Regulating fintech for financial stability in Nigeria: balancing cybersecurity risks and financial inclusion

Oluwasola Oni,[1]Abayomi Oluwaseun Japinye[2], Gilbert Deinde Ifarajim[3] & Oluwaseun Favour Olubowale[4]

Abstract

The growing reliance on financial technology (FinTech) firms in Nigeria has step up concerns surrounding cybersecurity vulnerabilities, the effectiveness of regulatory interventions, levels of consumer confidence, systemic resilience, and extent of financial inclusion. This has initiated the need to investigate how these variables interact, in order to understand their interdependencies, mitigate the frequency and impact of cyberattacks, and safeguard consumer trust in digital financial services. A total of 248 structured responses were obtained through a google form survey administered to three distinct groups FinTech users, regulatory bodies, and financial industry experts. Using a stratified random sampling, samples were drawn from three major cities in Nigeria, 84 respondents from Abuja, 91 respondents from Lagos and 73 respondents Port Harcourt. The empirical analysis was carried out employing the Structural Equation Modelling (SEM). To analyse the fundamental constructs of cybersecurity threats, regulatory measures, consumer confidence, systemic resilience, and financial inclusion are treated as the latent variables. Findings revealed that cybersecurity threats significantly affect regulatory measures, stressing the fact that heightened vulnerabilities catalysed the need for regulatory actions. The essential role in protecting the financial markets is highlighted as regulatory measures exert a positive effect on consumer confidence and systemic resilience. On the other hand, cybersecurity threats adversely impact financial inclusion. Furthermore, regulatory interventions moderate the connection between cybersecurity threat and financial inclusion indicating that while regulations enhance security, they may unintentionally impose obstacles to financial inclusion. In conclusion, this research offers new perspectives on the existing literature on FinTech regulation, financial inclusion and systemic resilience. It suggests policy aimed at integrating cybersecurity enforcement with financial inclusion. Adaptable regulatory framework is emphasised in the results, such that security threats are addressed effectively while ensuring financial access.

Keywords: Financial inclusion, regulatory, FinTech, cybersecurity, resilience

---

[1]Corresponding Author, PhD, Lecturer, Department of Economics, Caleb University, Lagos, Nigeria. Email: onioluwasola@yahoo.com

[2] Banking Supervision Department, Central Bank of Nigeria, Lagos, Nigeria. Email: aojapinye@cbn.gov.ng

[3] PhD. Senior Lecturer, Department of Economics, Caleb University, Lagos, Nigeria. Email: gilbert.ifarajimi@calebuniversity.edu.ng

[4] Researcher Assistant, Department of Economics, Caleb University, Lagos, Nigeria. Email: olubowalefavour9@gmail.com

---

Received: 31 March,2025

Accepted: 03 July 2025

DOI: https://dx.doi.org/10.4314/ajebr.v4i2.4

1. Introduction

The profitability of conventional banks has drastically reduced due to the competitive pressure of FinTech firms and the trend is projected to continue. Higher risk has been assumed by the firms pressing onto a long-standing industry rival. In preserving relevance and innovation, existing banks are motivated by these pressures. Authorities and regulators, whose responsibilities are to monitor and control challenging risks to maintain financial stability, ensure consumers get better access to outstanding financial services, are also confronted with these developments. Still a major challenge is how effectively the government handle cybersecurity problems while supporting innovation and financial inclusion.

Rural regions have benefited significantly from fintech solutions like mobile payments and digital loans that enhance access to digital financial services. Companies like Opay, Moniepoint, Palmpay, and Paga have granted financial access to low-income and rural populations through mobile banking and agent networks after previously being excluded from the financial system. In Nigeria, small businesses and individuals have been empowered by the expansion of access to financial services, thereby enhancing economic growth (World Bank, 2020). Such expansion has brought about vulnerabilities that could destabilize the banking industry.

A surge in cybersecurity challenges, including hacking and data breaches, is what the digitalisation of financial transactions has brought. In 2021 cyber-attacks rose by 173%, consequently increasing the worries about consumer safety and resilience of the financial institution (KPMG 2021). Much reliance on the external technology providers and insufficient regulatory control resulted in the growth of systemic risk in the FinTech sector, as evidenced in the failure of digital payment systems during the COVID-19 pandemic and revealed the level of vulnerabilities in FinTech system in Nigeria (Akinbowale et al., 2024). Financial, legal, security, operational, and product related risks are important concerns, which influence consumer reluctance to explore Fintech innovations (P2P lending, crowdsourcing, and blockchain) that are associated with increased transparency, reduced costs, and facilitated greater accessibility of financial information (Asiedu, 2025).

According to Cambridge Centre for Alternative Finance (CCAF, 2021), deficiency of strong enforcement for financial regulations, inconsistency in policy execution and pervasive corruption generate uncertainty about the regulatory environment that weakens investors' trust. Substantial governance and regulatory challenges degenerated into systemic risk's increase in the financial sector. The rapidly changing FinTech landscape requires a regulatory framework that balances innovative advancement and customer protection from risk to maintain customer safety and promote competitive market practices. A lot of monitoring gap allows the incidences of regulatory arbitrage and expose financial systems to risk from

unregulated digital services, resulting from a fragmented regulatory framework. Therefore, a thorough review is needed to enhance and sustain financial stability for long-term growth, governance structures, policy efficacy, and regulatory shortcomings.

Worldwide government and regulatory organisations have had to adjust to the dynamic environment to safeguard consumers so that financial stability and enforcement of current legislation can be guaranteed. The guidelines enacted for FinTech are designed to find a middle ground between innovations and minimize risks to the consumer and the financial system. While entities like the Central Bank of Nigeria have provided frameworks - The Payment Service Banks (PSBs) framework, to control FinTech firms, unfortunately enacted measures are not as rapid as the technology changes (Central Bank of Nigeria, 2021). Poor supervision may result from the regulatory gap, subsequently exposing the operations to risks that may represent a threat to the overall financial stability (Vijayagopal, 2024). For instance, market fragmentation growth resulting from competition of FinTech startups is likely to weaken the financial institutions' stability, thus offering systemic risks to the economy and questioning the future role of conventional banking (PwC Nigeria, 2020).

This study explores a critical, yet understudied, relationship in the financial innovation landscape – the interplay between fintech advancements, cybersecurity threats, regulatory measures, and financial inclusion in emerging economies, with a specific focus on Nigeria. According to Arner et al., (2019), the significance of FinTech is largely shown in the expanding financial access yet, the extent to which it has affected financial stability has not been thoroughly investigated in developing countries. Many literatures in this context have documented studies on advanced countries whose regulatory framework and environment, and technical infrastructure are distinctly different from the emerging countries (Chen et al., 2019)

This research provides insights into the various regulatory and infrastructure environments that characterise the developing countries using Nigeria as a case study. Especially in the underserved communities, limited internet accessibility and the gap in digital literacy have strengthened the vulnerabilities that accompany financial innovations (Klapper & Lusardi, 2020). Specifically, Familoni and Shoetan (2024); Atere (2022) observed that few studies have investigated the impact of FinTech-related cyber threats on financial stability in Nigeria. The expanding Fintech sector has given rise to a lot of pressing cybersecurity concerns that need to be addressed to avoid compromising customer confidence and destabilising the financial system.

The study seeks to empirically examine the nature and degrees of cybersecurity challenges and associated regulatory framework in the FinTech sector to ensure financial inclusion. Specifically, this article examines the following research questions:

1. How do the combined impact of cybersecurity risks and regulatory responses affect customer confidence and financial stability?
2. To what extent does regulatory responses mediate into the relationship between cybersecurity risks and financial inclusion.

2. Literature Review

2.1 Theoretical Framework

This study's theoretical framework integrates three core elements: financial stability theory (FST), the technology acceptance model (TAM), and the diffusion of innovation (DOI). This triangulated framework explore how cybersecurity risks and regulatory interventions interact with financial inclusion and systemic stability in Nigeria's evolving FinTech landscape.

Financial stability, technology adoption, and diffusion of innovation

The financial stability theory studies how financial systems manage threats from both internal and external disruptions to preserve economic stability (Claessens & Kodres, 2014). This framework examines whether technological advances in financial services introduce cybersecurity risks that might destabilize financial systems even as they enhance services (Arner et al., 2016). In weakly regulated environments such as Nigeria, risks are magnified, making the stability of the financial system contingent on the effectiveness of adaptive regulatory responses. In the context of this study the theory takes on renewed urgency as digital financial innovations introduce both efficiency and systemic vulnerabilities. Cyber security threats like data breaches, phishing, and algorithms manipulation can trigger trust failures, undermine digital payment systems, and propagate liquidity crises if not effectively managed. The dynamics (behavioural or diffusion) involve in FinTech integration cannot wholly be described with FST, hence Technology Acceptance Model (TAM) is employ to add dept to FST by explaining how individual user perceptions of the risk regulatory trust, and ease of use. A failure in perceived cybersecurity or regulatory trust translates into suppressed adoption, which in turn weakens the inclusion imperative central to macro-stability.

The Technology Acceptance Model (TAM), established by Davis in 1989, examines user adoption through the lens of perceived ease of use and usefulness. The application of TAM in Nigeria shows how

consumers evaluate mobile payment systems and automated investment advice while highlighting trust and regulatory assurance as crucial elements of adoption trends (Alalwan et al., 2018). Thus, TAM helps explain how perceived cybersecurity and regulatory quality can influence consumers' willingness to adopt Fintech services, which in turn feeds into the broader question of market depth and financial inclusion. The systemic stability envisaged by FST, therefore, partly hinges on micro-level behavioural factors that TAM captures particularly in economies where digital trust is volatile and informal systems persist. An improved TAM in this study reflects not only user-centric concerns with functionality and usability but also the intersecting influence of systemic financial health (financial stability theory) and the social transmission of innovation (Diffusion of Innovation theory).

The Diffusion of Innovation theory (DOI) from Rogers (1962) clarifies how FinTech innovations reach Nigerian financial consumers. The adoption rate of technologies depends on compatibility with existing systems, perceived complexity, and social influence (Akter et al., 2023; IMF, 2023). Public trust and FinTech adoption rates increase when regulatory endorsement and peer networks influence people's decisions, according to (Ifechukwu, 2022). DOI go together with TAM by shifting the unit of analysis to social systems and innovation characteristics. The theory underscores that innovations with vague regulatory backing or unsettled security disputes may spread randomly, initiating disintegrated financial ecosystems liable to exclusion, manipulation, or instability where regulatory framework are weak or lag behind innovation. Through DOI analysis, this study examines how regulatory measures alongside social forces affect the spread of FinTech solutions and subsequently determine Nigeria's financial stability.

Integrating these theories, the study set up a multilevel analytical framework: systemic (FST), behavioural (TAM) and societal (DOI). The layered approach allows for a higher degree of understanding of how regulation mediates the tension between cybersecurity risk and inclusion, and ultimately influences financial system resilience

2.2 Empirical Evidence

Multiple theoretical frameworks and methodologies have investigated FinTech cybersecurity to analyse various components of its risk landscape and security weaknesses. Bakari et al. (2023) applied victimisation theory to investigate the elements that affect cybercrime exposure in the service industry and found that economic inequality increases risk exposure. The research findings demonstrate that institutions and individuals must implement customised strategies to reduce cybersecurity risks. Agosto and Giudici (2023) evaluate cyber risks through a multivariate model with time-varying parameters validated with real-world

cyber loss datasets. The research produced tools to predict cyberattack probabilities while highlighting sectoral risk connections and the necessity of analysing time-dependent patterns.

Research has concentrated on the systemic risks of cyber threats to financial stability. Brando et al. (2022) analysed cybersecurity effects on global financial systems but did not thoroughly explain their research methods. Bouveret (2018) used operational risk frameworks and actuarial science tools to measure financial losses from cyberattacks by applying Bayesian methods and Poisson distributions to model possible outcomes. The analytical method supports adherence to regulations while improving financial risk management strategies. Eisenbach et al. (2022) investigated systemic connections across the U.S. wholesale payments network, revealing significant spillover effects from cyber disruptions. The research works demonstrate how cyber threats trigger widespread effects throughout financial systems.

Researchers have developed innovative methodologies and tools to address cybersecurity threats. Javaheri et al. (2024) uncovered 11 main cyber threats and nine defensive tactics while recommending modern defensive mechanism developments to tackle new security challenges. Bahar (2023) developed the Metric-Based Feedback Methodology (MBFM), which combines threat modelling with bug bounty programs to enhance security prioritisation while improving threat models. Falade and Ogundele's 2023 research revealed significant security weaknesses in UK digital banking applications, demonstrating the immediate need for stronger security measures. Haruna et al. (2022) opined the principle of defense-in-depth by correlating cybersecurity threats to their corresponding defensive measures while integrating technological solutions with application-specific strategies.

Research on cybersecurity within FinTech has expanded through investigations into particular regional and industry niches. Najaf et al. (2020) investigated risks traditional banks face during collaborations with FinTech firms and recommended joint risk management solutions to achieve operational effectiveness. AlBenJasim et al. (2024) developed a custom cybersecurity framework for Bahrain which aligned with global standards while focusing on regional challenges. Sidana et al. (2024) boosted financial data security by integrating green technology into cybersecurity practices. He (2023) showed worldwide investment priorities target cybersecurity and risk management through public-private sector collaborations. Arabyat et al. (2024) researched the interplay between technological advancements and regulatory policies in Jordan's financial sector and studied ethical and operational challenges of Islamic finance.

FinTech's growth has made its regulatory and governance concerns a key area for attention. Akinbowale et al. (2024) accentuate that establishing a unified policy framework serves as an essential countermeasure to the cyber fraud challenges faced by banks in South Africa. The authors demonstrate

detection system vulnerabilities in cyber fraud through mixed methods research combining surveys with statistical analysis and advocate for standardised regulatory frameworks to enhance system resilience. Similarly, Abrahams et al. (2024) examined global accounting and cybersecurity regulations to identify technological challenges from blockchain and AI innovations. Study outcomes reveal digital asset protection requires technological solutions and effective governance measures.

The ongoing fusion of advanced technologies and governance systems continues to be a leading trend. A new AI-based method for bettering GRC systems alongside strategic cybersecurity aid for FinTech firms was proposed by (Oluokun et al., 2024). Arner et al. (2022) researched the transformation of financial services through digitalisation by examining FinTech 4.0 progress and the growth of key digital finance platforms. The new framework blends functional supervision and activity-based regulation with entity-specific oversight to control concentration risks and preserve innovation benefits. Research findings demonstrate that new risks require handling through a technology-based regulatory framework.

Studies have analysed how regulatory measures affect FinTech companies which contribute to sustainable development and financial inclusion initiatives. The Pashang and Weber (2021) research recognizes FinTech's capacity to advance ESG targets but identifies fragmented governance structures as barriers to its development. Vijayagopal et al. (2024) studied how United States, United Kingdom and Indian regulatory frameworks advance balanced growth through digital infrastructure development and financial literacy education combined with effective regulator-stakeholder collaboration. Brown and Piroska (2021) condemn the regulatory sandbox framework for allowing "riskwashing" and emphasize the need for robust supervision systems to control the socially disruptive power of FinTech.

Recent studies reveal heightened systemic and cybersecurity risks stemming from influencer manipulation (Krause, 2025), regulatory gaps (Elumalai, 2025), and digital payment vulnerabilities (Oladinni & Odumuwagun, 2025; Nahidi, 2025). Fintech’s benefits for transparency, inclusion, and cost reduction are affirmed (Asiedu, 2025; Monica & Mounica, 2025), but risk perception remains a deterrent to adoption. Evidence from MENA (Afzal et al., 2025) and South Asia (Adnan & Kumar, 2024; Mustafa, 2024) supports fintech’s potential to enhance banking stability and financial development and when coupled with strong institutional oversight. The reviewed literature underscores the urgent need for integrated strategies involving real-time fraud detection, regulatory technology (regtech), and international coordination to mitigate emerging risks while sustaining inclusive financial innovation.

Experts recommend different regulatory approaches to oversee FinTech development and safeguard consumer rights in public spaces. Bains and Wu (2023) research passive monitoring techniques and innovation hubs and promote FinTech specialist recruitment into regulatory bodies to enhance monitoring

standards. The research by Biswas et al. (2024) highlights that regulatory authorities and industry participants need to collaborate to address technological advancements and market changes. The 2021 study by Giglio examines six primary FinTech business models to show how these models help integrate financial markets throughout the European Union. Findings indicate the need for flexible frameworks supporting innovative advancements while minimising systemic risks.

3. Materials and Method

3.1 Research Design

This research employs a quantitative methodological framework to investigate the interplay between cybersecurity apprehensions, regulatory interventions, consumer confidence, systemic resilience, and financial accessibility within Nigeria's fintech domain. A structural equation Model (SEM) methodology is utilized owing to its capability of concurrently assessing both measurement and structural interrelations among latent and manifest variables. The application of SEM is particularly pertinent to this inquiry as it facilitates hypothesis evaluation while rectifying measurement inaccuracies in observable indicators (Kline, 2023).

3.2 Population and Sampling Technique

The demographic focus of this research encompasses fintech consumers, financial regulatory entities, and industry practitioners within Nigeria. A stratified random sampling methodology was employed to guarantee a comprehensive representation across fintech service consumers, banking specialists, and regulatory personnel. The 284 samples were gathered from major FinTech hubs in Nigeria Lagos (91 respondents), Abuja (84 respondents), and Port Harcourt (73 respondents) areas where digital financial services are widely embraced. The research utilized a standardised instrument comprising closed-ended Likert scale questions (Strongly Disagree = 1 to Strongly Agree =5). The instrument was formulated based on validated constructs from preceding research (Rehman et al., 2021; Ozili, 2018).

This tool encompasses five principal constructs: Cybersecurity Risks (CSR) gauges users' perceptions regarding security threats associated with fintech, Regulatory Responses (RR) evaluates the sufficiency and efficacy of fintech regulations. Customer Trust (CTF) assesses the degree of confidence in fintech security and dependability. Systemic Stability (SSF) scrutinizes the resilience of Nigeria’s fintech sector in the face of cybersecurity threats, while Financial Inclusion (FIF) measures the accessibility and engagement with fintech services among individuals across various economic strata.

3.3 Measurement Model and Variable Specification

The measurement framework in this study is designed to capture the relationships among essential latent constructs—cybersecurity risks (CSR), regulatory responses (RR), customer trust (CTF), systemic stability (SSF), and financial inclusion (FIF)—utilizing multiple observable indicators. A Structural Equation Modelling (SEM) approach is implemented to authenticate the reliability and construct validity of these latent variables. All observable factors are rated on a 5-point Likert scale (1 - Strongly Disagree to 5 - Strongly Agree). Presented in Table 3.1 are the latent constructs and observable indicators.

Table 1: Latent constructs and observed indicators

Latent Variable	**Observed Variables**
Cybersecurity Risks (CSR)	csr2: It is possible to come across fraudulent activities or data breaches when using fintech services.
	csr3: Fintech services are safe from cyberattacks.
	csr4: Fintech providers should take adequate measures to protect users from cybercrime.
Regulatory Responses (RR)	rr3: Regulatory guidelines govern fintech services in Nigeria.
	rr5: Regulatory bodies are responsive to consumer concerns regarding fintech services.
Customer Trust (CTF)	ctf3: Fintech providers should enhance their cybersecurity measures.
	ctf4: Fintech companies can be trusted with personal and financial information
Systemic Stability (SSF)	ssf1: The financial system may become unstable as a result of regulatory uncertainty, which could hinder fintech growth.
	ssf2: Fintech companies are adequately regulated by government bodies.
	ssf3: Fintech companies offer better financial services compared to traditional banks.
Financial Inclusion (FIF)	fif1: What is your primary reason (Convenience, Cost savings, etc.) for using fintech services?
	fif2: How often (Daily, Weekly, etc.) do you use fintech services such as mobile banking or online payment platforms?

Model Specification

Latent Constructs and Measurement Equations

$$CSR = \alpha_1 + \alpha_2 csr2 + \alpha_3 csr3 + \alpha_4 csr4 + \varepsilon_{csr}$$

$$CTF = \alpha_5 + \alpha_6 ctf3 + \alpha_7 ctf4 + \varepsilon_{ctf}$$

$$FIF = \alpha_8 + \alpha_9 fif1 + \alpha_{10} fif2 + \alpha_{11} fif3 + \varepsilon_{fif}$$

$$RR = \alpha_{12} + \alpha_{13} rr3 + \alpha_{14} rr5 + \varepsilon_{rr}$$

$$SSF = \alpha_{15} + \alpha_{16} ssf1 + \alpha_{17} ssf2 + \alpha_{18} ssf3 + \varepsilon_{ssf}$$

Where:

α_i are the factor loadings (strength of each indicator with the latent variable).

ε represents the measurement error terms for each latent construct.

Structural Model (Hypothesized Relationships)

Latent model equations

$$RR = \lambda_1 CSR + e_1$$

$$CTF = \lambda_2 CSR + \lambda_3 RR + e_2$$

$$SSF = \lambda_4 RR + \lambda_5 CTF + e_3$$

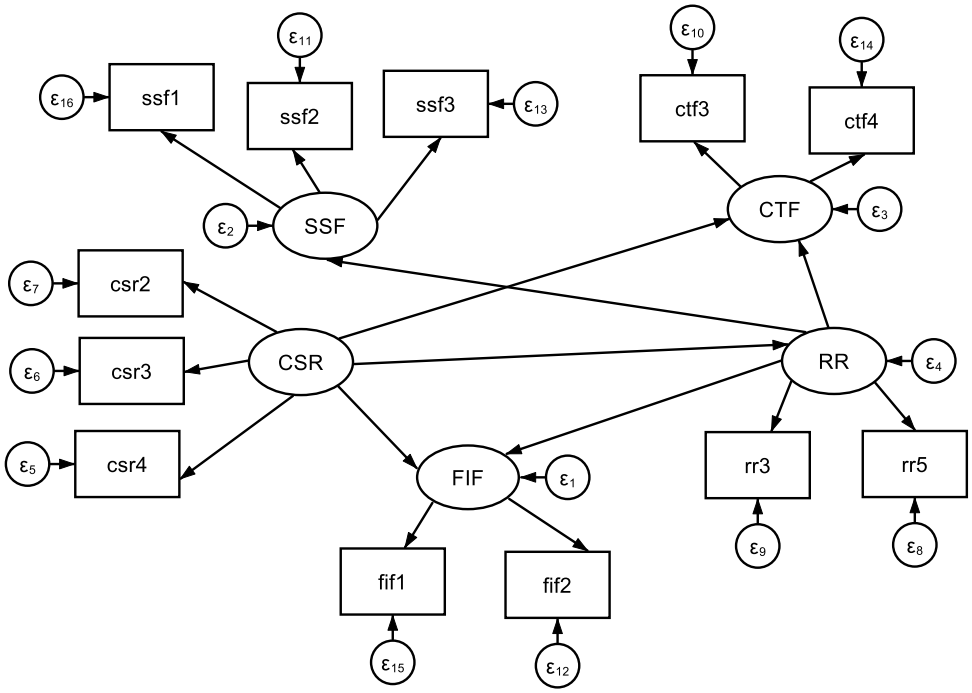
$$FIF = \lambda_6 CSR + \lambda_7 RR + e_4$$

Where:

λ_i are **path coefficients** measuring the strength and direction of influence.

e represents the **structural error terms** accounting for unexplained variance.

Figure 1: Structural Path Diagram Representation of Observed and Latent Variables



Source: Structural Path Diagram Representation from Stata 16 SEM Builder

4. Result and Discussions

Descriptive Statistics

There are 248 total responses in the survey dataset, and few changes in response rates based on minimum missing data across demographic groups. This summary is of the gender distribution, age range, income levels, labour force participation, and generational variations among the respondents. Male and female respondents are almost equally represented in the sample. With 52.0% (n = 128) men and 48.0% (n = 118) women make up respectively. This equal gender distribution guarantees different points of view on fintech uptake, cybersecurity issues, and regulatory impressions, therefore improving the representativeness of the research. Age distribution in the sample reflects a youth-dominated sample, with the largest group falling within the 30-34 age range (26.0%), followed closely by 25-29 years (24.0%) and 20-24 years (18.7%). The youngest group, 15-19 years, accounts for 11.4%, while only 9.8% of respondents are 40 years and above. The bias towards younger respondents indicates significant involvement with digital financial technology among this demographic, consistent with worldwide fintech adoption trends that reveal elevated usage rates among digitally native generations. The respondents are divided into three generational cohorts. Generation Z (37.6%) born after the mid-1990s are highly involved in digital finance. Millennials (37.2%) are a prominent fintech user segment driving adoption and market growth. Generation X (25.2%)—a smaller but substantial cohort that could be early consumers of digital financial services. The prevalence of Generation Z and Millennials (74.8% combined) shows that fintech adoption is highest among younger and middle-aged consumers who are more technologically savvy.

With 59.4% earning below ₦100,000 per month, most respondents are low-income earners. the remaining income ranges are somewhat fairly spread, with 13.5% earning between ₦100,000 - 199, 999, 12.7% in the ₦200,000 – 299, 999 range and 7.8% earning between ₦300,000 - 499, 999. Only 6.6% of respondents say they make ₦500,000 or more. This suggests that lower-income people are primarily responsible for fintech adoption in Nigeria, maybe because digital financial services are more freely accessible than traditional banking. The sample represents a diversified workforce. 38.0% of survey respondents are employed, 31.4% are self-employed, 12.2% are unemployed, and 18.4% are students. The significant proportion of wage workers and self-employed persons demonstrates fintech's relevance to both formal and informal industries. The 18.4% student representation implies that fintech solutions are increasingly popular among the younger, more financially active demographic.

The Structural Equation Modelling (SEM) results are interpreted in accordance with the study's two primary research topics and the larger literature. To validate the measurement model's validity, Confirmatory Factor Analysis (CFA) was performed prior to estimating the structural routes. The goodness-

of-fit indices corroborate the model's adequacy, model's adequacy to the hypothesised linkages between cybersecurity threats, regulatory responses, customer trust, systemic stability, and financial inclusion.

Standard indices were used to evaluate model fit, and the results showed that it was overall satisfactory. The Comparative Fit Index (CFI) of 0.903 exceeds the recommended threshold of 0.90, indicating a good level of model fit. The Root Mean Square Error of Approximation (RMSEA) is 0.097, somewhat higher than the ≤ 0.08 threshold, indicating a moderate match with room for improvement. Furthermore, the Standardised Root Mean Square Residual (SRMR) is 0.071, which is within the acceptable ≤ 0.08 range, demonstrating a strong alignment between the hypotheses model and observed data.

Research Question 1: How do the combined impact of cybersecurity risks and regulatory responses affect customer confident and financial stability?

Table 2: Structural Equation Path

Path	Standardized Coefficient (β)	Significance (p-value)	Interpretation
CSR → RR	1.123	0.000	Strong positive effect
CSR → CTF	1.027	0.000	Strong positive effect
RR → CTF	1.122	0.000	Strong positive effect
RR → SSF	1.014	0.000	Strong positive effect
CTF → SSF	1.058	0.000	Strong positive effect
CSR → FIF	-0.416	0.000	Significant negative effect
RR → FIF	-0.483	0.000	Significant negative effect

Source: Data processed by Stata 16, 2025

This section presents the interpretation of the structural equation model results in alignment with the research questions and broader literature. The findings are discussed under two key research questions. The first research question examines the relationships among the latent variables, the interconnectedness of cybersecurity risks (CSR), regulatory responses (RR), customer trust (CTF), and systemic stability (SSF). Table 2 displays the structural path of the coefficients which were used to explain the direct relationships between the latent variables. The p-value of 0.001 and a coefficient of 1.123 indicate that cybersecurity threats exert a positive and significant impact on regulatory responses. This indicates increased risks compel regulatory agencies to establish measures to alleviate potential hazards. KPMG (2021) underlines that rising legal and regulatory compliance requirements are complicate compliance risks and act as a primary driver of improvements to cybersecurity capabilities, so corroborating the idea that enhanced cybersecurity risks compel regulatory agencies to implement measures meant to mitigate possible hazards. Cyble (2024) also stresses the important junction between cybersecurity and regulatory compliance, pointing out that companies can reach compliance, improve their cybersecurity posture, and build customer confidence by using a proactive, integrated strategy. The coefficient and probability value ($\beta = 1.027$, $p < 0.001$) show that perceived security flaws directly affect customers' confidence in fintech services, suggesting that

cybersecurity risks (CSR) have a positive and significant impact on customer trust (CTF). This result, however, runs counter to the claims made by Wamba et al. (2020), who contend that trust might withstand sophisticated security measures in established marketplaces.

As displayed in Table 2, regulatory responses (RR) significantly impact customer trust (CTF) directly given that the coefficient $\beta = 1.122$ and probability value < 0.001. This finding shows the vital role of the regulation guidelines in enhancing FinTech customers' trust. The result aligns with Ozili's (2018) research, which underlines the need for good regulatory frameworks to generate trust in financial innovations. Furthermore, RR considerably enhances systemic stability (SSF) with its coefficient of 1.014 and P-value less than 0.001, implying that a well-designed regulatory framework supports the resilience of fintech ecosystems (Arner et al., 2020). With a correlation coefficient of 1.058 and with probability value $p < 0.001$, Customer trust encourages and promotes systemic stability. This highlights the view that trust is a keystone for the longevity of fintech services, consistent with the findings of Gomber et al. (2017). The results reveal that cybersecurity risks drive regulatory responses and directly influence customer trust. Regulatory interventions serve a moderating function by bolstering trust and stability. This underscores the necessity of combining security issues with proactive regulatory actions to sustain public confidence in fintech services.

Research Question Two: To what extent does regulatory responses mediate into the relationship between cybersecurity risks and financial inclusion.

Lastly, the structural equations model's results analysed the second research question: the extent to which regulatory responses mediate the relationship between cybersecurity risks and financial inclusion in Nigeria's fintech sector. The results were classified into three categories of impacts: direct, indirect, and total effects.

From Table 2 The result of the direct effects **(CSR → FIF)** shows that the coefficient ($\beta = -0.416$) and probability value ($p < 0.001$) is negative and less than 5% respectively. Cybersecurity risks negatively influence financial inclusion. This finding suggests that heightened risk perceptions may deter users from adopting fintech services, particularly in emerging economies where trust in digital platforms is still developing (Asongu et al., 2020).

Table 3: Mediation Effects

Path	Indirect Effect (β)	p-value	Interpretation
CSR → RR → FIF	Negative	0.000	Regulatory responses mitigate the negative link between cybersecurity threats and financial inclusion, highlighting policy-induced constraints.

Source: Data processed by Stata 16 2025.

Displayed in Table 3 is the mediation effects, showing the indirect effect (CSR → RR → FIF) which reveals that cybersecurity risks positively influence regulatory responses and regulatory responses negatively influence financial inclusion, possibly due to overregulation or policies that inadvertently limit access to fintech services. The mediating role of regulatory responses indicates an intricate dynamic. While CSR positively drives RR, the latter's impact on FIF is negative. This may reflect unintended consequences of regulatory policies, such as increased compliance costs or restrictions that limit access for underserved populations. Similar concerns were raised by Beck et al. (2016), who caution against the potential exclusionary effects of stringent financial regulations.

These findings underline regulatory organisations' need to implement inclusive approaches that address cybersecurity concerns without affecting accessibility. For example, tailored regulations that combine compliance requirements with financial inclusion goals could decrease the reported detrimental consequences.

Conclusions

In Nigeria's fintech market, this study investigates the interactions among cybersecurity threats, regulatory responses, customer trust, systemic stability, and financial inclusion. In the survey, the predominance of younger respondents and low-income earners aligns with fintech's promise of financial inclusion, indicating that digital financial services are filling gaps left by traditional banking institutions. Given the significant proportion of younger users and informal-sector workers, regulations should focus on consumer protection, cybersecurity, and financial literacy to ensure a safe digital finance ecosystem. With a high percentage of digitally engaged individuals in the sample, targeted cybersecurity education campaigns can further enhance trust and security in fintech usage.

The results, using a Structural Equation Modelling (SEM) approach, show that regulatory actions are mostly driven by cybersecurity concerns, therefore underlining the need for strong control systems. Customer confidence and systemic stability are greatly enhanced by regulatory measures, therefore guaranteeing resilience in the financial environment. However, the study finds a negative link between cybersecurity risks and financial inclusion, implying that even when increased security measures reduce hazards, they might also act as obstacles to more general access to fintech services.

Furthermore, the mediating role of regulatory actions in the relationship between cybersecurity threats and financial inclusion underlines the complicated interplay between security, compliance, and accessibility. Although stability and trust depend on rules, too stringent policies or overregulation could unintentionally inhibit financial inclusion, especially for lower-income people. These results emphasise the need to harmonise cybersecurity enforcement with rules promoting financial accessibility.

Policymakers should consider flexible rules that handle new cyber risks without thus restricting the use of fintech. Industry players have to cooperate to improve security systems and guarantee inclusiveness in digital financial services. Future studies should investigate the long-term effects of changing regulatory policies on financial inclusion and systemic stability especially in developing nations. Nigeria's fintech sector may reach sustained development, confidence, and resilience in the digital financial scene by encouraging a legislative environment that harmonises security with accessibility.

Funding: There is no specific financial support for this for research.

Competing Interests: All authors declare that there no conflicting interests.

Acknowledgement: Authors contributions are stated as follows:

Oluwasola Oni is the corresponding author; he provided the idea behind the research, develops the objective of the study, oversees data collection and methodology designs.

Abayomi Oluwaseun Jepinwa reviewed the relevant literature and situated the study within relevant literature.

Gilbert D. Ifarajimi involved in the writing and editing of the manuscript, he specifically reviewed and revised the manuscript for coherence and clarity.

Favour O. Olubowale assisted in data collection, designing of the estimation technique and statistical analysis.

References

Abrahams, T. O., Ewuga, S. K., Kaggwa, S., Uwaoma, P. U., Hassan, A. O., & Dawodu, S. O. (2024). Mastering compliance: a comprehensive review of regulatory frameworks in accounting and cybersecurity. *Computer Science & IT Research Journal*, *5*(1), 120-140.

Adnan, S. A., & Kumar, P. (2024). Financial Crimes and Fintech in India. In *E-banking, Fintech, & Financial Crimes: The Current Economic and Regulatory Landscape* (pp. 97-109). Cham: Springer Nature Switzerland.

Agosto, A., & Giudici, P. (2023). Cyber Risk Contagion. *Risks*, *11*(9), 165.

Akinbowale, O. E., Klingelhöfer, H. E., Zerihun, M. F., & Mashigo, P. (2024). Development of a policy and regulatory framework for mitigating cyberfraud in the South African banking industry. *Heliyon*, *10*(1).

Akter, M. S., Bhuiyan, M. R. I., Poli, T. A., & Hossain, R. (2023). Web-based banking services on E-customer satisfaction in private banking sectors: A cross-sectional study in developing economy. *Migration Letters*, *20*(S3), 894-911.

Alalwan A, Dwivedi YK, Rana NP et al (2016) Consumer adoption of mobile banking in Jordan: Examining the role of usefulness, ease of use, perceived risk and self-efficacy. Journal of Enterprise Information Management. 29(1): 118-139.

AlBenJasim, S., Dargahi, T., Takruri, H., & Al-Zaidi, R. (2024). Fintech cybersecurity challenges and regulations: Bahrain case study. *Journal of Computer Information Systems*, *64*(6), 835-851.

Anarfo, E. B., Abor, J. Y., & Osei, K. A. (2019). Financial inclusion and financial sector development in Sub-Saharan Africa: Do institutions matter? *Review of Development Finance*, 9(2), 69-82. doi:10.1016/j.rdf.2019.06.002.

Arabyat, Y.A., Alarabeyyat, A., Abuaddous, M. (2024). Overview of Cybersecurity Trends in Jordan's Financial Sector. In: Saeed, F., Mohammed, F., Fazea, Y. (eds) Advances in Intelligent Computing Techniques and Applications. IRICT 2023. Lecture Notes on Data Engineering and Communications Technologies, vol 211. Springer, Cham. https://doi.org/10.1007/978-3-031-59707-7_25

Arner, D. W., Barberis, J., & Buckley, R. P. (2020). FinTech and RegTech in a nutshell, and the future in a sandbox. *CFA Institute Research Foundation*.

Arner, D. W., Barberis, J., & Buckey, R. P. (2016). FinTech, RegTech, and the reconceptualization of financial regulation. *Nw. J. Int'l L. & Bus.*, *37*, 371.

Arner, D., Buckley, R., Charamba, K., Sergeev, A., & Zetzsche, D. (2022). Governing FinTech 4.0: BigTech, platform finance, and sustainable development. Fordham J. Corp. & Fin. L., 27, 1.

Asiedu, E. (2025). Risk factors affecting customer adoption of fintech in the financial services sector. In *Bentham Science Publishers eBooks* (pp. 21–27). https://doi.org/10.2174/9789815324907125010005

Asongu, S. A., Nwachukwu, J. C., & Pyke, C. (2020). The Mobile Phone in the Diffusion of Financial Services. *Technological Forecasting and Social Change*, 151, 119755.

Atere, T. O. (2022). *Cybersecurity regulation in the financial sector: reflexive risk management in the UK, USA and Nigeria* (Doctoral dissertation, Newcastle University).

Afzal, A. M., Khalaf, B. A., Al-Naimi, M. S., & Samara, E. (2025). The impact of fintech on the stability of Middle Eastern and North African (MENA) banks. *Risks*, *13*(6), 106. https://doi.org/10.3390/risks13060106

Bahar, S. W. (2023). Advanced Security Threat Modelling for Blockchain-Based FinTech Applications. *arXiv preprint arXiv:2304.06725*.

Bains, P., & Wu, C. (2023). *Institutional arrangements for fintech regulation: supervisory monitoring*. International Monetary Fund.

Bakari, N. A. B., Mohamed, I. S., & Nazuri, S. N. S. (2023). Understanding Cyber Threats Vulnerability of Future Victimization in Fintech. *Business and Management Horizons*, *11*(1).

Beck, T., Demirgüç-Kunt, A., & Levine, R. (2016). Finance, Inequality, and Poverty: Cross-Country Evidence. *World Bank Economic Review*, 24(1), 65-98.

Biswas, R., Sahab, P., Paulc, G., & Sahad, A. K. (2024). Regulatory Outlook in Fintech: A Review. International Journal of Research Publication and Reviews, 5, 7100-7108.

Bouveret, A. (2018). *Cyber risk for the financial sector: A framework for quantitative assessment*. International Monetary Fund.

Brando, D., Kotidis, A., Kovner, A., Lee, M., & Schreft, S. L. (2022). Implications of cyber risk for financial stability.

Brown, E., & Piroska, D. (2021). Governing Fintech and Fintech as Governance: The Regulatory Sandbox, Riskwashing, and Disruptive Social Classification. *New Political Economy*, *27*(1), 19–32. https://doi.org/10.1080/13563467.2021.1910645

Claessens, M. S., & Kodres, M. L. E. (2014). *The regulatory responses to the global financial crisis: Some uncomfortable questions*. International Monetary Fund. https://www.imf.org/external/pubs/ft/wp/2014/wp1446.pdf

Central Bank of Nigeria (2021). Supervisory Framework for Payment Service Banks. Retrieved from https://www.cbn.gov.ng/out/2021/ccd/supervisory%20framework%20for%20psbs.pdf.

CCAF (2021) FinTech Regulation in Sub-Saharan Africa, Cambridge Centre for Alternative Finance at the University of Cambridge Judge Business School, Cambridge. https://www.jbs.cam.ac.uk/wp-content/uploads/2021/11/2021-11-fintech-in-sub-saharan-africa.pdf

Chen, B., Yang, X., & Ma, Z. (2022). Fintech and financial risks of systemically important commercial banks in China: an inverted U-shaped relationship. *Sustainability*, *14*(10), 5912.

Cyble (2024). The Impact of Regulatory Compliance on Cybersecurity Strategy. https://cyble.com/knowledge-hub/the-impact-of-regulatory-compliance-on-cybersecurity-strategy/

Davis, F. D. (1989). Technology acceptance model: TAM. *Al-Suqri, MN, Al-Aufi, AS: Information Seeking Behavior and Technology Adoption*, *205*, 219.

Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the US financial system: A pre-mortem analysis. *Journal of Financial Economics*, *145*(3), 802-826.

Elumalai, D. (2025). Cybersecurity in Fintech: Protecting Digital Transactions and Financial Innovation. *QTanalytics Publication (Books)*, 97–107. https://doi.org/10.48001/978-81-980647-2-1-9

Falade, P. V., & Ogundele, G. B. (2023). Vulnerability analysis of digital banks' mobile applications. *arXiv preprint arXiv:2302.07586*.

Familoni, B. T., & Shoetan, P. O. (2024). Cybersecurity in the financial sector: a comparative analysis of the USA and Nigeria. *Computer Science & IT Research Journal*, *5*(4), 850-877.

Giglio, F. (2021). Fintech: A literature review. European Research Studies Journal, 24(2B), 600-627.

Gomber, P., Koch, J.-A., & Siering, M. (2017). Digital Finance and FinTech: Current Research and Future Research Directions. *Journal of Business Economics*, 87(5), 537-580.

Ifechukwu, A. (2022). Regulating Fintech in Developing Economies: Examining The Risks, Policies and Nigeria's Path to Financial Prosperity. *Policies and Nigeria's Path to Financial Prosperity (December 26, 2022)*.

Haruna, W., Aremu, T. A., & Modupe, Y. A. (2022). Defending against cybersecurity threats to the payments and banking system. arXiv preprint arXiv:2212.12307.

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*, *241*, 122697.

Klapper, L., & Lusardi, A. (2020). Financial literacy and financial resilience: Evidence from around the world. *Financial Management*, *49*(3), 589-614.

Kline, R. B. (2023). *Principles and practice of structural equation modeling*. Guilford publications.

KPMG (2021). Nigeria Cyber Security Outlook 2021. Retrieved from https://www.deloitte.com/ng/en/services/risk-advisory/perspectives/nigeria-cyber-security-outlook-2021.html.

Krause, D. (2025). The Impact of Financial Influencers on Crypto Markets: Systemic Risks and Regulatory Challenges. https://doi.org/10.2139/ssrn.5144847

Monica S, & Mounica V,. (2025). Exploring the Role of Fintech Solutions on Financial Inclusion Among MSMEs in Bengaluru: The Impact of Technology Infrastructure, Regulatory Environment, and Digital Literacy. *European Economic Letters (EEL)*, *15*(1), 155–168. https://doi.org/10.52783/eel.v15i1.2385

Mustafa, J. A. (2024). Integrating financial literacy, regulatory technology, and decentralized finance: A new paradigm in Fintech evolution. *Investment Management and Financial Innovations*, *21*(2), 213–226. https://doi.org/10.21511/imfi.21(2).2024.17

Nahidi, N. (2025). Cybersecurity in Fintech from a Corporate Finance Perspective. In: Zarifis, A., Cheng, X. (eds) Fintech and the Emerging Ecosystems. Financial Innovation and Technology. Springer. https://doi.org/10.1007/978-3-031-83402-8_20

Najaf, K., Schinckus, C., Mostafiz, M. I., & Najaf, R. (2020). Conceptualising cybersecurity risk of fintech firms and banks sustainability.

Oladinni A & Odumuwagun O.O (2025) Enhancing Cybersecurity in FinTech: Safeguarding Financial Data Against Evolving Threats and Vulnerabilities. International Journal of Computer Applications Technology and Research Volume 14–Issue 01, 62 – 78, 2025, DOI:10.7753/IJCATR1401.1005

Oluokun, A., Ige, A. B., & Ameyaw, M. N. (2024). Building cyber resilience in fintech through AI and GRC integration: An exploratory Study. *GSC Advanced Research and Reviews*, *20*(1), 228-237.

Ozili, P. K. (2018). Impact of Digital Finance on Financial Inclusion and Stability. *Borsa Istanbul Review*, 18(4), 329-340.

Pashang, S., & Weber, O. (2021). Fintech for good: Governance mechanisms for sustainable development (No. 257). CIGI Papers.

PwC Nigeria (2020). Changing the opportunity landscape: Fintech and Banking Sector in Nigeria. Retrieved from https://www.pwc.com/ng/en/assets/pdf/fintech-banking-sector-nigeria.pdf
Qiang, X. (2024). Digital Transformation in the Financial Sector Through Fintech. *Advances in Economics, Management and Political Sciences*, *76*, 226-234. https://doi.org/10.54254/2754-1169/76/20241656

Rehman, M., Bhatti, A., & Chaudhry, A. (2021). Cybersecurity and Regulatory Challenges for Fintech: A Systematic Review. *Information and Computer Security*, 29(2), 185-208.

Rogers, E. M. (1962). Diffusion of Innovations, Library of Congress Cataloguing in Publication Data. *Innovation*, *11*(2).

Sidana, N., Nidhi, J.S., Rathi, L., Goel, R. (2024). Greentech Guardians: Navigating the FinTech Cybersecurity Labyrinth for Sustainable Solutions. In: Mansour, N., Baral, S., Garg, V. (eds) E-Financial Strategies for Advancing Sustainable Development. Sustainable Finance. Springer, Cham. https://doi.org/10.1007/978-3-031-67523-2_22

Vijayagopal, P., Jain, B., & Ayinippully Viswanathan, S. (2024). Regulations and Fintech: A Comparative Study of the Developed and Developing Countries. *Journal of Risk & Financial Management*, *17*(8).

Wale-Awe, B., Folorunsho, D., & Shobande, A. (2020). Mobile banking adoption and financial inclusion in Nigeria. *Fuoye Journal of Finance and Contemporary Issues*, 4(1), 102-115.

Wamba, S. F., Akter, S., Edwards, A., Chopin, G., & Gnanzou, D. (2020). How "Big Data" Can Make Big Impact: Findings from a Systematic Review and a Longitudinal Case Study. *International Journal of Production Economics*, 165, 234-246.

World Bank (2020). Nigeria Digital Economy Diagnostic Report: Leveraging Digital Technology for a Resilient Economic Recovery. Retrieved from https://documents1.worldbank.org/curated/ar/387871574812599817/pdf/Nigeria-Digital-Economy-Diagnostic-Report.pdf