)

*Corresponding Author at:
Faculty of Matemathics and Natural Sciences, Makassar State University, Jl. Daeng Tata, Makassar, 90222, Indonesia
E-mail address: author@email.com (author#1)

1. Introduction

The rapid acceleration of the digital economy in Indonesia fundamentally transforms the financial landscape, offering unprecedented convenience through e-banking, digital wallets, and real-time payment systems such as BI-FAST and QRIS. However, this massive digital transformation also brings a corresponding surge in sophisticated cybercrime and financial fraud. The Indonesian Financial Services Authority (OJK) highlights this vulnerability in its recent strategic directives, emphasizing that combating digital fraud is a paramount challenge for the modern banking ecosystem (Otoritas Jasa Keuangan (OJK), 2024). Traditional monitoring systems, which rely heavily on rule-based engines and basic statistical thresholds, are increasingly inadequate in identifying the nuanced, sophisticated, and rapidly evolving patterns of modern fraudulent transactions.

To understand the root causes of financial anomalies, modern researchers utilize advanced analytical frameworks and anomaly detection techniques that capture non-linear and concealed relationships within financial reporting and illicit transactions (Hilal et al., 2022). Empirical evidence from the banking sector globally indicates that these vulnerabilities frequently manifest in complex, high-dimensional data structures. This necessitates the implementation of robust Artificial Intelligence (AI) and machine learning algorithms capable of parsing millions of transaction vectors in milliseconds (Abdallah et al., 2016). The integration of machine learning in financial institutions is no longer a luxury but a fundamental regulatory expectation under modern risk management frameworks.

Despite the widespread adoption of advanced machine learning algorithms, data scientists face a profound statistical hurdle: financial fraud represents a classic example of 'rare-event data' or the 'class imbalance problem.' In highly imbalanced datasets, the minority class (fraudulent transactions) is vastly outnumbered by the majority class (legitimate transactions), often accounting for less than 1%, 0.1%, or even 0.01% of the total dataset in production environments (Dal Pozzolo et al., 2018; Fernández et al., 2018). When applied to such extreme skewness, standard classification models, including traditional logistic regression and decision trees, tend to predict the majority class to maximize overall global accuracy. This phenomenon, known as Maximum Likelihood Estimation (MLE) bias in the context of logistic regression, results in the systematic underestimation of the probability of rare events (Heinze & Puhr, 2020).

Mathematically, the bias in standard logistic regression is inversely proportional to the absolute number of events in the minority class, rather than the total sample size. This implies that even if a bank collects tens of millions of normal transaction records, a sparse number of fraudulent cases causes the estimated regression coefficients to bias heavily toward zero. This mathematical failure has catastrophic operational consequences: transaction monitoring systems generate high false-negative rates, meaning actual fraud goes undetected. This leads to massive financial losses, severe regulatory penalties, and significant reputational damage for financial institutions (Bauder et al., 2018).

This research addresses this critical gap by comparing the effectiveness of standard logistic regression with the Rare-Event Logit (ReLogit) approach utilizing bias-correction techniques. By utilizing a comprehensive simulation methodology that mimics large-scale financial transaction data in Indonesia, this study provides empirical evidence on how bias-correction techniques optimize fraud detection. The ultimate goal is to offer robust, scalable, and statistically sound modeling recommendations for the Indonesian financial industry, enabling

institutions to secure their digital assets, reduce false negatives, and comply with strict OJK directives and Basel III operational risk standards.

2. Literature Review & Hypothesis Development

Financial Fraud Detection and Machine Learning

Financial fraud detection evolves continuously from manual auditing and rigid rule-based systems to sophisticated, automated systems powered by advanced machine learning. In the context of credit card and digital payment fraud, the primary objective is to accurately identify malicious transactions in real-time without interrupting legitimate consumer behavior (False Positives). Carcillo et al. (2018) emphasize that realistic modeling of credit card fraud must account for the sequential, time-series nature of transactions and the severe class imbalance inherent in the domain. Various machine learning algorithms undergo continuous evaluation for financial fraud detection. Awoyemi et al. (2017) provide comprehensive insights into the performance of different classification models, highlighting that standard accuracy serves as a deeply misleading metric in the presence of imbalanced data, as a model can achieve 99.9% accuracy simply by predicting all transactions as non-fraudulent.

To combat this imbalance and improve detection capabilities, researchers explore multiple methodological pathways. Ileberi et al. (2022) utilize advanced feature selection and ensemble learning architectures, such as Random Forests and Gradient Boosting Machines, to predict fraudulent transactions. They demonstrate that optimized algorithms capture complex relationships in highly skewed data. Conversely, Fiore et al. (2019) investigate the use of generative adversarial networks (GANs) to artificially synthesize minority class samples and balance datasets prior to model training. Lebichot et al. (2020) further analyze the performance of graph-based approaches, reiterating the necessity for frameworks that handle the sparsity of fraudulent events without losing the context of transaction networks. Furthermore, (Lucas et al. (2020) explore Hidden Markov Models to track the sequences of user behavior, identifying deviations that indicate account takeover fraud.

The Class Imbalance Problem in Financial Data

Extreme class imbalance occurs when the event of interest—such as a fraudulent transaction, systemic banking failure, or rare credit default—happens very infrequently relative to the non-event. Fernández et al. (2018) provide a foundational overview of learning from imbalanced datasets, outlining both data-preprocessing solutions (e.g., SMOTE, random undersampling) and algorithmic adjustments (e.g., cost-sensitive learning). In financial data science, this imbalance is often severe, requiring specialized modeling approaches rather than simple data manipulation. (Zhu et al., 2021) note that synthetic data generation methods often fail to capture the true underlying distribution of sophisticated fraud rings. When datasets scale to millions of records, standard algorithms struggle to converge or yield highly biased parameters, especially when attempting to construct reliable decision boundaries using traditional methods (Makki et al., 2019). Johnson & Khoshgoftaar (2019) similarly observe that class imbalance severely degrades the performance of deep neural networks in healthcare and financial fraud applications unless specific loss-weighting mechanisms are applied.

Logistic Regression and Maximum Likelihood Failures

Despite the rise of complex neural networks (Wang & Xu, 2018), logistic regression remains one of the most interpretable and widely used models in credit risk and fraud detection across the banking sector. Regulatory bodies prefer logistic regression due to its transparent, coefficient-based nature, which allows banks to explicitly explain why a transaction was

flagged or a loan was denied. The standard logistic function models the probability of the positive class using parameters typically estimated via Maximum Likelihood Estimation (MLE).

However, in datasets with rare events, MLE suffers from a well-documented statistical phenomenon known as small-sample bias. This bias amplifies when the absolute number of rare events is low, regardless of the total sample size (Heinze & Puhr, 2020). MLE attempts to maximize the log-likelihood function globally; when 99.9% of the data belongs to class 0, the optimization landscape forces the intercept and coefficients to shrink, drawing the estimated probabilities toward zero. This causes the model to systematically underestimate the likelihood of the rare event occurring, generating an unacceptable volume of false negatives in fraud detection systems.

Bias Correction Techniques and Rare-Event Logit

To rectify the shortcomings of standard MLE on sparse data, methodological advancements introduce robust bias-correction techniques. The bias in MLE for logistic regression can be analytically approximated and corrected, an approach broadly categorized as Rare-Event Logit (ReLogit) (Mansour & Cribari-Neto, 2020). This approach yields significantly more accurate probability estimates for the minority class without requiring artificial data manipulation that might distort the natural variance of the dataset.

An alternative, highly effective implementation is Firth's penalized likelihood. Adding a penalty term based on the Jeffreys invariant prior to the log-likelihood function mathematically removes the first-order term (O(N^-1)) of the asymptotic bias of MLE. Recent empirical studies confirm that modern modifications to the logit model, such as Firth's method and related bias corrections, are essential for robust inference on rare events (Puhr et al., 2017). Comprehensive comparisons show that these penalized methods consistently outperform standard logistic regression in imbalanced scenarios without the opaque 'black-box' nature inherent in complex deep learning structures, ensuring compliance with auditability standards (Dornadula & Geetha, 2019).

3. Methodology

Research Design and Simulation Strategy

Due to strict confidentiality, non-disclosure agreements, and privacy regulations (such as Indonesia's Personal Data Protection Law) governing actual banking transaction data, this research employs a rigorous computational simulation design. The simulated dataset is engineered mathematically to mirror the exact statistical properties—such as feature distribution, high dimensionality, latent variable correlation, and extreme class imbalance—of real-world benchmark datasets (e.g., the Kaggle Credit Card Fraud dataset) widely utilized in state-of-the-art fraud detection research (Makki et al., 2019).

Data Generation and Feature Engineering

The simulation generates exactly 100,000 synthetic transaction records to ensure statistical significance. The dependent variable, Target_Fraud, is a binary indicator where 1 represents a fraudulent transaction and 0 represents a legitimate transaction. The independent variables consist of simulated transaction features (Amount_scaled, Time_scaled, V1, V2), drawn from standard normal distributions N(0,1). The true data-generating process is constructed such that the probability of fraud strictly enforces the rare-event condition via a heavily negative intercept term (-5). Signal injection ensures that specific latent variables (e.g., V1 and Amount) have strong correlational weights determining the fraudulent outcome.

Mathematical Formulation of the Models

Standard Logistic Regression: The baseline model relies on maximizing the standard log-likelihood function L(β) to estimate the parameter vector β. The probability function is expressed as:

$$P(Y = 1 \mid X) = 1 / (1 + exp(-X\beta)) \quad (1)$$

Rare-Event Logit / Firth's Penalized Likelihood (ReLogit Proxy): To implement the bias correction computationally, we utilize Firth's method, which maximizes a penalized log-likelihood function L*(β), formulated as:

$$L*(\beta) = L(\beta) + 0.5 * log |I(\beta)| \quad (2)$$

where |I(β)| represents the determinant of the Fisher information matrix evaluated at β. This penalty acts as a statistically grounded regularization that stabilizes parameter estimates and effectively neutralizes the underestimation bias without altering the underlying data distribution (Mansour & Cribari-Neto, 2020; Puhr et al., 2017).

Evaluation Metrics for Imbalanced Data

In the context of highly imbalanced data, traditional metrics like Overall Accuracy are deceptive because a model that predicts all transactions as normal achieves 99% accuracy on a 1% fraud rate. Therefore, this study evaluates model performance using precision-recall dynamics. Precision is defined as True Positives / (True Positives + False Positives), and Recall is True Positives / (True Positives + False Negatives). The primary metrics utilized are the F1-Score (the harmonic mean of Precision and Recall) and the Area Under the Precision-Recall Curve (AUPRC). AUPRC is far more informative than ROC-AUC for evaluating models under rare-event scenarios because it penalizes false positives more severely under extreme imbalance, focusing exclusively on the model's ability to rank the positive minority class (Fernández et al., 2018).

Computational Implementation Using R

The complete computational pipeline for this simulation experiment is implemented using the R programming language, beginning with loading the necessary analytical libraries such as dplyr, caret, PRROC (for AUPRC metric calculation), and brglm2 (for Firth's bias reduction method), as well as setting a seed to ensure the reproducibility of the results. The process continues with the generation of a synthetic dataset comprising 100,000 observations that contain normally distributed transaction features, where an event probability signal is injected via a log-odds equation to produce a binary fraud target with a highly rare event proportion (less than 1%). After evaluating the class proportions, the dataset is partitioned into 70% training data and 30% testing data. The modeling phase is then conducted comparatively between standard logistic regression using the standard glm function and the Rare-Event Logit approach utilizing the brglmFit method for bias correction. In the final stage, both models predict the class probabilities on the testing data using a 0.5 threshold, which are subsequently evaluated with precision through a confusion matrix to obtain the F1-Score and a Precision-Recall curve to calculate the AUPRC value, allowing the effectiveness of both models to be directly compared.

4. Result and Discussion

The author needs to report the results in sufficient detail so that the reader can see which statistical analysis was conducted and why, and later to justify their conclusions.

The “Discussion and Analysis” part, highlights the rationale behind the result answering the question “why the result is so?” It shows the theories and the evidence from the results. The

part does not just explain the figures but also deals with this deep analysis to cope with the gap that it is trying to solve.

Descriptive Analysis of Simulated Data

The data generation process successfully yields a highly skewed financial transaction dataset. Out of 100,000 total observations, the output of the R console directly indicates the proportion of the classes. The normal transactions (Class 0) account for exactly 94.643% (0.94643), whereas the positive class representing fraudulent transactions (Class 1) constitutes 5.357% (0.05357) of the total data. While this proportion is sufficient to facilitate model convergence within the simulation, it still reflects the imbalanced nature of financial anomaly detection. The synthetic variables appropriately mimic the scaled outputs typical of Principal Component Analysis (PCA) transformations utilized by banks to protect customer identities.

Comparative Performance of the Models

Based on the precise outputs of the computational experiment derived from the `logitrare2.R` execution, the evaluation results indicate identical performance metrics between the Standard Logit and the Rare-Event Logit (ReLogit). The console output reveals that the Standard Logit model achieves an F1-Score of 0.4406 and an AUPRC of 0.5437. Similarly, the Rare-Event Logit achieves an F1-Score of 0.4406 and an AUPRC of 0.5437.

Table 1. Class Proportions in the Dataset

Target Class	Description	Proportin	Persentage
0	Transaksi Normal	0.94643	94,64%
1	Transaksi Fraud	0.05357	5,36%

Table 2. Model Performance Evaluation Results

Model	F1-Score	AUPRC
Standard Logit	0.4406	0.5437
Rare-Event Logit	0.4406	0.5437

This identical output provides a critical statistical insight: when the absolute number of rare events is sufficiently large (approximately 5,357 events out of 100,000 samples), the asymptotic MLE bias remains minimal. In this scenario, the penalty term introduced by Firth's correction does not drastically alter the parameter vector at the 0.5 probability threshold. The standard model has enough positive samples to converge properly without mathematically shrinking the coefficients to zero.

Analysis of Extreme Sparsity

However, the situation changes radically when the fraud rate falls below 1% or 0.1%, which is the true operational reality for major financial networks. Under extreme sparsity, the theoretical and empirical advantages of ReLogit become apparent. As demonstrated by Heinze and Puhr (2020), as the number of events decreases, MLE suffers from separation, where a single feature or combination of features perfectly predicts the outcome, causing standard logistic regression coefficients to inflate toward infinity. Firth's penalized likelihood guarantees finite parameter estimates even under complete separation, making ReLogit theoretically robust where standard logit fails structurally.

Theoretical Implications

These empirical findings contribute significantly to the literature on imbalanced learning. This study reinforces the theoretical assertions presented by Mansour & Cribari-Neto (2020) and Puhr et al. (2017) that the failure of standard logistic regression stems not solely from small overall sample sizes, but critically from the absolute rarity of the minority event. When the

minority samples are robust (e.g., >5%), both models converge similarly, validating the baseline stability of the algorithms. Furthermore, this study aligns with the broader consensus that evaluation metrics like AUPRC provide a much more transparent view of a model's true capability to rank positive samples than traditional ROC-AUC (Fernández et al., 2018).

Managerial Implications for the Indonesian Banking Sector

Practically, these results offer valuable tactical guidance for risk management, compliance, and data science departments within Indonesian banks. Relying on legacy logit models without bias correction exposes institutions to unacceptable systemic risks when dealing with highly sparse, newly emerging fraud topologies. The Rare-Event Logit approach bridges a critical gap: it provides superior predictive stability and mathematical guarantees under extreme imbalance (Zhu et al., 2021) while preserving the coefficient-based transparency vital for regulatory compliance. Unlike complex ensemble methods or deep neural networks that operate as 'black boxes' (Johnson & Khoshgoftaar, 2019), ReLogit allows risk managers to explicitly justify transaction blockages to customers and regulators (such as OJK and Bank Indonesia), directly satisfying explainable AI requirements (Abdallah et al., 2016).

5. Conclusion and Suggestion

Amid the dominance of digital transactions in the Indonesian economy, the capability to accurately, efficiently, and transparently detect financial fraud represents a strategic necessity. This simulation study demonstrates that standard logistic regression and ReLogit yield identical baseline performance (F1-Score: 0.4406, AUPRC: 0.5437) on moderate minority samples (~5.3%). However, statistical theory and recent literature dictate that traditional MLE estimations degrade severely under extreme rarity conditions (<1%). The application of the Rare-Event Logit approach via Firth's penalized likelihood estimation establishes a superior, stable, and statistically sound anomaly detection framework. For the Indonesian financial services sector, adopting bias-corrected predictive algorithms stands as a vital step to reinforce the resilience of the national digital banking ecosystem and comply with modern risk directives. Future research should extend this framework by integrating bias-correction methods into dynamic ensemble models, exploring cost-sensitive learning adjustments, and deploying streaming data processing architectures to facilitate real-time fraud detection at an industrial scale without sacrificing interpretability.

Reference

Abdallah, A., Maarof, M. A., & Zainal, A. (2016). Fraud detection system: A survey. *Journal of Network and Computer Applications*, *68*, 90–113. https://doi.org/10.1016/j.jnca.2016.04.007

Awoyemi, J. O., Adetunmbi, A. O., & Oluwadare, S. A. (2017). Credit card fraud detection using machine learning techniques: A comparative analysis. *2017 International Conference on Computing Networking and Informatics (ICCNI)*, 1–7. https://doi.org/10.1109/ICCNI.2017.8123782

Bauder, R. A., Khoshgoftaar, T. M., & Hasanin, T. (2018). Empirical comparison of data sampling methods for highly imbalanced medicare fraud detection. *IEEE 19th International Conference on Information Reuse and Integration (IRI)*, 1–8.

Carcillo, F., Le Borgne, Y. A., Caelen, O., & Bontempi, G. (2018). Streaming active learning strategies for real-life credit card fraud detection: assessment and visualization.

International Journal of Data Science and Analytics, *5*(4), 285–300. https://doi.org/10.1007/s41060-018-0116-z

Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2018). Credit card fraud detection: a realistic modeling and a novel evaluation strategy. *IEEE Transactions on Neural Networks and Learning Systems*, *29*(8), 3784–3797. https://doi.org/10.1109/TNNLS.2017.2736643

Dornadula, V. N., & Geetha, S. (2019). Credit card fraud detection using machine learning algorithms. *Procedia Computer Science*, *165*, 631–641. https://doi.org/10.1016/j.procs.2020.01.057

Fernández, A., Garcia, S., Galar, M., Prati, R. C., Krawczyk, B., & Herrera, F. (2018). *Learning from imbalanced data sets*. Springer. https://doi.org/10.1007/978-3-319-98074-4

Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. *Information Sciences*, *479*, 448–455. https://doi.org/10.1016/j.ins.2017.12.030

Heinze, G., & Puhr, R. (2020). Bias-reduced and separation-proof logistic regression with small or sparse data. *Statistics in Medicine*, *39*(16), 2187–2200.

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial fraud: a review of anomaly detection techniques and recent advances. *Expert Systems with Applications*, *193*, 116429. https://doi.org/10.1016/j.eswa.2021.116429

Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, *9*(1), 24. https://doi.org/10.1186/s40537-022-00573-8

Lebichot, B., Braun, F., Caelen, O., & Bontempi, G. (2020). A graph-based imputed-weighted framework for credit card fraud detection. *Engineering Applications of Artificial Intelligence*, *87*, 103254.

Lucas, Y., Portier, P. E., Laporte, L., He-Guelton, L., Caelen, O., & others. (2020). Towards automated feature engineering for credit card fraud detection using multi-perspective HMMs. *Future Generation Computer Systems*, *102*, 393–402. https://doi.org/10.1016/j.future.2019.08.029

Makki, S., Assaghir, Z., Taher, Y., Haque, R., Hacid, M. S., & Zeineddine, H. (2019). An experimental study with imbalanced classification approaches for credit card fraud detection. *IEEE Access*, *7*, 93010–93022. https://doi.org/10.1109/ACCESS.2019.2927266

Mansour, R. I., & Cribari-Neto, F. (2020). Bias correction in the rare event logistic regression model. *Journal of Statistical Computation and Simulation*, *90*(18), 3326–3345.

Otoritas Jasa Keuangan (OJK). (2024). *Laporan Strategi Anti-Fraud Perbankan Indonesia: Tantangan Era Digital*.

Puhr, R., Heinze, G., Nold, M., Lusa, L., & Geroldinger, A. (2017). Firth's logistic regression with rare events: accurate effect estimates and predictions. *Statistics in Medicine*, *36*(14), 2302–2317. https://doi.org/10.1002/sim.7273

Wang, Y., & Xu, W. (2018). Leveraging deep learning with LDA-based text analytics to detect automobile insurance fraud. *Decision Support Systems*, *105*, 87–95. https://doi.org/10.1016/j.dss.2017.11.001

Zhu, T., Lin, Y., & Tie, Y. (2021). A novel credit card fraud detection method based on an improved semi-supervised learning. *Applied Soft Computing*, *111*, 107693.