Legal And Regulatory Compliance in Software Development for Financial Systems.

Chukwu Nelson Okwudili[1], Chukwudi Jeremiah Paul[2], Ifesinachi Ignatius Nwankwo[3]
Chinoso Job[4], Onwe, Festus Chijioke[5]
[5]*Corresponding Author, Information Technology Department,*
University of Port Harcourt, Rivers State, Nigeria.
[12,3,4,] *University of Greater Manchester, United Kingdom*

***Abstract*—In the age of rapid technological growth, the financial services firm has undergone experienced a profound change by the integration of artificial intelligence, block chain, big data analytics and cloud computing. While these innovations render greater efficiency, hyper personalized services, and real-time transactions, they also expose the financial software to new legal, ethical, and regulatory issues. This report critically investigates the intersection of software engineering, regulatory frameworks, and professional ethics within the domain of digital finance systems. It elaborates how modern software design must account for compliance with global standards such as the general Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI-DSS), Sarbaness Oxley Act (SOX), and Payment Services Directive 2 (PSD2). It first gives contextual insights on the 2008 financial crisis which revealed the significant gaps in transparency and resilience, bidding the need for more robust legal and ethical foundations in digital finances with a critical analysis that identifies key challenges in identity theft, algorithmic bias, ethical failures and gaps in realtime compliance. It laid emphasis on the pressing need for secure by-design development, explainable AI models, and traceable transactions logs. Moreover, it appraises the social and sustainability concerns linked with digital finance such financial exclusion, environmental impact from blockchain infrastructure, and erosion of public trust following data breaches. In other to address these concerns, the report outlined a various proposed solution and professional practices, and these include the implementation of a secure Software Development Lifecycle (SSDLC), the use of legal-as-code tools within CI/CD, adoption of ISO/IEC 27001 for information security governance, and the embedding of professional ethics from bodies like ACM, IEE and ISO.**

I. INTRODUCTION

Rapid evolving digital age in financial systems today have been supportive ranging from Banking software, trading platforms, and digital wallet have become increasing complex, data driven and interconnected. Transformation of financial services in the environment highlights a remarkable shift where technologies like AI, blockchain, big data analytics and cloud computing have changed how financial services operate and systems now offer hyper-personalized, automated and real-time services though they face new regulatory, legal and ethical risks (Heckel and Waldenberger, 2022).

The overall technological disruption also entailed changes brought about by issues that occurred in 2008 fiscal crisis, which disclosed the need for transparency and resilience in financial institutions (Hall, 2020). Moreover, with the help of open banking APIs, machine learning-based trading and platforms the demand for compliance with robust frameworks like GDPR, PCI-DSS, SOX and PSD2. These great wave in finance system allow third party services to access financial data securely and improve user engagement. However, they also need strict obedience to data protection, transaction auditing, and user consent principles. With the sudden rise of AI in credit scoring and customer profiling stress the importance of building ethical systems that prevent algorithmic bias and discrimination (Arnaboldi et al., 2022).The introduction of AI into financial sector is not only a technological breakthrough but also boasted the economic ecosystem thereby regulating everything from credit scoring to customer engagement, automated risk assessments, fraud detection and tailored financial advice, while blockchain enhances transaction transparency and security that assisted in elevating customer experiences and improved operational efficiency across the sector but the risk of bias, lack of transparency and vulnerabilities in security stress the need of embedding legal and ethical safeguards from early stages to software development(Sayles, 2024) as a result of introduction of new legal, regulatory and ethical vulnerabilities that all finance institutions must adhere to strictly. With the growth of financial technologies in our environment that have become more embedded in daily life, it is essential that legal safeguards, ethical design principles and regulatory compliance are prioritized from the earliest stage of software development life cycle to the deployment stage. If the financial software engineers fail to follow these principles, the trust of the customer will be imperiled, and this also exposes organization to financial and reputational risks in an increasingly regulated economy.

II. RELATED LITERATURE

2.1 Critical Analysis of Issues:

One of the major challenges faced by the banking industry today is identity theft, ranging from debit cards, credits and the virtual card that enables the users to make transactions, though there have been some legal and regulatory rules that mitigate some of the challenges posed to both users, the financial bodies and the system engineers. But the rhetorical question that been left unanswered is to these entities follow the legal regulatory activities that has been stipulated or not.

2.2 Legal and Regulatory requirements:

The PCI-DSS (Payment Card Industry Data security standard) for payment software paid the ultimate price of securing users' data from threats (frauds, ransomware, phishing attacks) and confidentiality in companies since its introduction in December 2004 by major credit card companies (visa, MasterCard, American Express and JCB). Ever since it has been launched it served its purpose very well and this have boosted the trust among users with different financial bodies because the sudden rise of electronic transactions among individuals in European countries. Considering the myths of PCI-DSS stipulated by the payment card industry security standards council that helps to create honesty and transparency during the implementation of any electronic system for entities (i.e. merchant and operators), the software engineer has been privileged to build and maintain a secure network , protect card holders data , maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks and finally maintain an information of security policy(Williams, 2023). Moreover, in other to successfully apply this compliance stipulated as either a software engineer, network administrator or worker in a firm, you are obliged to validate the company's compliance either annually or quarterly, preferably onsite PCI assessments can be done by a qualified security Assessor (QSA) or internal Security

Assessor (ISA) which will be submitted as SAQ that shows the obtained signature on the document by the officer of the company. This compliance is being enforced to prove your transparency. Security in financial system should be well designed to prevent data breaches like the case of the card system breach in 2005 (Holtfreter and Harrington, 2015), the ATM machine network should be well secured by the service provider to ensure that that the machine is processing, storing and transmitting card holder data to the expected entity (ATM operators). Since the introduction of Ai in financial sector, the need to ensure algorithm transparency and user consent issues that are often neglected in deployment can be addressed as stipulated GDPR guidelines provided in different countries, most countries like Germany, US, Russia, prefer to host their data within the country in other to prevent giving out much information to other countries about user personal data. However, regulators have adopted Sup Tech (supervisory Technology) that helps to monitor financial systems suing AI-based tools and this has showed greater expectations on institutions to implement real time auditing, traceability and legal accountability into the software architecture.

2.3 Ethical Issues:

Since integration of AI in finance software ethical issues has been noted in areas like loan approvals, credits scoring and investment advice and this posed a concern and algorithm discrimination because of biases embedded in training datasets, flawed model logic that penalise vulnerable groups unfairly. Most cases of this unfair penalty experienced indifferent finance institutions like that of Tinkoff Bank in Russia, where a user was disqualified because of opaque credit algorithm, this highlights the ethical need for explainable AI and transparent model logic. Moreover, most fintech interface like use dark patterns deceptive Ui design (hidden fees, or default opt ins) to influence user decisions and this breaches ethical and legal standard. Software engineers that have been employed by most financial company face challenges in balancing innovation with user autonomy mostly in algorithmic trading where systems operate at the speed beyond human oversight. The need to embed ethical guidelines from ACM, IEEE and ISO/IEC 29100 inti design and testing phases can mitigate these risks (Pontes et al., 2021).

III. SOCIAL AND SUSTAINABILITY CONCERNS

Advanced technologies like AI, blockchain and big data in finance systems show not only legal and ethical issues but also the social and sustainability implications. The rapid digitalization in financial institutions in recent years tends to tend to balance the gap existing from technological progress with social equity, environmental responsibility and systemic resilience and the issues with this will be addressed under the following criteria:

3.1 Financial Inclusion and Digital Exclusion:

The fascinating facts of fintech and AI-based financial software is improved financial inclusion, and it enable the firm to reach underserved and unbanked populations using mobile banking, digital wallets, and micro-lending algorithms, and this allowed people without traditional credit histories to have access to essential services (Aziz and Naima, 2021).

Nevertheless, digital shift can create exclusion for those that do not have access to the internet, digital literacy, or computing devices (smartphones, pc, and notebooks). Finance application fails to consider marginalized communities whose data are diminished in training thereby leading to inaccessible outcome.

3.2 Algorithmic Bias and Social Justice

Wrong financial decision making is an outcome of algorithmic bias, and this pose a serious threat to fairness and equality. It has been prevalent in Ai powered credit scoring and investment platforms where biased training data have cause system injustice. Studies from most scholars revealed that bias in financial software could appear neutral but often reproduces existing social inequalities, mostly against women, ethnic minorities or low- income groups. The Tinkoff bank in Russia demonstrate how lack of explainability led to mistrust, reputational damage and social harm because of controversial algorithmic decision made (Wajid, 2017).

3.3 Environmental Sustainability and Technology Footprint

In other for financial firms to adopt green IT policies (server virtualization, energy-efficient data centers and carbon offset strategies) there is need to investigate the energy consumption associated with high frequency trading severs, cloud storage for big data and blockchain` systems that is very vital to economic ecosystem. Studies have showed that bitcoin mining consumes more electricity annually in United States of America than other countries. This offset the efficiency of digital financial services (paperless banking, remote transactions) that are evident. Most researchers argued that sustainability in financial systems must consider not just service delivered but the infrastructure that supports them.

3.4 Trust, Transparency and Social License

Interdependence of social sustainability on clear communication, accessible redress mechanisms and human oversight in automated decision making. For this to be feasible, the concept of social license to operate must be in place to help the firm earn and maintain public trust while using the software systems for finance. Although failure due to poor compliance, security breaches have eroded user confidence and public good will. The case of Equifax data breach that affected over 140 million individuals both economically and emotionally due to technical failures (Daswani and Elbayadi, 2021). As a software engineer in a fintech, it is vital to ensure transparency in system design, decision making and data usage in other to uphold societal trust.

3.5 Ethical Sustainability and Long-Term Governance

In a quest to bridge the gap between compliance and conscience ensuring that innovation does not come at the expense of social integrity. Technical fixes, true social responsibility in software design requires embedding ethical foresight and long-term governance. The ethical sustainability enhances developing systems that not only comply with current law but also anticipate the future impacts on the society. Fostering human-centric design, value-sensitive development, and stakeholder inclusion mostly when the applications are affecting creditworthiness, wealth distribution and economic mobility. The need for governance framework to enable continuous improvement, participatory design and inclusive policy shaping is vital.

IV. PROPOSED SOLUTION AND PROFESSIONAL PRACTICES

The challenges of legal and regulatory practices surrounding financial software development require not only compliance but initiative-taking integration of professional practices during the development lifecycle. In other to increase the data-driven, distributed, and autonomous, financial software, as the system grow, software engineers must set security standards, transparency, and accountability by design. However, critical solution can address these demands with practical approaches and internationally recognized standards.

4.1 Secure Software Development lifecycle (SSDLC) with Compliance Checks

Software design is not perfect without security; regulatory software design has been the secure software development lifecycle (SSDLC). Apart from SDLC approaches, the SDDLC include security, privacy and compliance validation ate every stage from planning to maintenance. This reduces vulnerabilities and illegal liabilities (Stella, 2021).

In a financial system, compliance should protect industry specific framework like PCI-DSS for payment systems, SOX for audit trails, and GDPR for data protection. However, integrating threat modelling, security requirements analysis and regulatory validation at design stage helps software are built based on the laws and ethical norms from the outset.

4.2 Integration Legal as Code Tools into CI/CD Pipelines

Handling complexity of financial regulation has led to the emergence of legal as code solution that provide automated rules to turn legal provisions into machine-readable logic. Using continuous Integration and continuous deployment (CI/CD) pipelines, firms can perform automatic compliance checks each time is pushed or deployed. For instance, conditions defined by the payment service directive 2 (PSD2) are encoded into smart contract logic, automated scripts that test for secure API exposure or consent handling tends to create a fail- fast compliance model where violation are detected before the code is released.

4.3 Building Auditability, Traceability and Logging Mechanisms

For finance systems to include built-in audit trails, traceability logs and version histories which are immutable and tamper-evident, these mechanisms are essential not just for compliance with regulations like SOX and GDPR but also for operational resilience and public trust. financial technologies like blockchain offer cryptographic integrity for transaction histories, secure logging frameworks that can track internal access on sensitive data. Additionally, storing logs in secure, access-controlled environment allows regulators and auditors to verify system behavior when needed.

4.4 Applying ISO/IEC 27001 for Secure Software Governance

Best practice standards for establishing, maintaining and improving an information security management system (SMS) have been stipulated by the ISO/IEC 27001.In view of financial software, this lay out a structured approach to managing Security risks (risk assessment, control selection, staff training and incident response). Therefore, implementing ISO/IEC 27001 helps organization demonstrate compliance with data protection laws, manage risks effectively, and establish internal accountability structures. However, it supports continues improvement audits and security metrics tracking that ensure long-term resilience (Wong, 2020).

4.5 Legal Collaboration during Architecture Planning

Frequently, legal experts are led into the development process post-deployment, when it is very costly to reconstruct compliance. This elaborates why cross functional collaboration between legal professionals, architects and software engineers during the design and architecture planning phrase which is very vital. Hence, setting legal and ethical foresight into software architecture enrich the creation of AI systems that are not only lawful but socially beneficial. This shows that early collaboration ensures legal constraints such as data residency, consent protocols, reporting duties are reflected in the technical architecture from the beginning.

4.6 Embedding Codes of Ethics: ACM, IEE and ISO 29100

It very evident to say that legal compliance alone is insufficient in ethically sensitive sectors like finance. Both developers, workers in the firm and end users must follow professional codes of ethics that relates to computing and the major organizations in charge of these are:

A. The ACM code of ethics that promotes responsibility, privacy and fairness in computing.
B. The IEEE ethically Aligned Design that guides responsible AI development across transparency, accountability, and human values.
C. The ISO/IEC 29100 Privacy Framework that set principles for personal data protection including consent, purpose specification and minimization.

Emphasis on the codes of ethics serve as internal moral compasses, enabling software professionals to recognize, question and avoid unethical practices (Walker, 2023).

V. CONCLUSION

Software development for financial systems appears at the intersection of law, ethics, and technology. Moreover, a persistent challenge noticed across the industry is the habit for organization to manage legal and regulatory compliance as a review, addressed only during post-deployment audits or in reaction to breaches. This part approach is not only ineffective but also seriously unsustainable in today's rapid evolving digital finance landscape. To establish long-term resilience and regulatory fitness, compliance must be replanned as design principle rather than a reactive checklist. With legal requirements, ethical considerations, and privacy expectations are embedded into the software architecture, it makes it possible to build systems that are not only functional and secure but also socially responsible and robust, as this aligns the concept of privacy by design and security by design that have been endorsed by global data protection authorizes like the Uk information Commissioner's Office (ICO). A key recommendation is to strengthen the early stage of legal and compliance expertise at the software architecture planning phase rather than siloing legal reviews at until final deployment. The team of software engineers need to collaborate with legal advisors from the conceptual design through prototyping. This method enables informed decision around the authority constraints, consent models, audit mechanisms and data handling strategies.

Additionally, addressing compliance cannot rely solely on governance structure, management frameworks but it should extend to the professional competencies of developers and engineers. The increasing need for continuous education and legal literacy training for software practitioners working in firms has to address the issues faced by developers which they must understand not just how to write secure code, but also how their design decisions may intersect with legal obligations like GDPR, PSD2 and other financial regulations.

However, embedding regulatory awareness into engineering culture builds both accountability and innovation capacity. Lastly, the shift concerning legally and ethically sustainable financial systems starts with an initiative-taking culture change. Compliance needs to be integrated at every layer from the strategy and architecture to coding and deployment that shows the integrative collaboration, professional development and values-based engineering.

REFERENCES

[1] M. Arnaboldi, H. de Bruijn, I. Steccolini, and H. Van der Voort, "On humans, algorithms and data," Qual. Res. Account. Manag., vol. 19, no. 3, pp. 241–254, 2022.
[2] A. Aziz and U. Naima, "Rethinking digital financial inclusion: Evidence from Bangladesh," Technol. Soc., vol. 64, p. 101509, 2021.
[3] N. Daswani and M. Elbayadi, Big Breaches:

Cybersecurity Lessons for Everyone, 1st ed. Berkeley, CA, USA: Apress, 2021.

[4] A. S. George, "Finance 4.0: The Transformation of Financial Services in the Digital Age," Partners Universal Innovat. Res. Publ., vol. 2, no. 3, pp. 104–125, 2024.

[5] A. Hall, Útrásarvíkingar: The Literature of the Icelandic Financial Crisis (2008–2014). Brooklyn, NY, USA: Punctum Books, 2020.

[6] M. Heckel and F. Waldenberger, The Future of Financial Systems in the Digital Age: Perspectives from Europe and Japan, 1st ed. Singapore: Springer Nature, 2022.

[7] R. E. Holtfreter and A. Harrington, "Data breach trends in the United States," J. Financ. Crime, vol. 22, no. 2, pp. 242–260, 2015.

[8] G. S. Pontes, G. Allocio, G. Miranda, R. L. P. Marques, and V. Dosne, "Artificial Intelligence: Implications in the Customer Journey," Master's thesis, ProQuest Dissertations & Theses, 2021.

[9] J. Sayles, Principles of AI Governance and Model Risk Management: Master the Techniques for Ethical and Transparent AI Systems, 1st ed. Berkeley, CA, USA: Apress, 2024.

[10] J. Stella, "How to secure cloud infrastructure across the development lifecycle," InfoWorld, 2021. [Online]. Available: https://go.exlibris.link/p3DkClP0

[11] D. Wajid, "Moody's upgrades Russia's Tinkoff Bank," SNL Eur. Financ. Daily, 2017.

[12] P. G. A. Walker, "Technology law, rights and ethics one choice, one future," Int. Lawyer, vol. 56, no. 1, pp. 1–89, 2023.

[13] B. R. Williams, PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance, 5th ed. Boca Raton, FL, USA: CRC Press, 2023.

[14] B. Wong, "The journalism exception in UK data protection law," J. Media Law, vol. 12, no. 2, pp. 216–236, 2020.