GJR Publication
OPEN ACCESS

Global Journal of Research in Engineering & Computer Sciences
ISSN: 2583-2727 (Online)
Volume 05| Issue 06 | Nov.-Dec. | 2025
Journal homepage: https://gjrpublication.com/gjrecs/

Original Research Article

Cybersecurity Implications of Nigeria's Momo PSB Breach: Organizational Responses, Policy Adaptation and User Trust

*Iyanu Emmanuel Olatunbosun

Department of Criminology and Security Studies, National Open University of Nigeria.
ORCID ID: 0009-0005-6059-6832

DOI: 10.5281/zenodo.17574348 **Submission Date: 28 Sept. 2025 | Published Date: 10 Nov. 2025**

Abstract

The 2022 security breach at MoMo Payment Service Bank (PSB), a subsidiary of MTN Nigeria, is a critical case study of cybersecurity challenges in emerging digital financial ecosystems. The incident, which resulted in unauthorised transfers totalling approximately ₦22.3 billion ($53 million), occurred just days after the service's launch, highlighting systemic vulnerabilities in Nigeria's rapidly expanding fintech landscape. This research examines the organizational responses to the MoMo PSB breach, analyzes subsequent policy adaptations, and assesses the implications for user trust in digital financial services. The study employs a systematic literature review methodology, analyzing secondary data from academic publications, official statements, regulatory filings, and media reports between 2022 and 2025. Data were synthesized using thematic analysis to identify patterns in organizational crisis response, regulatory evolution, and trust-repair strategies. The analysis reveals a multi-layered response strategy comprising technical containment, regulatory compliance, and trust-rebuilding measures. MTN Group's incident response included immediate service suspension, fraud reversal processes, and collaboration with law enforcement agencies. Regulatory investigations by the Nigeria Data Protection Commission (NDPC) identified deficiencies in data governance, prompting enhanced compliance requirements. The breach triggered a strategic reorientation at MoMo PSB, including investments in digital infrastructure and applications for additional licensing to strengthen security capabilities. These responses occurred against a backdrop of declining user adoption, with active wallets decreasing by 46% following the incident. The MoMo PSB case demonstrates the critical intersection of cybersecurity, regulatory oversight, and consumer trust in digital financial services. Effective organizational response requires not only technical remediation but also transparent communication and proactive policy engagement. The incident underscores the necessity of collaborative security frameworks involving financial institutions, telecommunications providers, regulators, and consumers to strengthen Nigeria's digital financial ecosystem against evolving threats.

Keywords: *Cybersecurity, Mobile Money, Data Breach, Organizational Response, Policy Adaptation, User Trust, Nigeria, MoMo PSB.*

1.0 Introduction

The rapid digital transformation of Nigeria's financial sector has positioned payment service banks (PSBs) as crucial vehicles for advancing financial inclusion, particularly among rural and underserved populations. MoMo Payment Service Bank (PSB), launched in 2022 as a subsidiary of MTN Nigeria, emerged as a significant player in this landscape, leveraging MTN's extensive telecommunications infrastructure to deliver mobile-based financial services. However, within days of its launch, the platform experienced a devastating cybersecurity breach resulting in approximately ₦22.3 billion ($53 million) in unauthorised transfers through 700,000 transactions to 8,000 accounts across 18 commercial banks (Quartz Africa, 2022). This incident represents one of the most significant cybersecurity breaches in Nigeria's fintech history and offers critical insights into the vulnerabilities of emerging digital financial ecosystems.

The digital financial services sector in Nigeria has experienced exponential growth, driven by increasing mobile penetration and regulatory initiatives aimed at expanding financial inclusion. Payment service banks were established by

*Corresponding author: **Iyanu Emmanuel Olatunbosun**

the Central Bank of Nigeria (CBN) to leverage telecommunications infrastructure and agent networks to serve populations traditionally excluded from formal banking (TechCabal, 2025). MoMo PSB launched with ambitious plans to capitalize on MTN Nigeria's extensive subscriber base of over 70 million users, positioning itself as a catalyst for financial inclusion while potentially challenging traditional banks and fintech companies in the payment processing space (RegTech Africa, 2024).

The timing and scale of the MoMo PSB breach magnified its significance within Nigeria's cybersecurity landscape. Occurring just days after the service's highly publicised launch, the incident exposed critical vulnerabilities in a system designed to handle sensitive financial data and transactions. According to Quartz Africa, the breach involved unauthorised access to a settlement account held at First Bank, one of Nigeria's oldest and largest financial institutions (Quartz Africa, 2022). The sophistication of the attack, coordinated across multiple banking institutions, suggested significant planning and possibly insider knowledge, raising questions about the security frameworks governing interbank transactions and settlement processes in Nigeria.

The broader context of cybersecurity in Nigeria reveals systemic challenges that transcend the MoMo PSB incident. As Olumofin (2024) notes in a comprehensive literature review, "Cybersecurity is a serious issue in Nigeria, and there is no improvement of the laws guarding Cybercrime as it is still rampant in the country and around the globe" (Olumofin, 2024). This assessment highlights the regulatory and institutional challenges that provided the backdrop for the MoMo PSB breach. Meanwhile, the Nigeria Data Protection Commission (NDPC) has intensified its scrutiny of data controllers and processors, particularly in the financial and telecommunications sectors, initiating investigations into numerous organisations for potential privacy violations (Okafor, et al. 2025).

Despite efforts by regulatory bodies such as the Nigeria Data Protection Commission (NDPC) and the Central Bank of Nigeria (CBN), systemic weaknesses remain. The breach highlights the importance of integrated frameworks that combine technological resilience and institutional trust to maintain the credibility of digital finance.

This paper, therefore investigates:

1. How Nigerian financial institutions respond organizationally to cybersecurity breaches.
2. How regulatory and policy frameworks adapt post-incident.
3. How user trust develops after a high-profile cyber incident.

This research article examines the cybersecurity implications of the MoMo PSB breach through a multidimensional analytical framework focusing on organisational responses, policy adaptation, and user trust. By synthesising evidence from diverse sources, including regulatory findings, corporate statements, and industry analysis, this study aims to contribute to a more comprehensive understanding of cybersecurity challenges in emerging digital financial ecosystems. The analysis offers insights relevant to policymakers, financial institutions, telecommunications providers, and cybersecurity practitioners seeking to strengthen the resilience of digital financial services against evolving threats.

2.0 Literature Review

2.1 Cybersecurity Landscape in Nigeria

The cybersecurity environment in Nigeria reflects the complex interplay of technological advancement, regulatory evolution, and persistent criminal threats. Olumofin's (2024) literature review provides a comprehensive assessment of the Nigerian cybersecurity landscape, noting that cybercrime remains rampant despite legislative efforts to combat it (S. Okafor & Lilian, 2022; Olumofin, 2024). The study identifies limited public awareness, insufficient cybersecurity education, and structural vulnerabilities in critical information infrastructure as fundamental challenges. Olumofin recommends "the introduction of standardised computer learning in schools, thereby reducing the vulnerability of computer illiterates" (Okafor, 2025; Olumofin, 2024), highlighting the educational dimension of cybersecurity capacity building.

The financial impact of cybercrime in Nigeria has shown a disturbing upward trajectory, with reported incidents increasing in both frequency and sophistication. According to Quartz Africa, Nigerian banks lost approximately ₦3.5 billion (about $9 million) to fraud between July and September 2020 alone, representing a 534% increase compared to the same period in 2019 (Quartz Africa, 2022). This trend underscores the economic significance of cybersecurity breaches and their potential impact on financial stability. The MoMo PSB breach, estimated at ₦22.3 billion, therefore represents an extreme manifestation of a broader pattern of financial cybercrime in Nigeria.

The regulatory framework for cybersecurity and data protection in Nigeria has evolved significantly in recent years. The establishment of the Nigeria Data Protection Commission (NDPC) in 2022 represented a major institutional advancement, creating a dedicated regulator with authority to investigate data privacy violations and impose penalties. The NDPC has signalled its intent to "ramp up enforcement efforts in 2024, evidenced by the issuance of a Code of Conduct for Data Protection Compliance Organisations (DPCOs) earlier in the year" (IT Edge News, 2024). This regulatory strengthening occurred alongside ongoing investigations into "over 110 data controllers and data processors

for various degrees of data privacy and protection breaches, particularly in the financial, telecom, gaming, and online lending industries" (IT Edge News, 2024).

2.2 Mobile Money Security in Developing Economies

The security of mobile money platforms represents a distinct subset of cybersecurity literature, particularly in developing economies where these services often reach populations with limited prior exposure to formal financial services. The structural characteristics of mobile money systems, including reliance on mobile networks, integration with banking infrastructure, and dependence on agent networks, create unique vulnerability profiles. In the Nigerian context, PSBs face particular security challenges due to their mandate to "offer deposits and withdrawals, and cross-border remittances" while operating under restrictions that prohibit them from offering "loans, forex services, or invest beyond government-approved securities" (TechCabal, 2025).

The agent network model prevalent in mobile money ecosystems introduces distinctive security considerations. According to TechCabal, "In Nigeria, mobile money adoption is primarily driven by banking agents due to poor internet connectivity and low smartphone penetration" (TechCabal, 2025). This reliance on human intermediaries creates potential vulnerabilities, including social engineering attacks, identity fraud, and agent misconduct. The security implications of this model are reflected in MoMo PSB's strategic shift following the breach, which involved "deliberately reducing its reliance on agents and merchants, many of whom engage in transactions solely for commissions" (TechCabal, 2025).

2.3 Organisational Response to Cybersecurity Incidents

The literature on organisational response to cybersecurity incidents emphasises the importance of rapid containment, transparent communication, and comprehensive remediation. MTN Group's response to the April 2025 cybersecurity incident, which the company described as resulting in "unauthorised access to personal information of some MTN customers in certain markets" (MTN Group, 2025) exemplifies standard crisis response protocols, including immediate engagement with law enforcement agencies. The company's statement that it "immediately activated its cybersecurity response processes including informing the South African Police Service (SAPS) and the Hawks in South Africa" (MTN Group, 2025) reflects established best practices in incident response.

The concept of cyber resilience has emerged as a critical framework for understanding organisational capacity to withstand and recover from cybersecurity incidents. As emphasised by participants at a Nigerian cybersecurity workshop, "cyber resilience is a shared responsibility requiring coordinated action from all. We cannot afford to operate in silos; a unified, ecosystem-driven approach is the only way forward in today's threat landscape" (Babcock University, 2025). This perspective highlights the interconnected nature of cybersecurity in digital financial ecosystems and the limitations of organisation-centric security approaches.

2.4 Theoretical Framework: Institutional Trust in Digital Financial Services

This research draws on institutional trust theory to examine the relationship between cybersecurity incidents and user confidence in digital financial services. The conceptual underpinnings of institutional trust emphasise the role of perceived competence, integrity, and benevolence in shaping user attitudes toward financial institutions. The MoMo PSB breach potentially compromised all three dimensions of trust: competence through the technical failure that permitted unauthorised transfers; integrity through questions about data governance practices; and benevolence through communication strategies following the incident.

The empirical evidence from MoMo PSB's user trends following the breach provides insights into the trust implications of cybersecurity incidents. According to TechCabal, "the number of active wallets fell to 2.8 million, and cash deposits from wallet users dropped by half, from ₦7.6 billion to ₦3.8 billion" in 2024 (TechCabal, 2025). This decline occurred alongside substantial reductions in the platform's agent and merchant networks, suggesting broader reputational damage beyond immediate financial losses.

Table 1: Theoretical Framework of Institutional Trust in Digital Financial Services

Trust Dimension	Definition	Potential Impact of Breach	Evident in MoMo PSB Case
Competence Trust	Perception of technical capability and reliability	Undermined by security vulnerabilities	Unauthorized access to settlement accounts
Integrity Trust	Belief in organizational honesty and ethical principles	Compromised by insufficient safeguards	NDPC investigation into data handling practices
Benevolence Trust	Perception that institution acts in users' best interests	Weakened by communication failures	Decline in active users and transaction volumes

3.0 Methodology

This research employs a systematic literature review to analyse secondary data on the MoMo PSB cybersecurity breach and its implications. The approach follows established guidelines for systematic reviews in cybersecurity research, emphasising transparent search strategies, explicit inclusion criteria, and systematic data extraction and synthesis procedures.

3.1 Data Collection and Sources

The study utilised a comprehensive search strategy to identify relevant secondary data sources, including academic publications, corporate reports, regulatory filings, media accounts, and industry analyses. Search criteria focused on documents referencing MoMo PSB, MTN Nigeria cybersecurity incidents, payment service bank regulations, and related cybersecurity developments in Nigeria. The temporal scope encompassed materials published between 2022 (when MoMo PSB launched) and 2025 to capture evolving developments and responses.

The final source portfolio included seven primary references representing diverse perspectives on the breach and its aftermath: MTN Group's official incident statement (MTN Group, 2025); reports on Nigeria's broader cybersecurity context (Babcock University, 2025); analysis of MoMo PSB's strategic response (TechCabal, 2025); detailed accounts of the breach mechanics (Quartz Africa, 2022); reports on regulatory investigations (IT Edge News, 2024); information about MTN's fintech expansion plans (RegTech Africa, 2024); and academic research on Nigerian cybersecurity (Olumofin, 2024). These sources provided complementary viewpoints enabling triangulation of key findings.

3.2 Data Analysis

The data analysis followed a thematic synthesis approach comprising three primary phases: initial coding of source materials, theme development through iterative categorization, and synthesis of patterns across sources. The coding framework focused on identifying information related to organisational response strategies, regulatory actions, technical security measures, user behaviour changes, and strategic business adaptations.

Analytical techniques included content analysis of corporate and regulatory communications to identify framing strategies and priority issues; comparative analysis of pre- and post-breach business metrics; and pattern matching between incident characteristics and response initiatives. The analysis paid particular attention to discrepancies between different accounts of the breach's scale and impact, using these variations to identify areas of contested narrative or information asymmetry.

3.3 Design and Approach

A Systematic Literature Review (SLR) adhering to PRISMA 2020 guidelines was conducted. Data sources included *Scopus*, *ScienceDirect*, *Google Scholar*, *Quartz Africa*, *Reuters*, *CBN* circulars, and *NDPC* reports (2022–2025).

3.4 Inclusion and Exclusion Criteria

Inclusion	Exclusion
English-language studies (2022–2025)	Non-English materials
Academic and credible institutional sources	Opinion pieces lacking evidence
Focus on fintech, cybersecurity, or digital-trust issues	Purely technical encryption studies

3.5 Screening Process:

Out of 120 records identified, 96 remained after duplicates were removed. After full-text screening, 45 met quality and relevance criteria.

Figure 2. PRISMA Flow Diagram:

Identification → Screening → Eligibility → Inclusion (45 studies included).

3.6 Data Analysis:

NVivo 12 Plus was used for open coding, producing 78 codes aggregated into three major themes:

1. Organisational Response,
2. Policy and Regulatory Adaptation,
3. User Trust and Perception.

Inter-coder reliability achieved **Cohen's κ = 0.83**.

3.7 Ethical Considerations and Limitations

The use of secondary data in this research presents specific ethical considerations, particularly regarding the representation of sensitive financial information and allegations of regulatory non-compliance. The study addressed these concerns through rigorous source verification, contextual interpretation of disputed claims, and transparent acknowledgement of information limitations.

The research acknowledges several methodological limitations. First, the reliance on publicly available information necessarily excludes confidential operational details that might provide additional insights into the breach's causes and containment. Second, the potential for strategic representation in corporate and regulatory communications necessitates cautious interpretation of official accounts. Third, the dynamic nature of the cybersecurity threat landscape means that subsequent developments may render specific findings less relevant. Despite these limitations, the systematic analysis of available secondary data provides valuable insights into the complex interplay of technological vulnerability, organisational response, and regulatory oversight in digital financial services.

4.0 Summary of Findings:

4.1 The MoMo PSB Breach: Incident Analysis and Immediate Aftermath

The cybersecurity breach affecting MoMo Payment Service Bank in May 2022 represents one of the most significant security incidents in Nigeria's fintech history. Analysis of multiple sources reveals a complex attack vector involving unauthorised access to settlement accounts and coordinated transfers across the banking system. According to Quartz Africa, "MoMo PSB lost $53 million following 700,000 unauthorised transfers to about 8,000 accounts in 18 Nigerian commercial banks" (Quartz Africa, 2022). The scale and coordination of these transactions suggest sophisticated understanding of interbank settlement processes, potentially indicating insider knowledge or extensive reconnaissance.

The temporal aspect of the attack heightened its impact, occurring within days of MoMo PSB's official launch. This timing suggests the perpetrators may have exploited vulnerabilities in initial operational procedures or targeted the platform during its most vulnerable phase. A senior banking official quoted by Quartz Africa indicated that the breach's scale might have been broader than officially acknowledged, with an "initial loss from the error was N36 billion ($86 million) but some banks returned N14 billion within days" (Quartz Africa, 2022). This discrepancy between initial and final loss figures highlights challenges in incident assessment during active cybersecurity crises.

The technical response to the breach included suspending services immediately and attempting to reverse transactions. MoMo PSB's CEO Usoro Usoro stated that the company had "worked with relevant stakeholders to reverse the vast majority of those wrong transactions, whilst through the legal processes we are working to reverse the remaining" (Quartz Africa, 2022). This containment approach prioritised financial recovery while maintaining service integrity, though the temporary service suspension inevitably disrupted user access and potentially eroded confidence in platform reliability.

Table 2: Chronology of MoMo PSB Security Incidents and Responses

Date	Event	Key Developments	Public Communication
May 2022	Initial security breach	Unauthorised transfers from settlement accounts; estimated ₦22.3 billion loss	Limited initial disclosure; emphasis on service restoration
May 2022	Immediate response	Service suspension; transaction reversal efforts; engagement with banks	Statement emphasizing customer fund security
2023 - 2024	Strategic reassessment	Agent network reduction; digital banking investment; license applications	Framing as strategic shift rather than security response
April 2025	MTN Group incident	Unauthorized access to customer information in "certain markets"	Comprehensive disclosure with cybersecurity recommendations
2024-2025	Regulatory investigations	NDPC probe into data protection compliance; expanded industry scrutiny	Regulatory emphasis on accountability and compliance

4.2 Organizational Response and Strategic Adaptation

MTN Group and MoMo PSB implemented a multi-layered response strategy addressing immediate security concerns while initiating longer-term structural adaptations. The initial crisis management approach emphasized service integrity and financial remediation, with the company noting it had worked to reverse "the vast majority of those wrong transactions" while pursuing legal processes for recovery of remaining funds (Quartz Africa, 2022). This financial recovery focus represented the first phase of organizational response, prioritizing stabilization of the platform's economic position.

The strategic reorientation at MoMo PSB following the breach reflected fundamental reassessment of the platform's operational model. According to TechCabal, the company implemented significant reductions in its agent and merchant networks, with agents declining by 79.2% to 68,016 and merchants shrinking by 76.8% to 75,168 during 2024 (TechCabal, 2025). This substantial network restructuring aligned with what industry expert Victor Asemota characterized as "deliberately reducing its reliance on agents and merchants, many of whom engage in transactions solely for commissions" (TechCabal, 2025). The strategic shift also addressed potential security vulnerabilities associated with extensive agent networks.

The technological enhancement component of MoMo PSB's response included application for additional regulatory licenses to strengthen security capabilities. By applying for Payment Service Solutions Provider (PSSP) and Payment Terminal Service Provider (PTSP) licenses, the company sought to "process payments in-house: minimizing dependence on external providers, streamlining operations, and enhancing service delivery" (RegTech Africa, 2024). This vertical integration strategy aimed to reduce vulnerability points in the payment processing chain while increasing direct control over security protocols.

The broader organizational response extended beyond MoMo PSB to include MTN Group's cybersecurity posture. The April 2025 cybersecurity incident disclosure by MTN Group emphasised that there was "no evidence of compromise to any of our critical infrastructure, core MTN platforms or services" (MTN Group, 2025), suggesting organisational efforts to distinguish between different levels of security vulnerability. MTN's communication strategy included detailed customer security recommendations, including placing fraud alerts, using strong passwords, and activating multifactor authentication (MTN Group, 2025), representing proactive trust-building through security education.

4.3 Policy and Regulatory Adaptation

The regulatory response to the MoMo PSB breach reflected growing institutional capacity in Nigeria's data protection and cybersecurity governance. The Nigeria Data Protection Commission (NDPC) initiated investigations into "alleged data privacy breaches involving MTN's MoMo Payment Service Bank" (IT Edge News, 2024), signaling regulatory attention to potential compliance failures. The investigation scope included "suspected misuse of customer data, involving the unauthorized use of such data without proper consent, thereby violating user privacy rights and trust" (IT Edge News, 2024), indicating concern beyond immediate financial losses to encompass broader data governance issues.

The systemic nature of regulatory scrutiny expanded following the MoMo PSB incident, with the NDPC reportedly widening "their scope of inquiry to include approximately 150 other organisations" (IT Edge News, 2024). This broadening investigation reflected recognition of industry-wide vulnerabilities rather than isolated compliance failures. The Commission's approach aligned with previously expressed concerns by NDPC National Commissioner Dr. Vincent Olatunji regarding "the compliance of many financial and telecom companies with data privacy laws" and ongoing investigations into "over 110 data controllers and data processors for various degrees of data privacy and protection breaches" (IT Edge News, 2024).

The policy discourse surrounding cybersecurity in Nigeria intensified following the MoMo PSB breach, with stakeholders emphasizing collaborative approaches to ecosystem resilience. At a cybersecurity workshop hosted by Babcock University, Chairman of the Senate Committee on ICT and Cybersecurity Honourable Shuaib Afolabi Salisu "emphasized the need for a tripartite collaboration involving the academia, industry, and government agencies to develop a robust cybersecurity ecosystem" (Babcock University, 2025). This perspective reflected growing recognition of the interconnected nature of cybersecurity challenges in digital financial services.

The regulatory framework for payment service banks itself underwent reassessment following the breach, with attention to the specific security challenges facing non-bank financial services providers. The PSB licensing model inherently created security complexities through its integration of telecommunications infrastructure with financial services, operational requirements in rural areas with limited digital infrastructure, and restrictions that limited revenue diversification potential (TechCabal, 2025). These structural characteristics necessarily influenced the security options available to PSBs and potentially created distinctive vulnerability profiles compared to traditional financial institutions.

4.4 User Trust and Market Response

The impact of the MoMo PSB breach on user trust manifested through measurable changes in platform adoption and usage patterns. According to TechCabal analysis, MoMo PSB experienced significant declines in key performance metrics following the security incident, with "active mobile money wallets fell to 2.8 million, and cash deposits from wallet users dropped by half, from ₦7.6 billion to ₦3.8 billion" in 2024 (TechCabal, 2025). This reduction in active users and transaction values suggests erosion of confidence in the platform's security and reliability.

The behavioral response extended beyond individual users to include platform intermediaries, with the agent network declining by 79.2% to 68,016 agents and merchants shrinking by 76.8% to 75,168 during the same period (TechCabal,

2025). This contraction in the distribution network reflected both strategic decisions by MoMo PSB and potentially diminished economic viability for agents operating in a post-breach environment. Industry interpretation of these trends varied, with CEO Karl Toriola framing them as part of "a strategic shift to enhance service penetration, boost monetisation, and lower customer acquisition costs" (TechCabal, 2025) rather than primarily trust-related phenomena.

The competitive context of the breach influenced its market impact, as MoMo PSB operated in an increasingly crowded fintech landscape. TechCabal noted that "PSBs have struggled to gain the same market traction as fintech giants like Opay, Moniepoint, and Palmpay, which have onboarded millions of users" (TechCabal, 2025). This competitive pressure potentially amplified the trust implications of the breach, as users and agents had alternative platforms available rather than returning to MoMo PSB following security remediation.

The longitudinal perspective on user trust suggests complex recovery patterns rather than simple linear restoration. While MTN Nigeria continued to express confidence in MoMo PSB's strategic position, envisioning it as "the top fintech platform in Nigeria, aiming to attract 30-40 million active users by 2025" (RegTech Africa, 2024), the platform's progress toward these targets necessarily occurred in the shadow of the breach's trust implications. The company's ongoing investment in the platform, including additional ₦9.4 billion capital injection in 2024 (TechCabal, 2025), signaled organizational commitment to overcoming trust challenges through sustained resource allocation.

Table 3: Impact of Cybersecurity Breach on MoMo PSB Key Performance Indicators

Performance Indicator	Pre-Breach (2023)	Post-Breach (2024)	Percentage Change	Interpretation
Active Wallets	5.3 million	2.8 million	-46%	Significant user attrition following breach
Cash Deposits	₦7.6 billion	₦3.8 billion	-50%	Reduced user confidence in platform security
Agent Network	327,000	68,016	-79.2%	Strategic restructuring and trust implications
Merchant Network	324,000	75,168	-76.8%	Reassessment of commercial viability
Transaction Volume	Not specified	Increased by 4.3%	+4.3%	Possible indicator of engaged user retention

5.0 Discussion

5.1 Theoretical Implications: Cybersecurity and Institutional Trust

The MoMo PSB case offers several theoretical contributions to understanding the relationship between cybersecurity incidents and institutional trust in digital financial services. The decline in active users and transaction values following the breach supports predictions from institutional trust theory regarding the sensitivity of user confidence to perceived competence failures. However, the simultaneous increase in transaction volume among remaining users (TechCabal, 2025) suggests more complex trust dynamics than straightforward abandonment, potentially indicating differentiated response patterns across user segments.

The theoretical framework of institutional trust requires refinement to account for the distinctive characteristics of digital financial services in emerging markets. Unlike traditional banking relationships characterised by personal interaction and established institutional histories, mobile money platforms often operate with limited interpersonal contact and relatively brief organisational track records. This context may amplify the trust implications of cybersecurity incidents while simultaneously creating opportunities for more rapid trust restoration through demonstrated technical competence.

The multi-dimensional nature of trust repair emerges clearly from the MoMo PSB case, with organizational responses addressing technical competence through system enhancements, integrity through compliance efforts, and benevolence through customer protection measures. The company's communication strategy, following subsequent security incidents, emphasises transparency and provides detailed security guidance (MTN Group, 2025), suggesting organisational learning regarding the trust implications of cybersecurity management.

5.2 Policy and Regulatory Implications

The regulatory response to the MoMo PSB breach highlights the evolutionary challenges in governing convergent digital financial services that span telecommunications and banking sectors. The Nigeria Data Protection Commission's investigation into "suspected misuse of customer data" and "inadequate consent practices" (IT Edge News, 2024) reflects appropriate regulatory attention to data governance dimensions beyond immediate financial losses. This comprehensive approach acknowledges the interconnected nature of data protection, financial regulation, and cybersecurity in digital financial services.

The systemic regulatory approach evidenced by the NDPC's expansion of investigations to approximately 150 other organisations (IT Edge News, 2024) represents constructive regulatory learning from individual incidents to address industry-wide vulnerabilities. This scaling from specific breach to general compliance reinforcement demonstrates adaptive regulatory capacity essential for keeping pace with technological evolution in financial services. The emphasis on ecosystem resilience rather than isolated compliance aligns with academic recommendations for "a unified, ecosystem-driven approach" to cybersecurity (Babcock University, 2025).

The policy emphasis on collaborative security frameworks emerging from cybersecurity workshops and regulatory statements suggests recognition of the distributed responsibility for cybersecurity in interconnected digital ecosystems. As expressed by Oluwafemi Aminu, Executive Director of Momo PSB, "cyber resilience is a shared responsibility requiring coordinated action from all. We cannot afford to operate in silos" (Babcock University, 2025). This perspective challenges traditional organization-centric security models and suggests need for innovative governance mechanisms that match the interconnected nature of digital financial services.

5.3 Organizational Strategy and Cybersecurity Management

The MoMo PSB case demonstrates the strategic significance of cybersecurity management beyond technical compliance functions. The breach triggered substantial strategic reorientation, including network restructuring, operational model refinement, and technological enhancement through license applications (RegTech Africa, 2024; TechCabal, 2025). This strategic response reflects an understanding of cybersecurity as a business imperative rather than a technical speciality, with implications for organisational structure and leadership engagement in security governance.

The resource allocation decisions following the breach illustrate the economic significance of cybersecurity failures in digital financial services. MTN Nigeria's additional investment of ₦9.4 billion in MoMo PSB following the breach (TechCabal, 2025) represents a substantial financial commitment to strategic recovery, exceeding the immediate financial losses from unauthorised transfers. This investment pattern underscores the broader business impact of security incidents beyond direct financial losses to include reputational damage, strategic constraint, and recovery costs.

The competitive implications of cybersecurity management emerge from the MoMo PSB case, where the platform struggled to achieve market traction comparable to that of fintech competitors (TechCabal, 2025) following the breach. This competitive dynamic suggests potential market discipline through user migration following security incidents, creating economic incentives for security investment independent of regulatory requirements. However, the case also demonstrates the challenge of rebuilding market position once trust has been compromised, even with substantial resource allocation.

6.0 Conclusion

The cybersecurity breach at MoMo Payment Service Bank represents a significant case study in the challenges of securing digital financial services in emerging markets. The incident demonstrates the vulnerability of interconnected financial ecosystems to sophisticated attacks, the complex trust implications of security failures, and the multi-layered response strategies required for effective crisis management and recovery. The analysis offers several key insights for researchers, practitioners, and policymakers engaged with cybersecurity in digital financial services.

6.1 Theoretical and Practical Contributions

This research contributes to the theoretical understanding of institutional trust dynamics in digital financial services, particularly the differentiated response patterns across user segments following security incidents. The coexistence of user attrition with increased transaction volume among remaining users suggests complex trust repair processes rather than straightforward relationship termination. This insight enriches institutional trust theory by highlighting the need for segment-specific approaches to trust restoration in digital financial services.

The study offers practical insights regarding organisational cybersecurity strategy in interconnected financial ecosystems. The MoMo PSB case demonstrates the limitations of organisation-centric security approaches when financial transactions span multiple institutions through settlement systems. The case underscores the necessity of collaborative security frameworks that address vulnerabilities across organisational boundaries, particularly in systems integrating telecommunications infrastructure with financial services.

6.3 Policy Implications

The research identifies several policy implications for regulatory governance of digital financial services. The Nigeria Data Protection Commission's expansion from specific investigation to industry-wide compliance reinforcement represents promising approach to regulatory learning and adaptation. This scalable regulatory response matches the systemic nature of cybersecurity vulnerabilities in interconnected financial ecosystems and offers model for efficient regulatory resource allocation.

The findings also suggest need for regulatory frameworks that address the distinctive characteristics of payment service banks, particularly their integration of telecommunications and financial services, operational requirements in underserved areas, and business model constraints. These structural factors create distinctive security challenges that may require tailored regulatory approaches rather than simple extension of traditional banking regulations.

6.4 Limitations and Future Research

This research acknowledges several methodological limitations that suggest directions for future investigation. The reliance on publicly available secondary data necessarily excludes confidential operational details that might provide additional insights into breach causation and response strategies. Future research incorporating confidential regulatory findings or organizational post-incident reviews would enrich understanding of cybersecurity management in digital financial services.

The temporal scope of this study necessarily excludes longer-term developments in MoMo PSB's security posture and market position. Longitudinal tracking of the platform's recovery trajectory would provide valuable insights into the extended process of trust restoration following major security incidents. Similarly, a comparative analysis of cybersecurity approaches across different payment service banks would help identify industry-wide patterns versus organisation-specific practices.

The conceptual framework employed in this study focuses primarily on organisational response, policy adaptation, and user trust. Future research might expand this conceptualisation to include additional dimensions such as employee experience, competitor responses, or international comparative analysis. Such expanded analytical frameworks would further enrich the understanding of cybersecurity challenges in emerging digital financial ecosystems.

Despite these limitations, this research provides a comprehensive analysis of the MoMo PSB cybersecurity breach and its implications for organisational strategy, regulatory policy, and user trust. The case offers valuable lessons for stakeholders across digital financial ecosystems seeking to strengthen cybersecurity resilience while advancing financial inclusion objectives in emerging markets.

References

1. Babcock University. (2025). Experts call for strengthening Nigeria's cybersecurity. *Babcock University*. https://www.babcock.edu.ng/news/experts-call-for-strengthening-nigerias-cybersecurity
2. IT Edge News. (2024). NDPC probes MTN's MoMo PSB over privacy breach. *IT Edge News*. https://www.itedgenews.africa/ndpc-probes-mtns-momo-psb-over-privacy-breach/
3. MTN Group. (2025). MTN cybersecurity incident, but critical infrastructure secure. *MTN Group*. https://www.mtn.com/mtn-cybersecurity-incident-but-critical-infrastructure-secure/
4. Okafor, S., & Lilian, U. C. (2022). Financial deepening and economic growth in Nigeria: Evidence from 1982–2019. *International Journal of Innovation in Engineering, 2*(3), 23–28. https://doi.org/10.59615/ijie.2.3.23
5. Okafor, S. O. (2025). Using predictive analytics for credit risk evaluation in Nigerian microfinance organizations. *Global Journal of Applied, Management and Social Sciences, 33*, 21–32.
6. Okafor, S. O., Olalude, O. V., & Angelonu (Ejelonu), H. O. (2025). Impact of big data on accounting practices: Empirical evidence from Nigeria. *International Journal of Data Science and Big Data Analytics, 5*(1), 1–20. https://doi.org/10.51483/IJDSBDA.5.1.2025.1-20
7. Olumofin, O. (2024). Literature review on cybersecurity in Nigeria. *SSRN Electronic Journal.* https://doi.org/10.2139/ssrn.4850477
8. Quartz Africa. (2022). MTN's mobile money push into Nigeria was hacked for millions within days. *Quartz Africa*. https://qz.com/africa/2183438/mtn-nigerias-momo-psb-is-suing-banks-after-53-million-breach
9. RegTech Africa. (2024). MTN Nigeria strengthens fintech presence with application for new licenses for MoMo PSB. *RegTech Africa*. https://regtechafrica.com/nigeria-mtn-nigeria-strengthens-fintech-presence-with-application-for-new-licenses-for-momo-psb/
10. TechCabal. (2025). MoMo PSB resets strategy as active wallet users decline by 46%. *TechCabal*. https://techcabal.com/2025/03/05/mtns-momo-psb-resets-strategy/

CITATION
Olatunbosun, I. E. (2025). Cybersecurity Implications of Nigeria's Momo PSB Breach: Organizational Responses, Policy Adaptation and User Trust. In Global Journal of Research in Engineering & Computer Sciences (Vol. 5, Number 6, pp. 1–9). https://doi.org/10.5281/zenodo.17574348