

Data ethics and privacy in machine learning-driven financial systems: Implications for U.S. Credit Unions and Community Banks

Evelyn Agyei ^{1,*} and Matthew Oman-Amoako ²

¹ Independent Researcher, Connecticut, USA.

² Independent Researcher, Texas, USA.

Magna Scientia Advanced Research and Reviews, 2026, 17(02), 300–309

Publication history: Received on 22 June 2026; revised on 29 July 2026; accepted on 01 August 2026

Article DOI: <https://doi.org/10.30574/msarr.2026.17.2.0154>

Abstract

This paper explores data ethics and privacy issues in machine learning-driven financial systems, with particular attention to their implications for U.S. credit unions and community banks. As financial institutions increasingly adopt machine learning for credit risk assessment, fraud detection, anti-money laundering monitoring, personalization, and operational risk management, ethical concerns surrounding algorithmic bias, data misuse, transparency, explainability, and regulatory accountability have become more significant. Drawing on recent literature, the paper shows that although machine learning can improve efficiency and predictive accuracy, it may also reinforce historical inequities, expose sensitive customer data, and weaken trust when governance mechanisms are inadequate. The analysis emphasizes that smaller financial institutions face distinctive challenges because they often operate with limited technical resources, smaller datasets, and greater dependence on third-party vendors. It further discusses privacy-preserving approaches such as federated learning, explainable AI, data minimization, and ethical auditing as practical tools for responsible adoption. The paper concludes that credit unions and community banks can benefit from machine learning only when innovation is balanced with fairness, privacy protection, human oversight, vendor accountability, and community-centered governance.

Keywords: Data; Ethics; Machine Learning (ML); Finance; Credit Unions.

1. Introduction

Machine learning (ML) has emerged as a transformative force across various industries, and its impact on financial services has been particularly profound. ML encompasses a range of technologies and methodologies, including deep learning, natural language processing, and computer vision (Chieng et al., 2026). These technologies enable systems to perform tasks that typically require human intelligence, such as pattern recognition, decision-making, and problem-solving. In financial institutions, particularly credit unions, ML offers unprecedented capabilities for data analysis, predictive modeling, and automation (Agyei & Lettu, 2026). The ability of ML systems to process vast amounts of structured and unstructured data in real time has opened up new possibilities for risk identification, assessment, and management. ML algorithms can detect subtle patterns and correlations that may elude human analysts, providing deeper insights into potential risks and opportunities (Xu et al., 2024).

As technology advances, financial fraud has also become more sophisticated due to the increasing availability, accessibility, and evolution of digital technologies and online financial systems (Efendi et al., 2025; Shah et al., 2025). Financial fraud represents a highly significant problem, resulting in grave consequences across business sectors and impacting people's daily lives (Singh et al., 2022). Therefore, credit risk assessment and fraud detection are crucial tasks in the financial industry, vital to preserving financial organizations' legitimacy and sustainability. Traditional methods

* Corresponding author: Evelyn Agyei.

often fall short in accurately assessing risk and detecting fraudulent activities in a timely manner. In recent years, machine learning has emerged as a powerful tool for enhancing these processes, leveraging large dimensions of transactional statistics and superior algorithms for making more informed decisions (Surana, 2024). This has led to the integration of machine learning into financial systems and institutions.

The rapid integration of machine learning in banking has significantly reshaped financial operations by offering improved efficiency, tailored customer experiences, and advanced risk management. However, these technological advances have introduced critical ethical concerns, particularly around data privacy, algorithmic bias, transparency, fairness, and regulatory oversight (Fundira & Mbohwa, 2025). Data privacy and confidentiality protect customers' sensitive identity data from misuse or breaches that may cause severe harm (Qureshi et al., 2024). Therefore, data ethics must be taken seriously through responsible data practices such as encryption, minimization, anonymization, consent, clear data-use policies, opt-out options, and staff training, which are recommended for safeguarding data and maintaining customer confidence.

Credit unions and community banks are similar in size because they are smaller and member-oriented institutions with three constraints for machine learning: limited data, fewer technical resources, and cooperative, trust-based governance (Agyei & Lettu, 2026). The search for efficiency in the cooperative credit sector has led to the adoption of new technology and managerial know-how. The process of granting credit is one of the central functions of a credit union; therefore, the use of instruments that support that process is desirable and may become a key factor in credit management (De Moraes Sousa & Figueiredo, 2014).

The growing adoption of machine learning (ML) technologies in financial services has significantly improved operational efficiency, fraud detection, customer personalization, and credit risk assessment. However, these benefits are accompanied by substantial ethical and privacy concerns, including algorithmic bias, opaque decision-making, data misuse, and regulatory compliance challenges (Remolina, 2022; Sargeant, 2023). For U.S. credit unions and community banks, these concerns are particularly significant due to their limited technological resources, strong community-oriented mandates, and heightened dependence on consumer trust (Agyei & Lettu, 2026). Though machine learning (ML) systems can simplify lending and banking operations, they may also unintentionally perpetuate discriminatory practices, risk client privacy, and weaken transparency in automated financial decision-making. There is still limited research explicitly looking at how data ethics and privacy issues affect smaller financial institutions like credit unions and community banks, despite growing scholarly attention to AI ethics in large financial institutions. This leaves a gap in our knowledge of how these companies could reach a compromise between the efficiency benefits of adopting machine learning and their ethical obligations, regulatory compliance, and customer trust preservation.

This review aims to use available literature on data ethics and privacy challenges in machine learning (ML)-driven financial systems, with a skewed focus on their implications for the U.S. credit unions and community banks. Extracting from recent studies addressing algorithmic bias, data privacy, transparency, and governance frameworks, the review integrates both conceptual and technical perspectives. The review seeks to identify and critically examine key ethical risks associated with ML adoption in financial services, localize existing technical and governance-based solutions and analyze how these challenges and solutions translate to the operational realities of credit unions and community banks.

2. ML-Driven Financial Systems: Core Applications and Why Ethics Matters

Before turning to the ethical dimensions, it is useful to outline the principal applications of machine learning in finance, namely credit risk assessment, fraud detection, anti-money laundering monitoring, and risk management, since these are the contexts in which ethical concerns subsequently arise (Agyei & Lettu, 2026; Xu et al., 2024).

Credit risk assessment and underwriting are foundational processes in financial services, determining the eligibility of individuals and businesses to access credit. These processes have traditionally relied on rule-based decision frameworks and standardized credit scoring models, such as Fair Isaac Corporation (FICO) credit scores and internal risk-rating systems, which use a narrow set of variables, most commonly income, employment history, and repayment records (Chieng et al., 2026; Young, 2026). While these traditional methods offer a degree of consistency and regulatory compliance, they are often limited by their static nature, inability to adapt to evolving borrower behaviors, and susceptibility to systematic bias (Chirputkar et al., 2026). Additionally, these models may not adequately serve individuals with limited or no credit histories, such as young adults, gig economy workers, or residents in underbanked regions, thereby excluding potentially creditworthy applicants (Bravo et al., 2026). In response to these limitations, the financial services industry is increasingly adopting machine learning (ML) as a transformative tool to enhance the precision, efficiency, and inclusivity of credit risk assessment and underwriting (Bravo et al., 2026; Chirputkar et al., 2026).

Machine learning enables the analysis of vast and diverse datasets ranging from transactional data and social media behavior to mobile usage and psychometric assessments to derive more accurate and dynamic credit risk profiles. Unlike traditional models, ML systems can learn from historical patterns, continuously improve over time, and detect subtle signals that may indicate creditworthiness or financial stress. This has led to a paradigm shift in how financial institutions approach risk modeling, loan origination, and portfolio management (Adewuyi et al., 2023).

Digital banking plays a vital role in the evolution of the financial industry as a source of enabling financial inclusion in times of changed logistics of financial services delivery (Awosika et al., 2024). The transformation is hinged on the democratization of banking facilities that internet banking services have brought, which have made banking easier, faster, and more convenient. Digital banking is impactful because it can improve service delivery and integrate excluded, unbanked, and underserved populations into the formal financial ecosystem. Clearly, the rapid growth of digital banking has revolutionized financial services (Oduro et al., 2025). Nevertheless, cyber fraud risk has also increased to a level that can bring about substantial financial and reputational loss for institutions and customers (Efendi et al., 2025). The major challenges to fully utilizing the incentive of digital banking are digital literacy, cybersecurity concerns, and the need for a strong regulatory framework. Machine learning can play a major role in enhancing user data security and fraud detection in order to reduce these challenges. Traditional fraud detection systems, such as predefined rules and historical data, are often not sophisticated enough to address emerging fraud types. Manual detection through traditional methods is time consuming, expensive, and inaccurate, and in the big data age, it is impractical. However, machine learning-based security enhancement provides significant benefits because these sophisticated methods can process large datasets and detect commonalities that may not be noticed by manual methods (Oduro et al., 2025).

Machine learning has also become increasingly important in anti-money laundering (AML) systems and suspicious transaction monitoring. Financial institutions process millions of transactions daily, making manual monitoring highly inefficient and prone to error. ML algorithms can identify anomalous patterns, flag unusual customer behavior, and improve real-time detection of potentially illicit transactions. Compared to rule-based AML systems, ML-driven monitoring tools can reduce false positives and improve operational efficiency while strengthening regulatory compliance (Paleti, 2024; Young, 2026). Furthermore, predictive analytics and anomaly detection models help institutions respond proactively to evolving financial crime techniques and emerging cyber threats (Shah et al., 2025).

2.1. Personalization, Trust and Risk Management

Personalization and trust are intertwined aspects of a successful business-customer relationship. Personalization enhances customer experience and engagement, while trust underpins customer confidence and loyalty. Together, they create a strong foundation for long-term customer relationships and business success (Fundira & Mbohwa, 2025). In the financial industry, digital finance is a sector that leverages new technology often known as FinTech to improve and automate the delivery and use of financial services (Fahim et al., 2023; Kanaparthi, 2024). With net banking and credit card swipes for financial transactions, digital finance had its start a long time ago. However, because of the COVID-19 pandemic and the need for people to rely solely on digital payment methods while they were isolated, digital payments increased dramatically and the stress on the entire digital banking system rose significantly (Oduro et al., 2025). Like traditional financial services, digital finance is governed by financial regulations and oversight. Compliance with regulatory requirements is crucial, and digital finance providers must adhere to the same legal and security standards (Kanaparthi, 2024).

A further application of ML in finance is operational risk management, which involves identifying risks in an establishment's financial industry that can threaten organizational capital (Xu et al., 2024; Young, 2026). Some of the risks are credit risk, which is risk associated with borrowers being unable to meet the repayment of loans; market risk, which is risk in fluctuations in market prices; operational risks, which emanate from within or outside the institution; and liquidity risk, which is risk related to the institution's ability to meet its short-term commitments (Sarioguz & Miser, 2024). Risk management is critical in an institution's capacity to absorb these shocks, protect assets, and meet ambitious and demanding legal rules (Young, 2026). As the global economy becomes more uncertain and the pace of technological and regulatory change accelerates, sound risk management practices remain critical to continuing stability and investor confidence. The use of AI and ML in risk management has the potential to produce better forecasting accuracy and timely decision-making, making it easy for institutions to prevent risks and uncertainties (Sarioguz & Miser, 2024; Xu et al., 2024).

2.2. Core Ethical Challenges in ML-Driven Financial Systems

Achieving algorithmic fairness in AI systems is a complex and multifaceted challenge. Fairness is not merely about avoiding explicit biases but ensuring that AI decisions do not disproportionately disadvantage certain groups or perpetuate societal inequalities. The definition of fairness can vary depending on the context and stakeholders involved,

making it difficult to establish universally applicable standards. Key barriers to algorithmic fairness include the inherent biases in training data, the complexity of algorithmic decision-making processes, and the trade-offs between fairness and other desirable outcomes such as accuracy and efficiency (Bhatti, 2026; Vallarino, 2025). Addressing these challenges requires a nuanced approach incorporating fairness-aware techniques during the development and deployment of AI systems. This includes adopting fairness metrics to evaluate AI models, considering the broader societal impacts of algorithmic decisions, and engaging diverse stakeholders to ensure that fairness considerations are adequately addressed (Agu et al., 2024; Singh et al., 2026).

Artificial intelligence (AI) in financial services promises efficiency and personalization but raises serious ethical issues around how sensitive data is used, who is harmed by model decisions, and whether those decisions can be understood or challenged (Fundira & Mbohwa, 2025). Privacy concerns emerge as AI systems harness vast amounts of personal data to tailor financial solutions, raising questions about data protection and user consent. Bias in AI, stemming from skewed datasets or algorithmic design, can perpetuate discrimination, affecting credit scoring, loan approvals, and investment advice. Algorithmic transparency becomes critical as the opaque nature of AI decision-making processes can obscure the rationale behind significant financial advisories or decisions, undermining trust and accountability (Qureshi et al., 2024).

The integration of artificial intelligence (AI) into financial decision-making has significantly altered credit scoring systems by introducing data-driven methodologies to assess creditworthiness. AI-driven models utilize extensive financial and nonfinancial datasets to evaluate an individual's ability to repay loans, thereby enhancing the efficiency and accessibility of credit. However, despite these advancements, ethical and security challenges remain prevalent, particularly concerning algorithmic bias and data privacy risks. The extensive collection and processing of personal financial data increases the risk of cybersecurity breaches, while algorithmic bias, a primary ethical concern in AI-driven credit scoring, can arise from various sources, including biased training data, flawed feature selection, and systemic discrimination embedded in historical financial transactions. Bircan and Özbilgin (2025) aver that research has demonstrated that AI models disproportionately disadvantage specific demographic groups, thereby perpetuating existing disparities.

Commercial use of artificial intelligence (AI) is accelerating and transforming nearly every economic, social, and political domain. AI is used to assess financial risk, diagnose medical conditions, evaluate job applicants, pilot autonomous vehicles, and score potential recidivism rates (Houser, 2019). These task-based processes are just a few well-known and widely discussed applications that demonstrate machine intelligence. What they share in common is the aim to identify patterns in data to classify people and for classifications to be statistically correlated in making predictions (Qureshi et al., 2024). Companies have been attempting to classify and label items, processes, and people for a long time. However, the modern capacities of converging foundational technologies enable analytics of the vast data required for AI (Rai, 2022; Slavina, 2025). Banks rapidly adopted these new capacities to transform their front- and back-end services (Fahim et al., 2023). The most prevalent use of AI in the financial sector is algorithmic credit scoring. The reason for its prevalence is twofold. First, the traditional statistical processes of credit granting and scoring are well suited to the correlation and classification techniques of ML (Remolina, 2022). Second, inadequate processes to analyze creditworthiness may affect repayment capacity, exposure to credit risk, inaccurate portfolio quality, and may materially affect earnings and capital. Ensuring responsible lending is essential to protect consumers from over-indebtedness and potential bankruptcy (Siby & Jha, 2025; Young, 2026). While access to credit is necessary for many consumers to afford a car, house, or daily expenses, credit has historically been inaccessible to many consumers. Discriminatory and exclusionary practices bar or price out many people from the consumer credit market. Such practices have been reinforced over time as banks rely on historical data and behaviors to assess future applications (Sargeant, 2023; Salami et al., 2025).

The emergence of ethical issues in AI is attributed to the prioritization of technological advancements over crucial components such as emotions, culture, values, and ethics (Rai, 2022). This prevailing technological mindset surrounding AI and other emerging technologies often neglects the importance of these human-oriented aspects. Consequently, a significant challenge arises when highly advanced autonomous agents engage with humans on a large scale, as they lack a comprehensive understanding and appreciation of the humane part of human beings (Rai, 2022). Understanding data privacy and safety in AI requires an awareness of how machine learning (ML) processes data. Unlike human cognition, which involves conscious reasoning, ML relies on statistical methods to detect patterns and correlations that might escape direct human scrutiny (Houser, 2019). Safety and security concerns around AI are escalating due to the interconnectedness of devices and software, all of which are vulnerable to hacking (Salami et al., 2025; Shah et al., 2025). Malicious actors can exploit AI systems integrated into critical infrastructures such as power grids, transportation networks, and healthcare facilities (Slavina, 2025). The societal impact can be profound, and the cost of developing harmful AI is often relatively low since most necessary tools are publicly available. The issue of bias in AI is a significant

ethical concern involving both societal and technical factors, particularly in data-driven systems (Bhatti, 2026; Vallarino, 2025). Bias may stem from flawed data, whether incomplete, discriminatory, or poorly structured, or from values embedded within algorithms (Bircan & Özbilgin, 2025; Salami et al., 2025). For instance, a decision might rely on biased data about specific individuals, such as incomplete datasets, or on the algorithm's internal parameters, such as selected properties. When data lacks accuracy or is mismanaged, it creates a garbage in, garbage out scenario (Houser, 2019), producing outcomes with potentially discriminatory consequences for individuals or groups (Slavina, 2025).

Algorithmic decision-making in housing finance is a rapidly growing area where machine learning (ML), artificial intelligence (AI), and big data analytics are employed to automate, enhance, and accelerate financial decisions, especially in the realm of lending and credit (Sargeant, 2023). Traditionally, lending institutions such as banks, credit unions, and mortgage lenders relied on human judgment to assess loan applications. This manual approach involved evaluating borrower characteristics, including income levels, credit history, job stability, and personal references. While this system allowed for personalized, relationship-driven decisions, it was also slow, inconsistent, and prone to human biases, which often resulted in uneven lending practices (De Moraes Sousa & Figueiredo, 2014). With the advent of digital technology and data analytics, a shift occurred toward algorithmic systems. These systems leverage complex statistical models, historical data, and real-time information to evaluate the risk associated with a borrower (Adewuyi et al., 2023; Chirputkar et al., 2026). In housing finance, this means that algorithms can automatically process large volumes of applications, analyze borrower data from multiple sources, and offer precise credit scores or risk assessments based on a wider array of factors than ever before (Bravo et al., 2026). Key elements such as financial history, transaction records, social media behavior, and psychometric data are being increasingly incorporated into the decision-making process (Adewuyi et al., 2023; Salami et al., 2025). At its core, algorithmic decision-making seeks to reduce the subjectivity inherent in human-driven processes, making the lending process more data-driven, objective, and scalable (Remolina, 2022). However, despite its many advantages, the rise of algorithmic decision-making in housing finance has raised important questions about transparency, accountability, and fairness (Qureshi et al., 2024; Kothandapani, 2025). While algorithms are typically designed to eliminate human biases, they can inadvertently perpetuate or even exacerbate these biases, especially if they are trained on historical data that reflects past inequalities in the housing market (Bircan & Özbilgin, 2025; Vallarino, 2025).

Financial technology (FinTech) has transitioned from a peripheral innovation to a core component of the United States financial system. Digital payments, algorithmic credit scoring, peer-to-peer lending, robo-advisory services, and embedded finance platforms now shape how households and firms access financial services. By 2022, FinTech firms were deeply integrated into payment infrastructure, consumer credit markets, and small-business financing, positioning them as *de facto* extensions of traditional financial intermediaries rather than mere technological disruptors (Fahim et al., 2023). This structural transformation elevates FinTech from a private innovation concern to a matter of public interest, financial stability, and national economic resilience. In the United States, FinTech innovation has delivered tangible benefits, including reduced transaction costs, expanded financial inclusion, and improved service efficiency. Digital wallets and mobile payment systems have enhanced access for underbanked populations, while data-driven lending models have lowered entry barriers for consumers and small enterprises historically excluded from conventional credit markets (U.S. Government Accountability Office, 2025). At the same time, the rapid scaling of FinTech has introduced new forms of systemic risk, regulatory fragmentation, and consumer vulnerability. Unlike traditional banks, many FinTech firms operate across jurisdictional and institutional boundaries, creating gaps in oversight that challenge existing regulatory architectures (Fahim et al., 2023).

Siby and Jha (2025) further extend this discussion by arguing that retail credit default risk models cannot be evaluated only by predictive accuracy. Since default predictions have a direct impact on loan price, client dignity, collection strategies, and credit availability, their position is crucial. When training data represents historical exclusion, income instability, or unequal access to formal banking, machine learning models can imitate hidden disparities in retail lending, but they may also improve portfolio quality by spotting early warning signals (Sargeant, 2023; Salami et al., 2025). This presents a practical ethical dilemma for credit unions and community banks since they have to carefully control a default risk while also providing services to members and communities that larger commercial banks would not adequately serve (Agyei & Lettu, 2026). Therefore, the ethical use of ML in retail credit requires a balance between risk control, explainability, proportionality and human review (Remolina, 2022; Young, 2026).

3. Implications for U.S. Credit Unions and Community Banks

The implications of data ethics and privacy in ML-driven financial systems are especially significant for U.S. credit unions and community banks because these institutions operate under a unique framework of community trust, member service and regulatory responsibility (Agyei & Lettu, 2026). Smaller banks may rely significantly on external vendors for credit scoring, fraud detection, customer analytics, and digital banking services, in contrast to larger banks with

sizable technical teams and sophisticated model governance divisions (U.S. Government Accountability Office, 2025). Although the ethical risk does not go completely when a model is outsourced, this dependence presents a governance difficulty (Fundira & Mbohwa, 2025). If an automated tool produces biased lending outcomes, exposes sensitive customer data or gives explanations that staff cannot reasonably understand, the reputational and compliance burden may still fall on the institution that deploys the system.

AI use in banks and credit unions offers both operational advantages and supervisory problems, according to recent oversight talks (U.S. Government Accountability Office, 2025). Financial institutions employ AI in areas like credit decisions, customer service, and managing risks, according to the U.S. Government Accountability Office. Additionally, it stated that biased lending judgments, privacy issues, issues with data quality, and vulnerabilities related to cybersecurity could be introduced by AI. The audit also noted that the National Credit Union Administration lacks direct jurisdiction to investigate certain technological service providers utilized by credit unions and has limited model risk recommendations linked to AI (U.S. Government Accountability Office, 2025). This is important because credit unions increasingly rely on external vendors for AI-enabled services, yet vendor opacity may limit internal accountability and weaken examination readiness. (Young, 2026).

For community banks, the challenge is similar but also shaped by the economics of local relationship banking. According to De Moraes Sousa and Figueiredo (2014), community banks are frequently reliant on comprehensive information of local borrowers, small enterprises, and household financial behavior. By enhancing monitoring, decreasing manual review, and spotting early indicators of financial instability, machine learning systems can assist these institutions (Agyei & Lettu, 2026). However, by overemphasizing measurable variables and underrepresenting contextual knowledge, models that are adopted without adequate oversight may undermine relationship-based judgment (Sargeant, 2023). This is particularly important in underprivileged or rural locations where borrowers may have unconventional financial profiles, inconsistent income, or insufficient credit histories (Bravo et al., 2026). In such cases, ML should function as a decision support tool rather than a substitute for accountable human judgment (Remolina, 2022).

3.1. Privacy-Preserving and Explainable ML Approaches

Financial companies can profit from predictive analytics without necessarily disclosing client data thanks to privacy-preserving machine learning algorithms (Fundira & Mbohwa, 2025). Federated learning is especially pertinent because it allows multiple institutions to train models collaboratively while maintaining raw customer data within each institution. According to Awosika et al. (2024), institutions can maintain secrecy while yet producing interpretable model outputs by combining explainable AI alongside federated learning in financial fraud detection. Since credit unions and community banks frequently have smaller datasets and may profit from shared learning while upholding privacy standards and member trust, this strategy is appropriate for these organizations (Agyei & Lettu, 2026; Aljunaid et al., 2025).

Explainable AI is also central to ethical deployment because financial decisions require reasons (Qureshi et al., 2024). Appropriate explanations should be provided to customers who are impacted by denied loans, higher interest rates, account freezes, or fraud alerts (Remolina, 2022). In order to validate a warning, spot model problems, and convey choices in a way that adheres to fair lending standards, internal staff members also require explanations (Young, 2026). However, explainability ought not to be constrained to a technical output because a model explanation needs to be comprehensible to the target audience, which might be a client, loan officer, compliance officer, or examiner (Awosika et al., 2024). As a result, institutions should incorporate staff training, model documentation, plain-language decision notices, and technical explainability tools (National Institute of Standards and Technology, 2023).

Other privacy-enhancing practices remain essential because AI-enabled financial services depend on confidential customer information (Houser, 2019). Data minimization reduces the quantity of client data utilized for model operation and training (Fundira & Mbohwa, 2025). When datasets are utilized for testing or analytics, anonymization and pseudonymization can mitigate vulnerability (Slavina, 2025). Encryption protects data in storage and transmission, while access controls restrict internal misuse and audit logs help trace unauthorized access or model changes (Fundira & Mbohwa, 2025). Clear data retention guidelines and regular evaluations of whether the data in the model remains required, accurate, and compliant with the law should support these controls (National Institute of Standards and Technology, 2023). In this regard, privacy must be treated as a continuous governance practice rather than a one-time compliance activity (Houser, 2019; Slavina, 2025).

3.2. Governance Frameworks for Responsible Adoption

Governance over the entire model lifecycle is necessary for responsible ML adoption (Young, 2026). The govern, map, measure, and manage features of the National Institute of Standards and Technology AI Risk Management Framework offer an effective framework (National Institute of Standards and Technology, 2023). The ethical issues addressed in financial machine learning literature are strongly aligned with its emphasis on legitimate and trustworthy systems, safety, security, accountability, transparency, explainability, privacy enhancement, and fairness (Qureshi et al., 2024). This framework can be customized to create beneficial controls for smaller financial institutions, including model inventory, documented model purpose, risk classification, validation testing, bias monitoring, vendor due diligence, incident response, and board-level reporting (U.S. Government Accountability Office, 2025; Young, 2026).

A practical governance model for credit unions and community banks should commence before procurement because model risk should be evaluated before systems are obtained or implemented (National Institute of Standards and Technology, 2023). Institutions should identify the data needed, clarify the business problem, ascertain the ethical and legal restrictions, and establish whether machine learning is required (Young, 2026). Vendors should be obliged to provide information on the model's objective, training data characteristics, validation evidence, security controls, explainability features, limitations, and protocols for dealing with unfavorable outcomes during the procurement process (U.S. Government Accountability Office, 2025). Institutions should monitor model drift, test for unequal consequences, set thresholds for human review, and save records for examiners during deployment (Remolina, 2022; National Institute of Standards and Technology, 2023). After deployment, models should be periodically reviewed to determine whether they remain accurate, fair and consistent with the institution's mission (Rai, 2022; Young, 2026).

Ethical auditing should be a component of the governance process. Rai (2022) highlights the significance of ethical audits in AI because automated systems can affect human welfare in ways that cannot be assessed by technical performance metrics alone. Also, as stated by Rai (2022), an ethical audit in the financial services industry should aim at whether a model respects privacy, yields fair results, promotes client knowledge, and permits meaningful questionability. Customers must have a fair chance to challenge choices that impact their capacity to obtain financing, which makes contestability particularly crucial (Remolina, 2022). This is in accordance with cooperative principles for credit unions since member-oriented governance promotes accountability to the persons the organization serves (Agyei & Lettu, 2026).

4. Challenges and Future Direction

The future of ML-driven financial systems will be shaped by the ability of institutions to combine innovation with accountability. The creation of standardized and lightweight governance systems for smaller financial institutions is one important avenue. According to the U.S. Government Accountability Office (2025), many ethical AI frameworks presume a level of technical capacity that may be present in major financial institutions but not in local credit unions and community banks. Therefore, scalable governance templates, streamlined bias testing techniques, vendor evaluation checklists, and shared compliance utilities that are affordable should be the main focus of future research. Such tools would help smaller institutions participate in responsible innovation rather than being excluded from advanced analytics due to resource limitations.

Another future direction is the strengthening of privacy-preserving collaboration. Community banks and credit unions often lack the amount of data required to independently train reliable models. Institutions are potentially able to gain from collective intelligence without centralizing sensitive consumer data due to federated learning, secure multiparty computation, and privacy-enhancing analytics. These technologies, however, also necessitate for cybersecurity protections, uniform data standards, technical maturity, and explicit accountability mechanisms. Without these prerequisites, privacy-preserving methods might provide users a false sense of security while disregarding problems related to participation bias, model quality, and governance accountability.

Regulatory development will additionally impact future practice because existing U.S. financial laws already address fair lending, consumer protection, privacy, model risk and cybersecurity. Yet when sophisticated and adaptive systems make decisions, AI raises new concerns regarding how these responsibilities should be understood. Regulators may increasingly expect institutions to prove that automated decisions are explainable, documented, monitored and subject to human oversight. This implies that in addition to technology acquisition, future preparedness for credit unions and community banks will additionally be contingent on staff training, governance maturity, and the capacity to provide evidence during audits and examinations.

The trade-off between efficiency, fairness, and precision poses another challenge. Making decisions using algorithms frequently entails conflicts between conflicting goals. If an extremely accurate credit scoring model learns from historically inconsistent patterns, it may nevertheless yield unequal results. Certain prediction performance metrics may be lowered by a model intended to enhance fairness. In the absence of a significant appeal mechanism, an efficient automated process may diminish client voice. Therefore, the issue of ethics is to make trade-offs readily apparent, justified, and consistent with institutional principles and legal standards rather than entirely eliminating them.

Finally, future research should examine customer perception of ML in community-based financial institutions since trust is not only a technical or legal issue but also a relational one. When members trust that the organization is acting in their best interests, preserving their data, and providing them with equal opportunities to comprehend and contest decisions, they may accept automated tools. Thus, empirical research ought to inquire into how consumers of community banks and credit unions regard data sharing, automated lending, fraud monitoring, and personalized offers. This would offer useful proof for creating machine learning systems that support community trust and operational efficacy.

5. Conclusion

Machine learning has become integral to modern financial systems, supporting credit risk assessment, fraud detection, anti-money laundering monitoring, personalization, and operational risk management. Yet the same capabilities that make it valuable also raise serious ethical and privacy concerns, including algorithmic bias, opaque decision-making, excessive data collection, cybersecurity exposure, and weak accountability. These concerns are especially significant for U.S. credit unions and community banks, whose institutional identities rest on trust, local service, and member welfare. This study has shown that responsible adoption requires more than technical proficiency: it demands data minimization, explainability, fairness testing, ethical auditing, vendor accountability, and continuous monitoring, supported by frameworks such as the NIST AI Risk Management Framework and by privacy-preserving technologies like explainable AI and federated learning embedded within strong governance. When implemented in this way, ML-driven systems can enhance the efficiency, resilience, and inclusivity of community-based institutions while safeguarding privacy, fairness, accountability, and human dignity.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

- [1] Adewuyi, A., Nwangele, C. R., Oladuji, T. J., & Akintobi, A. O. (2023). Advances in machine learning for credit risk and underwriting automation: Emerging trends in financial services. *International Journal of Advanced Multidisciplinary Research and Studies*, 3(6), 1860–1877.
- [2] Agu, E. E., Abhulimen, A. O., Obiki-Osafiele, A. N., Osundare, O. S., Adeniran, I. A., & Efunniyi, C. P. (2024). Discussing ethical considerations and solutions for ensuring fairness in AI-driven financial services. *International Journal of Frontier Research in Science*, 3(2), 1–9.
- [3] Agyei, E., & Lettu, E. A. (2026). Machine learning in credit unions: A review of predictive analytics for fraud detection and loan risk assessment. *EPRA International Journal of Research & Development*. <https://doi.org/10.36713/epra26818>
- [4] Awosika, T., Shukla, R., & Pranggono, B. (2024). Transparency and privacy: The role of explainable AI and federated learning in financial fraud detection. *IEEE Access*, 12, 64551–64560. <https://doi.org/10.1109/access.2024.3394528>
- [5] Bhatti, A. (2026). *Algorithmic fairness in artificial intelligence systems*.
- [6] Bircan, T., & Özbilgin, M. F. (2025). Unmasking inequalities of the code: Disentangling the nexus of AI and inequality. *Technological Forecasting and Social Change*, 211, 123925.
- [7] Bravo, C., Maldonado, S., & Oskarsdottir, M. (2026). *Deep learning in banking: Integrating artificial intelligence for next-generation financial services*. Springer.

- [8] Chieng, T. S., Teck, T. S., & Geok, L. S. (2026). The transformative role of artificial intelligence in the financial sector: A critical review of applications and challenges. *Advances in Decision Sciences*.
- [9] Chirputkar, A., Ashok, P., & Deshmukh, R. (2026). Technological disruption in credit markets through digital lending networks. In *Digital lending networks*. IGI Global.
- [10] De Moraes Sousa, M., & Figueiredo, R. (2014). Credit analysis using data mining: Application in the case of a credit union. *JISTEM Journal of Information Systems and Technology Management*, 11, 379–396. <https://doi.org/10.4301/s1807-17752014000200009>
- [11] Efendi, M. N., Adinugroho, M., & Khomairoh, S. (2025). Evolution and patterns of crime in banking systems: From traditional fraud to cybercrime. *AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism*, 3(2), 168–196.
- [12] Fahim, A., Ibrahim, M., Pritty, A. A., & Tania, T. A. (2023). Algorithmic accountability in U.S. consumer FinTech: Governance mechanisms for credit risk, fair lending, and financial stability. *Journal of Economics, Finance and Accounting Studies*, 5(4), 80–93.
- [13] Fundira, M., & Mbohwa, C. (2025). AI ethics in banking services: A systematic and bibliometric review of regulatory and consumer perspectives. *Discover Artificial Intelligence*, 5. <https://doi.org/10.1007/s44163-025-00432-4>
- [14] Houser, K. A. (2019). *Artificial intelligence and data ethics*.
- [15] Kanaparthi, V. (2024). AI-based personalization and trust in digital finance. *arXiv preprint arXiv:2401.15700*.
- [16] Kothandapani, H. P. (2025). Social implications of algorithmic decision-making in housing finance: Examining the broader social impacts of deploying machine learning in lending decisions, including potential disparities and community effects. *Journal of Knowledge Learning and Science Technology*, 4(1), 78–97.
- [17] Oduro, D. A., Okolo, J. N., Bello, A. D., Ajibade, A. T., Fatomi, A. M., Oyekola, T. S., & Owoo-Adebayo, S. F. (2025). AI-powered fraud detection in digital banking: Enhancing security through machine learning. *International Journal of Science and Research Archive*, 14(3), 1412–1420.
- [18] Paleti, R. (2024). *Machine learning approaches for anti-money laundering and suspicious transaction monitoring*.
- [19] Qureshi, N. I., Choudhuri, S. S., Nagamani, Y., Varma, R. A., & Shah, R. (2024). Ethical considerations of AI in financial services: Privacy, bias, and algorithmic transparency. In *2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS)* (Vol. 1, pp. 1–6). IEEE.
- [20] Rai, N. (2022). Why ethical audit matters in artificial intelligence? *AI and Ethics*, 2(1), 209–218.
- [21] Remolina, N. (2022). The role of financial regulators in the governance of algorithmic credit scoring. *SMU Centre for AI & Data Governance Research Paper*, 2.
- [22] Salami, I. A., Adesokan-Imran, T. O., Tiwo, O. J., Metibemu, O. C., Olutimehin, A. T., & Olaniyi, O. O. (2025). Addressing bias and data privacy concerns in AI-driven credit scoring systems through cybersecurity risk assessment. *Asian Journal of Research in Computer Science*, 18(4), 59–82.
- [23] Sargeant, H. (2023). Algorithmic decision-making in financial services: Economic and normative outcomes in consumer credit. *AI and Ethics*, 3(4), 1295–1311.
- [24] Sarioguz, O., & Miser, E. (2024). Data-driven decision-making: Transforming management in the information age. *International Research Journal of Modernization in Engineering Technology and Science*. <https://doi.org/10.56726/irjmets49577>
- [25] Sarioguz, O., & Miser, E. (2024). Integrating AI in financial risk management: Evaluating the effects of machine learning algorithms on predictive accuracy and regulatory compliance. *No. November*.
- [26] Shah, S. A. H., Husain, S., & Quadri, H. M. A. (2025). The impact of cybercrime on digital financial systems: Challenges and preventive strategies.
- [27] Siby, A., & Jha, B. (2025). Managing retail credit default risk using artificial intelligence and machine learning: Ethical considerations and challenges. In *International Conference on Information and Communication Technology for Intelligent Systems* (pp. 351–359). Springer Nature Singapore.
- [28] Singh, A., Jain, A., & Biabale, S. E. (2022). Financial fraud detection approach based on firefly optimization algorithm and support vector machine. *Applied Computational Intelligence and Soft Computing*, 2022(1), 1468015.

- [29] Singh, A., Jain, A., & Biabie, S. E. (2026). *Algorithmic fairness and stakeholder engagement in AI systems*.
- [30] Slavina, Z. (2025). Toward ethical AI: Addressing bias, privacy, and accountability in data-driven systems. *Świat Idei i Polityki*, 24(1), 65–81.
- [31] Surana, P. (2024). Credit risk assessment and fraud detection in financial transactions using machine learning. *Journal of Electrical Systems*. <https://doi.org/10.52783/jes.1807>
- [32] Vallarino, M. (2025). *Fairness, accuracy, and efficiency trade-offs in algorithmic decision-making*.
- [33] Xu, H., Niu, K., Lu, T., & Li, S. (2024). Leveraging artificial intelligence for enhanced risk management in financial services: Current applications and future prospects. *Engineering Science & Technology Journal*. <https://doi.org/10.51594/estj.v5i8.1363>
- [34] Young, R. G. (2026). *AI and ML governance in financial services: Balancing innovation, risk, and equity*. Routledge.
- [35] U.S. Government Accountability Office. (2025). *Artificial intelligence: Use and oversight in financial services* (GAO-25-107197).
- [36] National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1). U.S. Department of Commerce.
- [37] Aljunaid, S. K., Almheiri, S. J., Dawood, H., & Khan, M. A. (2025). Secure and transparent banking: Explainable AI-driven federated learning model for financial fraud detection. *Journal of Risk and Financial Management*, 18(4), 179.