Universal Library of Business and Economics Research Article

ISSN: 3064-9951 | Volume 2, Issue 3

Open Access | PP: 129-133

DOI: https://doi.org/10.70315/uloap.ulbec.2025.0203024

Fraud in Consumer and Mortgage Lending: Algorithms for Detection and Prevention

Dikopoltseva Svetlana Aleksandrovna

Abstract

In the paradigm of accelerated digital transformation of the lending sector and the exponential growth of loan volumes the relevance of countering fraudulent schemes increases manifold resulting in economic losses for both banking institutions and end borrowers. The study is focused on substantiating comprehensive algorithmic solutions for detecting and suppressing fraud activities in the consumer and mortgage lending segments. The objective of the work is to systematize modern anti-fraud methods and to formulate a scientific and methodological foundation for designing highly scalable and adaptive security systems. The methodological basis of the research relies on an extensive analysis of specialized publications in recent years an overview of advanced practices in the application of machine learning big data processing and their integration with external information ecosystems. As empirical justification the results of the implementation of the author automated system for comprehensive borrower verification are presented. Experimental data demonstrate the superiority of hybrid architectures combining multi-level verification against governmental and commercial registers with intelligent encoding of risk profiles and interregional matching of applications. The expediency of evolving from fully manual processing to 90 % automation of decision-making is argued which ensures the processing of multimillion flows of credit applications with high speed and reliability. It is concluded that further development of fraud prevention systems will take place at the intersection of artificial intelligence technologies and predictive analytics creating a synergistic effect to enhance the quality of risk management. The materials presented in this article will be of interest to specialists in financial risk management fintech industry researchers and software developers for credit institutions.

Keywords: *Credit Fraud Mortgage, Fraud Fraud Detection, Fraud Prevention, Machine Learning, Scoring, Automation, Big Data, Borrower Verification, Fraud Monitoring.*

INTRODUCTION

Intensive digitization of the credit and financial sector has expanded and accelerated the population's access to borrowed resources while simultaneously creating favorable conditions for the development of increasingly sophisticated fraudulent schemes. The dynamics of credit growth are explained by general macroeconomic trends; however, alongside this there is an increase in both the absolute and relative number of fraud-related transactions. Thus, according to estimates by the Frank RG analytical center, in 2024 the volume of new loans using borrowed funds in the second quarter reached 182.2 billion dollars, more than twice the figure for the same period in 2023, which amounted to 79.5 billion dollars, and approaches the record levels of 2021 [4]. At the same time, banks in the euro area reported a renewed tightening of requirements for loans and credit lines to enterprises in the fourth quarter of 2024 [5], clearly demonstrating the scale of the damage inflicted and the seriousness of the challenge to financial stability and public trust.

Concern is also raised by the evolution of fraudulent schemes from the use of forged identity documents to multi-stage attacks with elements of social engineering, phishing and creation of synthetic identities (synthetic identity fraud), the detection of which by traditional tools is complicated by the high degree of masking and adaptability of criminals [8]. The current situation reveals a scientific gap in countering fraud risks: existing models and algorithms often lack sufficient flexibility to operate under rapidly changing threats.

Most studies are limited to the analysis of individual vectors of the problem, for example the development of machine-learning models to detect anomalies in transactional data [7] or the study of legal mechanisms for preventing fraud [5]. Meanwhile, an ultimate integrated approach that would combine technological, organizational and analytical

Citation: Dikopoltseva Svetlana Aleksandrovna, "Fraud in Consumer and Mortgage Lending: Algorithms for Detection and Prevention", Universal Library of Business and Economics, 2025; 2(3): 129-133. DOI: https://doi.org/10.70315/uloap.ulbec.2025.0203024.

measures into a single adaptive fraud-monitoring system has yet to be presented. The absence of a clear methodology that would not only respond to already known schemes but also predictively track and block new, as yet undescribed patterns remains a key task for further scientific research and practical development.

The aim of this work is the systematization of modern anti-fraud methods and the formulation of a scientific and methodological foundation for the design of highly scalable and adaptive security systems.

The scientific novelty manifests itself in demonstrating the effectiveness of a fundamentally new comprehensive algorithm for combating credit fraud, which is based on a synergistic combination of automatic verifications with state and commercial registries, subsequent intellectual systematization of identified risks and interregional comparison of credit applications.

The author's hypothesis is that the implementation of a multilevel verification system providing for the automatic verification of applicant data across a wide range of independent sources and their subsequent classification using machine-learning methods will make it possible to:

1. Reduce the share of manual operations and the associated operational costs.
2. Improve the accuracy of detecting complex fraud schemes, including those of an organized nature.

MATERIALS AND METHODS

Modern research in the field of detection and prevention of fraud in consumer and mortgage lending can be conventionally divided into three main groups based on semantic and methodological proximity. The first group includes works devoted to the development and application of machine learning and artificial intelligence algorithms for the detection of anomalies and suspicious transactions. The second group comprises analytical reports and reviews that form an understanding of current trends and the scale of fraud at the industry level. The third group includes practical recommendations and corporate publications on the implementation of specialized software to combat synthetic identities and anti-fraud systems.

In the first group, primary attention is paid to algorithmic approaches and evaluation of their effectiveness. In the work Tanouz D. et al. [1] an ensemble of classical machine learning methods (random forest, support vector machine and gradient boosting) for detection of fraudulent credit card transactions is proposed: the authors demonstrate that combining models increases anomaly detection accuracy to 96 %. Hashemi S. K., Mirtaheri S. L., Greco S. [7] investigate the application of clustering algorithms and autoencoders for preprocessing banking data and reducing the share of false positives, showing the advantages of hybrid approaches combining supervised and unsupervised learning. In the review by Olowu O. et al. [6] a wide range of methods from classical decision trees to deep neural networks and graph analytics algorithms is systematized, with emphasis on the role of feature engineering and the importance of sample balancing. Velloor Sivasubramanian S., Skillicorn D. [10] apply deep recurrent and convolutional neural networks to analyse texts of the MD&A sections of annual company reports, demonstrating high sensitivity to linguistic features and the possibility of early detection of financial irregularities. Rehan H. [2] focuses on implementation of solutions in cloud infrastructure using real-time data streaming, which ensures minimization of latency in transaction analysis.

The second group of sources emphasizes current trends and macroeconomic factors influencing the level of fraud. In the 2024 Payment Threats and Fraud Trends Report [3] new attack vectors (API fraud, digital wallet compromise) are analysed and a 15 % increase in artificially coordinated campaigns compared to the previous year is predicted. In the review Credit Markets Update Q2 2024 [4] by KPMG it is noted that against the backdrop of tightening lending conditions and reduced availability of borrowed funds, motivation for fraudulent schemes in the consumer and mortgage lending segment increases, requiring strengthened monitoring of payment discipline. The euro area bank lending survey [5] of the European Central Bank provides data on lending trends and default risks, allowing assessment of the relationship between changes in interest rate policy and fraudster activity in the banking sector.

The third group combines publications focusing on compliance tools and practical solutions. In the material The Role of AML Sanctions Screening Software in Detecting Synthetic Identity Fraud [8] mechanisms of sanctions screening and their effectiveness in detecting synthetic identities are considered, emphasising the importance of integrating external sanctions lists and behavioural analysis. In the article The New Frontline of Finance: Why Every Business Needs an Anti-Fraud System in 2025 [9] the strategic role of automated anti-fraud platforms integrating machine learning modules, social network analysis and biometric checks to minimise operational risks is emphasised.

Thus despite the fact that many authors concur on the high effectiveness of hybrid algorithms and real-time hybrid systems, the literature exhibits contradictions in the assessment of the trade-off between model sensitivity and the level of false positives. Issues of standardisation of algorithm evaluation metrics and exchange of anonymised data between banks to improve cross-portfolio fraud detection, as well as legal and ethical aspects of using biometric data for borrower authentication, remain poorly covered.

RESULTS AND DISCUSSION

The transformation of fraud protection systems in the lending sector is driven not only by the exponential quantitative growth of loan issuances but also by the increasing complexity of the essential characteristics of fraudulent scenarios. In accordance with leading international practices up to 90 %

of decisions are generated by algorithmic means while the remaining 10 % of applications with an elevated level of uncertainty are redirected to expert evaluation and detailed manual analysis. It is in this context that the development and implementation of advanced fraud detection methods serves as the foundation for ensuring the reliability of the banking and credit infrastructure

Based on the analysis of global practices in combating fraud and our own empirical database a multi-tiered architecture of an anti-fraud algorithm has been developed (see Figure 1). This complex integrates a cascade system of automated checks (rule-based) intelligent coding of risk profiles based on expert knowledge and adaptive machine learning modules that provide dynamic enhancement of mechanisms for detecting anomalies and suspicious patterns

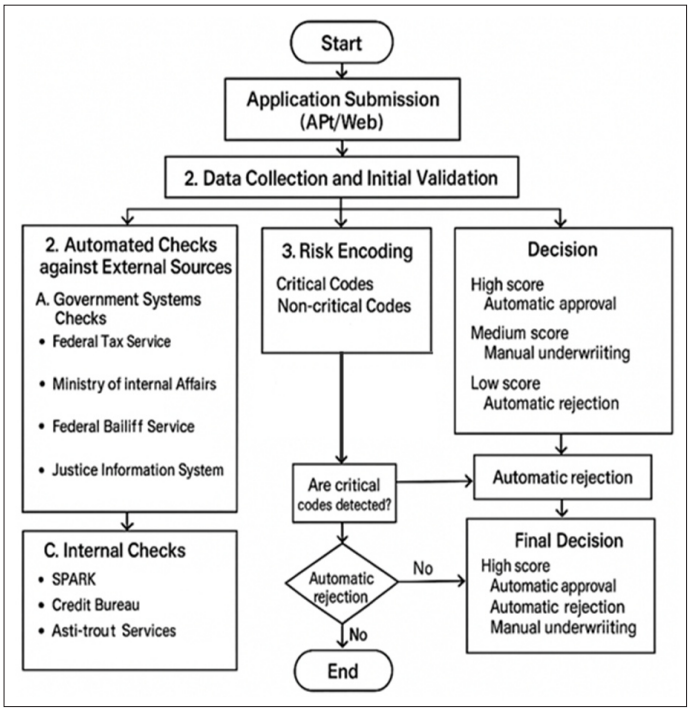

Fig. 1. Comprehensive algorithm for identifying and preventing credit fraud (compiled by the author based on [6, 7]).

As can be seen from Figure 1, at the first foundational yet decisive stage a technological integration of the client verification system is realized through automated access to state information registries and specialized internet portals . Within this procedure an attestation of key identifiers is performed. Of particular significance is the interfacing with the SPARK analytical system, which not only confirms the existence of the employer organization but also provides an instrumental framework for assessing its reliability: analysis of registration date, principal financial metrics, detection of indicators of one-day firms, concentration of mass addresses or nominal leadership [10]. This comprehensive approach enhances resilience to false employment schemes.

At the subsequent stage the verification outcomes are classified into critical and non-critical indicators forming the basis of automated scoring. Critical data are those unequivocally indicating a high risk of fraudulent actions or non-repayment of funds — for example inclusion of the passport in the list of invalid documents, presence of convictions under economic statutes, as well as the fact of liquidation of the employing organization at the time of application submission. Detection of at least one such marker entails an immediate refusal without further consideration. In contrast non-critical indicators in themselves do not constitute grounds for denial but are taken into account in the scoring model, increasing the overall assessed risk level.

In the course of evolution of this system its efficiency has demonstrated stable growth driven by continuous refinement of algorithmic and methodological components. At the initial stage any information regarding the client's involvement in legal proceedings was automatically interpreted as a sign of high risk. The implementation of a mechanism for categorization of judicial data allowed distinction of the legal status of the individual (accused, respondent, witness), which in turn substantially reduced the number of false-positive alerts and rejections of bona fide borrowers whose participation was exclusively in the capacity of witness.

The next significant improvement was the introduction of a procedure for cross-referencing loan applications. This system of cross-analysis facilitated the detection of organized fraudulent groups employing a strategy of partial modification of personal data — for example alteration of registration address — to mass-submit applications to various regional branches of one or multiple banks. Centralized analytics revealed characteristic schemes of such operations and allowed prevention of significant financial losses. The approach is fully consistent with the conclusions of several researchers emphasizing the importance of data unification and consolidation for combating synthetic and hybrid identities [8].

Empirical confirmation of the performance of the comprehensive automated system is provided by statistics: Figure 2 presents the dynamics of growth of the unsecured lending market.

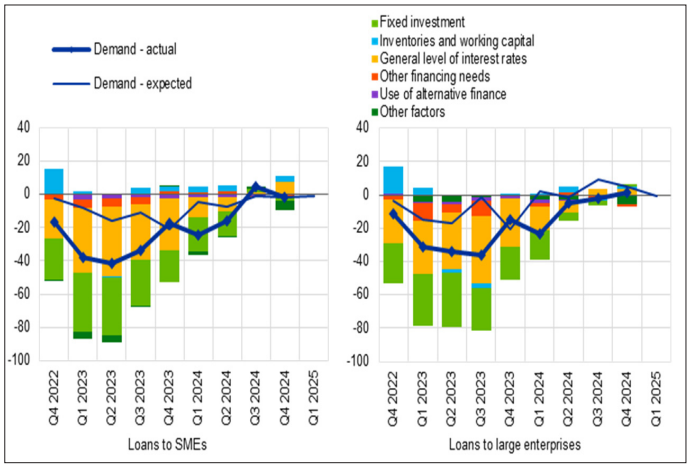

Fig. 2. Dynamics of the consumer loan portfolio and losses from fraud [3, 5].

The growing volume of the unsecured credit portfolio

exacerbates the vulnerability of banking structures to fraudulent schemes, and in the absence of adaptive AI tools the level of financial losses would have been higher.

Table 1 provides a comparison of the key performance metrics of traditional manual application processing and the automated review process.

Table 1. Comparative efficiency of manual and automated processing of credit applications (compiled by the author based on [1, 6]).

Indicator	100 % manual processing (before implementation)	90 % automated processing (after implementation)
Average processing time per application	45 – 60 minutes	1 – 3 minutes
Throughput (applications/hour/employee)	1 – 2	up to 1000 (system) + manual post-processing
Fraud detection rate	55 – 60 %	80 – 85 %
False positive rate	~ 10 %	~ 3 – 5 %
Cost per application	~ 300 – 400 ₽	~ 50 – 70 ₽

Comparative analysis indicates that the automated platform demonstrates multiple-fold superiority over traditional manual processing in both time expenditure and economic efficiency, while delivering higher fraud-detection accuracy rates and reducing the number of false declines. Achieving such performance levels is made possible by eliminating the influence of the operator subjective factor, the system capability for large-scale parallel analysis of big data and the application of multistage logical algorithms in combination with ML models processing hundreds of features for each request [2, 9].

Implementation of these methodologies has enabled the resolution of a fundamental problem: to ensure continuous processing of an exponentially growing flow of credit applications while simultaneously improving the quality of fraud-monitoring. Architecturally the system integrates rigid stop factors aimed at the immediate blocking of suspicious operations with flexible machine-learning models that adapt to the emergence of new behavioral patterns. This combination of deterministic rules and self-learning algorithms generates a synergistic effect, becoming the cornerstone of a proactive risk-management platform capable of responding promptly to the evolution of threats in the digital economy.

CONCLUSION

As a result of the comprehensive analysis of modern methods for combating fraud in the consumer and mortgage lending segments, a generalized model of key approaches and tools was formed. It was established that with the rapid growth of the digitalization of financial services and the constant complication of fraud schemes, classical methodologies based predominantly on manual verification and rigidly fixed rules currently not only lose an increasing share of effectiveness but also prove to be excessively costly in terms of operational resources.

The conclusion of the study confirms the hypothesis of the superiority of a multi-level, modularly constructed system of algorithms combining various technological components into a single working pipeline. In its architecture, the following priority subsystems have been identified:

Automated data collection and verification. Systematic access to an extensive spectrum of external information sources — from state registries to commercial databases — allows in online mode the confirmation of the applicant's identity and the correctness of the information declared by them, minimizing the human factor.

Intelligent risk classification. All detected anomalies are categorized as critical (so-called stop-factors), which automatically lead to the rejection of the application, and non-critical, serving as syllabi for scoring models. This differentiation optimizes the work of underwriting specialists, focusing their attention on the most ambiguous cases.

Application of machine learning and big data analytics methods. In particular, interregional comparison of applications reveals signs of organized and systematic fraud, including attempts to use synthetic identities. This subsystem is dynamically trained on historical and current samples, enhancing adaptability to new fraud scenarios.

The practical value of the proposed model is confirmed by pilot data: the transition from fully manual application review to a hybrid format, where approximately 90 % of decisions are made automatically, made it possible not only to cope with the sharp increase in application volumes but also to improve the accuracy of fraud detection while simultaneously reducing operational costs.

Thus, the implementation of the presented approach creates a solid methodological foundation for banking and non-banking credit organizations seeking to modernize or build from scratch their own fraud monitoring systems, thereby ensuring increased resilience and security of the financial sector.

REFERENCES

1. Tanouz D. et al. Credit card fraud detection using machine learning //2021 5th international conference on intelligent computing and control systems (ICICCS). – IEEE, 2021. – pp. 967-972.
2. Rehan H. Leveraging AI and cloud computing for Real-Time fraud detection in financial systems //Journal of Science & Technology. – 2021. – Vol. 2 (5). – pp. 127.

3. 2024 Payment Threats and Fraud Trends Report [Electronic resource] Access mode: https://www.europeanpaymentscouncil.eu/sites/default/files/kb/file/2024-12/EPC162-24%20v1.0%202024%20Payments%20Threats%20and%20Fraud%20Trends%20Report_0.pdf (accessed: 06/12/2025).
4. Credit Markets Update Q2 2024. [Electronic resource] Access mode: https://corporatefinance.kpmg.com/us/en/insights/2024/credit-markets-update-q2-2024.html (date accessed: 15.06.2025).
5. The euro area bank lending survey. [Electronic resource] Access mode: https://www.ecb.europa.eu/stats/ecb_surveys/bank_lending_survey/html/ecb.blssurvey2024q4~e1ddae0f19.en.html#toc2 (date of access: 18.06.2025).
6. Olowu O. et al. AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity //Advanced Research and Review. – 2024. – Vol. 21 (2). – pp. 227-237.
7. Hashemi S. K., Mirtaheri S. L., Greco S. Fraud detection in banking data by machine learning techniques //Ieee Access. – 2022. – Vol. 11. – pp. 3034-3043.
8. The Role of AML Sanctions Screening Software in Detecting Synthetic Identity Fraud. [Electronic resource] Access mode: https://lucinity.com/blog/the-role-of-aml-sanctions-screening-software-in-detecting-synthetic-identity-fraud (date of access: 06/24/2025).
9. The New Frontline of Finance: Why Every Business Needs an Anti-Fraud System in 2025. [Electronic resource] Access mode: https://www.tookitaki.com/compliance-hub/anti-fraud-system-fintech-2025 (date of access: 06/28/2025).
10. Velloor Sivasubramanian S., Skillicorn D. Predicting fraud in MD&A sections using deep learning //Journal of Business Analytics. – 2024. – Vol. 7 (3). – pp. 197-206.