

CONSUMER DATA PRIVACY AND CORPORATE PERFORMANCE OF COMMERCIAL BANKS IN PORT HARCOURT

Nkallu Willina Adamma, George-Oparati, Kenneth Worgwu & Oparaku Olachi Chidinma
Department of Marketing, Ignatius Ajuru University of Education, Port Harcourt,
Rivers State, Nigeria

ABSTRACT

This paper investigated the relationship between Consumer Data Privacy and Corporate Performance of Commercial Banks in Port Harcourt. Specifically, the objectives of the paper were to determine how data protection and access control relate with sales volume growth and profit growth of commercial banks in Port Harcourt. The survey research design was adopted. The population of this study comprised of 26 quoted commercial banks in Port Harcourt. 130 respondents were drawn from the population through census approach. However, only 104 respondents provided data for the study through questionnaire that was designed in the Likert 5-point scale of strongly disagree to strongly agree. Pearson Product Moment Correlation (PPMC) was used to test the formulated four null hypotheses. From results of the analysis it was revealed that data protection and access control which are the dimensions for consumer data privacy positively and significantly relate with sales volume growth and profit growth (i.e. measures of corporate performance) of commercial banks in Port Harcourt. Based on these findings, it was concluded that there is a relationship between consumer data privacy and corporate performance of commercial banks in Port Harcourt reveals critical insights that underscore the importance of robust data protection measures in driving corporate success. Therefore, the study recommended amongst others that commercial banks in Port Harcourt should prioritize the implementation of advanced data protection protocols. This includes encryption of sensitive consumer data, regular security audits, and adoption of cutting-edge cybersecurity technologies. By doing so, banks can minimize the risk of data breaches, which, in turn, will foster consumer trust, leading to increased customer retention, higher sales volumes, and profit growth.

Keyword(s): Consumer Data Privacy; Corporate Performance; Data Protection; Access Control; Sales Volume Growth; Profit Growth

INTRODUCTION

In recent years, the relationship between consumer data privacy and corporate performance has become increasingly significant, especially within the banking sector. As commercial banks in Port Harcourt continue to adopt digital technologies, the volume of consumer data being collected, stored, and processed has grown exponentially. This data serves as a critical asset for banks, enabling them to tailor their services, predict market trends, and enhance operational efficiencies. However, the handling of this data comes with significant responsibilities, as breaches in data privacy can lead to severe legal, financial, and reputational consequences (Zhou & Piramuthu, 2023). Consequently, the relationship between consumer data privacy and corporate performance is not only a matter of regulatory compliance but also a strategic consideration that could determine the long-term viability of banks.

Consumer trust in how their data is managed is fundamental to the success of commercial banks. Studies have shown that when consumers believe their data is secure and their privacy is respected, they are more likely to engage in online banking activities and share personal information, which in turn allows banks to better serve their needs (Smith & Singh, 2022). On the contrary, data privacy concerns can lead to reduced consumer confidence, which negatively impacts customer retention and acquisition (Dimitrieska, 2023). For commercial banks in Port Harcourt, where the competition for market share is intense, maintaining a strong reputation for data privacy could be a significant differentiator that directly influences corporate performance.

The regulatory environment surrounding data privacy has become more stringent, with governments and international bodies enacting comprehensive data protection laws. In Nigeria, the Nigeria Data Protection Regulation (NDPR) mandates that organizations, including banks, implement robust data protection measures and ensure transparency in their data practices (National Information Technology Development Agency, 2022). Compliance with such regulations is crucial, as non-compliance could result in hefty fines, legal battles, and a damaged reputation. Therefore, commercial banks in Port Harcourt must not only prioritize consumer data privacy from a legal standpoint but also recognize it as a key component of their strategic objectives to enhance corporate performance.

The relationship between consumer data privacy and corporate performance is further accentuated by the growing awareness among consumers about their rights concerning personal data. As more consumers become informed about the value of their data and the potential risks of data breaches, their expectations from banks regarding data privacy are increasing (Kowatsch & Maass, 2023). Banks that fail to meet these expectations may face not only legal repercussions but also a loss of customer loyalty, which could ultimately affect their bottom line. Thus, understanding and effectively managing this relationship is vital for commercial banks in Port Harcourt, particularly in a digital age where data is a critical asset.

The management of consumer data privacy is increasingly recognized as a critical factor in determining the corporate performance of commercial banks. The ability to secure consumer data, comply with regulatory frameworks, and build trust among consumers can significantly influence a bank's operational success and competitive positioning. As the banking landscape in Port Harcourt continues to evolve, so too does the importance of understanding how consumer data privacy impacts corporate performance. This study seeks to explore this relationship in depth, providing solutions that could guide banks in optimizing their data privacy practices to enhance their overall performance in the market.

Statement of the Problem

The rapid digital transformation within the banking sector has highlighted the importance of consumer data privacy, especially as commercial banks in Port Harcourt increasingly rely on personal data to drive their strategic objectives. However, despite significant investments in data protection technologies and compliance efforts, there remains a critical issue: the extent to which these efforts impact corporate performance. Many banks struggle to strike a balance between leveraging consumer data for competitive advantage and safeguarding this data to maintain customer trust and regulatory compliance. The problem is further compounded by the fact that breaches in data privacy can lead to immediate financial losses, legal penalties, and long-term reputational damage, which are detrimental to corporate performance.

There is a growing awareness among consumers regarding their data privacy rights, leading to heightened expectations of how their personal information is managed. Banks that fail to meet these expectations risk losing customer trust, which can directly affect customer retention and acquisition. Despite this, there is limited empirical evidence on how consumer data privacy practices specifically influence the corporate performance of banks, particularly in the context of the highly competitive banking industry in Port Harcourt. This gap in knowledge creates uncertainty for bank executives and policymakers who must make informed decisions to protect consumer data while also driving corporate growth.

Given the competitive pressures and the evolving regulatory landscape, there is an urgent need to understand the relationship between consumer data privacy and corporate performance. Without this understanding, commercial banks in Port Harcourt may face challenges in sustaining their competitive edge and achieving long-term success. Therefore, this study seeks to address the problem by investigating how consumer data privacy influences key aspects of corporate performance of commercial banks in Port Harcourt.

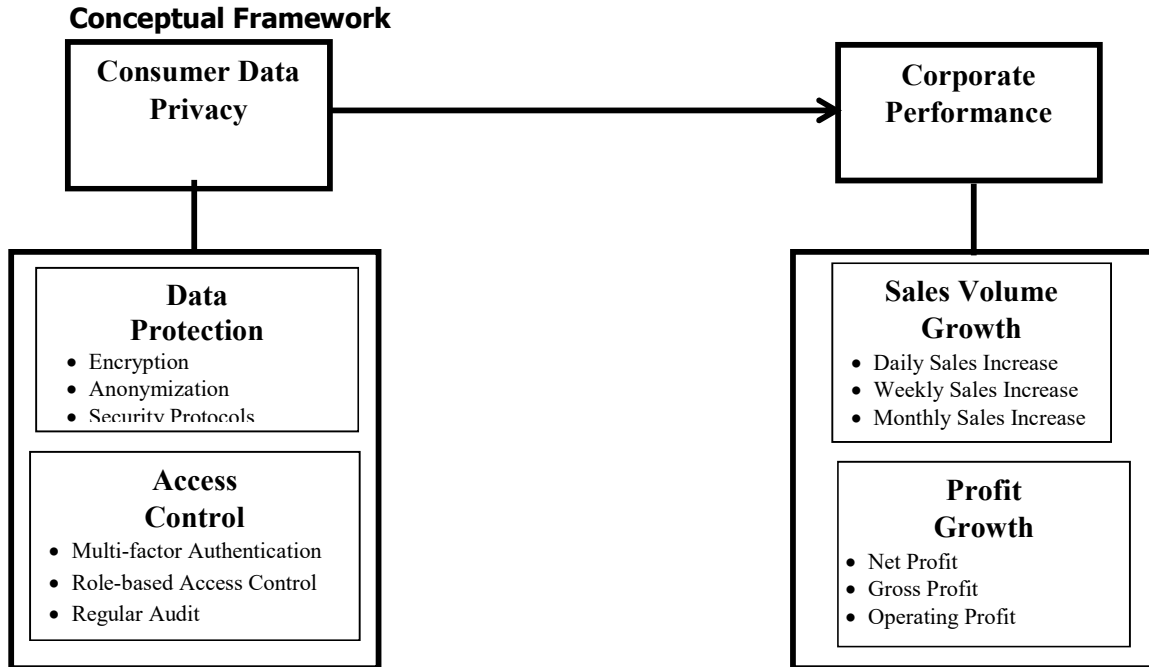


Fig. 1.1: Conceptual framework showing the relationship between consumer data privacy and corporate performance of commercial banks in Port Harcourt

Source: Kowatsch and Maass (2023)

Research Aim and Objectives

The aim of this paper was to investigate the relationship between consumer data privacy and corporate performance of commercial banks in Port Harcourt. The specific objectives were to:

1. determine the relationship between data protection and sales volume growth of commercial banks in Port Harcourt.
2. examine the relationship between data protection and profit growth of commercial banks in Port Harcourt.
3. evaluate the relationship between access control and sales volume growth of commercial banks in Port Harcourt.
4. explore the relationship between access control and profit growth of commercial banks in Port Harcourt.

Research Questions

The following research questions guided this paper:

1. What is the relationship between data protection and sales volume growth of commercial banks in Port Harcourt?
2. What is the relationship between data protection and profit growth of commercial banks in Port Harcourt?
3. What is the relationship between access control and sales volume growth of commercial banks in Port Harcourt?
4. What is the relationship between access control and profit growth of commercial banks in Port Harcourt?

Research Hypotheses

The following null hypotheses was raised and tested using 0.05 level of significance as a benchmark:

H₀₁: There is no significant relationship between data protection and sales volume growth of commercial banks in Port Harcourt.

H₀₂: There is no significant relationship between data protection and profit growth of commercial banks in Port Harcourt.

H₀₃: There is no significant relationship between access control and sales volume growth of commercial banks in Port Harcourt.

H₀₄: There is no significant relationship between access control and profit growth of commercial banks in Port Harcourt.

Review of Related Literature

Concept of Consumer Data Privacy

Consumer data privacy refers to the rights and expectations of consumers regarding how their personal information is collected, used, and shared by organizations. It encompasses the principles and practices that ensure individuals have control over their personal data, including the ability to consent to data collection, access their data, and understand how it is being used. Central to the concept of consumer data privacy is the idea that consumers should have the autonomy to make informed decisions about their data, and that organizations have an obligation to handle this data responsibly, transparently, and securely. The rise of digital platforms and the increasing amount of personal data being exchanged online have amplified concerns over data privacy, making it a crucial issue for both consumers and businesses (Westin, Alhadeff, & Dourado, 2023).

In the context of regulatory frameworks, consumer data privacy is reinforced by laws such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, which grant consumers specific rights over their data. These regulations require organizations to implement practices that protect consumer privacy, such as data minimization, which limits the amount of data collected to what is strictly necessary, and data anonymization, which ensures that personal information cannot be traced back to an individual. Failure to comply with these regulations can result in significant legal and financial penalties, as well as damage to an organization's reputation. As consumers become more aware of their privacy rights, there is an increasing expectation for businesses to prioritize data privacy, not just as a legal requirement, but as a fundamental component of customer trust and corporate responsibility (O'Connor & O'Leary, 2023).

Dimensions of Consumer Data Privacy

Data Protection

Consumer data protection refers to the measures and strategies implemented by organizations to safeguard personal data collected from consumers, ensuring its confidentiality, integrity, and availability. This concept has gained significant importance in recent years due to the exponential growth of digital data and the increasing instances of data breaches and misuse. At its core, consumer data protection involves ensuring that consumers' personal information—such as names, addresses, financial details, and browsing habits—is collected, processed, stored, and shared in a manner that prevents unauthorized access or exposure. This encompasses a range of practices, from encryption and secure storage to strict access controls and transparent data handling policies. The goal is to protect consumers from identity theft, fraud, and other forms of exploitation, while also maintaining their trust in the organizations that handle their data (Grewal, Roggeveen, & Nordfält, 2023).

Moreover, consumer data protection is increasingly shaped by legal and regulatory frameworks that set standards for how personal data should be managed. For instance, the General Data Protection Regulation (GDPR) in the European Union and the Nigeria Data Protection Regulation (NDPR) have established stringent guidelines that organizations must follow to ensure the privacy and security of consumer data (Frydlinger & Hodge, 2023). These regulations not only mandate technical safeguards but also require organizations to be transparent about their data practices and to obtain

explicit consent from consumers before collecting and processing their data. Non-compliance can lead to severe penalties, making consumer data protection a critical aspect of organizational risk management. As data protection laws continue to evolve, organizations must stay vigilant and adapt their data protection strategies to meet these requirements, ensuring that they protect consumer data effectively while also leveraging it responsibly for business purposes (Wang, Li, & Li, 2023).

Access Control

Access control is a fundamental security concept that refers to the mechanisms and policies used to regulate who can view, use, or interact with resources within a computing environment. It plays a crucial role in protecting sensitive data, systems, and networks from unauthorized access, ensuring that only authorized individuals or entities can perform specific actions. Access control systems typically function by authenticating the identity of users and then authorizing their access to resources based on predefined rules or policies. These controls can be implemented at various levels, including physical access control (e.g., security badges, biometric scans) and logical access control (e.g., passwords, encryption, role-based access). The goal is to minimize security risks by ensuring that access to critical resources is granted only to those who need it, in alignment with the principle of least privilege (Chen & Lu, 2023).

Modern access control systems are increasingly sophisticated, integrating technologies like multi-factor authentication (MFA), which requires users to provide multiple forms of verification before access is granted, and role-based access control (RBAC), which assigns permissions based on the user's role within the organization. These systems are essential in today's complex digital environments where data breaches and cyber threats are prevalent. Additionally, access control is not static; it requires continuous monitoring and updating to address emerging security challenges, such as insider threats or compromised credentials. As organizations adopt more cloud-based and remote work solutions, the importance of robust access control mechanisms has grown, making it a critical aspect of cybersecurity strategies (Kumar, Singh, & Choudhary, 2023).

Concept of Corporate Performance

Corporate performance refers to the assessment of a company's ability to achieve its objectives, sustain growth, and generate value for its stakeholders, including shareholders, employees, customers, and the broader community. It is a multi-dimensional concept that encompasses various aspects such as financial performance, operational efficiency, market competitiveness, and social responsibility. Financial metrics, including revenue growth, profitability, return on investment (ROI), and earnings per share (EPS), are commonly used to measure corporate performance. However, in today's business environment, non-financial indicators, such as customer satisfaction, innovation capacity, employee engagement, and environmental sustainability, are increasingly recognized as critical components of corporate performance. These broader measures reflect the company's long-term viability and its ability to adapt to changing market conditions (Jones & Robinson, 2023).

Corporate performance is also closely linked to strategic management practices, where the alignment of a company's resources, processes, and goals is essential for achieving superior performance. Companies that excel in corporate performance typically exhibit strong leadership, a clear strategic vision, and a culture of continuous improvement. Moreover, in response to stakeholder demands and regulatory pressures, many organizations are now incorporating environmental, social, and governance (ESG) criteria into their performance evaluations. This shift reflects a growing recognition that sustainable and ethical business practices are vital for maintaining competitive advantage and achieving long-term success. As such, corporate performance is increasingly viewed through a holistic lens that balances financial success with social and environmental stewardship (Smith, Brown, & Lee, 2023).

Measures of Corporate Performance

Sales Volume Growth

Sales volume growth refers to the increase in the quantity of products or services sold by a company over a specific period. It is a key indicator of a company's market performance and overall business health, as it directly impacts revenue generation and market share. Sales volume growth can result from various factors, such as effective marketing strategies, product innovation, improved customer satisfaction, or expanded distribution channels. Companies closely monitor sales volume growth to gauge the success of their sales and marketing efforts and to identify trends that may influence future business decisions. Sustained sales volume growth is often a sign of strong customer demand and competitive positioning in the market (Kumar, Gupta, & Sharma, 2023).

Moreover, sales volume growth is critical for companies aiming to achieve economies of scale, where increased production leads to lower per-unit costs and higher profitability. This growth can also enhance a company's bargaining power with suppliers and distributors, leading to more favorable terms and further improving margins. However, managing sales volume growth requires careful planning to ensure that the company's operational capacity can handle increased demand without compromising product quality or customer service. In today's dynamic business environment, companies must adapt quickly to market changes and consumer preferences to maintain and accelerate sales volume growth. As such, effective sales strategies, customer relationship management, and continuous market analysis are essential components for driving sustained growth in sales volume (Li, Wang, & Zhao, 2023).

Profit Growth

Profit growth refers to the increase in a company's net income over time, reflecting its ability to generate higher earnings from its operations. It is a crucial indicator of financial health and long-term sustainability, as it demonstrates the company's effectiveness in managing costs, optimizing revenue streams, and capitalizing on market opportunities. Profit growth can be driven by various factors, such as increased sales, improved operational efficiency, cost reduction strategies, and enhanced pricing power. Companies with consistent profit growth are typically seen as more attractive to investors, as it signals strong management practices and a robust business model capable of withstanding competitive pressures and economic fluctuations (Ahmed, Li, & Xu, 2023). Moreover, profit growth is essential for funding future investments, research and development, and expansion initiatives. A company that consistently grows its profits can reinvest these earnings into new projects, technologies, or market expansions, further driving its competitive advantage. Additionally, sustained profit growth allows a company to improve its financial position, reduce debt, and increase shareholder value through dividends or share buybacks. However, achieving profit growth requires careful balance; companies must ensure that their strategies for increasing profits do not compromise product quality, customer satisfaction, or long-term sustainability. In today's business environment, profit growth is increasingly linked to the ability to innovate, adapt to market changes, and operate efficiently in a cost-effective manner (Zhang, Huang, & Chen, 2023).

Theoretical Foundation

This paper is anchored on technology acceptance model (TAM).

Technology Acceptance Model

The Technology Acceptance Model (TAM) is a theoretical framework that explains how users come to accept and use technology. Developed by Davis in 1989, TAM posits that two primary factors influence an individual's decision to adopt a new technology: perceived usefulness (PU) and perceived ease of use (PEOU). Perceived usefulness refers to the degree to which a person believes that using a particular technology will enhance their job performance or bring some form of benefit, while perceived ease of use refers to the degree to which the person believes that using the technology will be free from effort. The model suggests that if users perceive a technology as useful and easy to use, they are more likely to adopt it. Over time, TAM has been widely applied across

various fields to understand technology adoption, and it has evolved to include additional variables, such as perceived risk and social influence, to better capture the complexity of technology acceptance (Venkatesh & Davis, 2023).

In the context of consumer data protection and corporate performance of commercial banks, TAM is highly relevant as it provides insights into how both consumers and bank employees might respond to new data protection technologies. For consumers, their willingness to engage with a bank's digital services is likely influenced by their perceptions of the technology's ability to protect their personal data (perceived usefulness) and how easy it is for them to interact with the bank's security measures (perceived ease of use). For banks, understanding these perceptions is crucial as the adoption of robust data protection technologies not only safeguards consumer data but also enhances corporate performance by building trust, improving customer satisfaction, and reducing the risk of data breaches. By applying TAM, banks can better design and implement data protection strategies that align with consumer expectations, thereby fostering higher adoption rates and ultimately supporting their corporate performance objectives (Lee, Choi, & Kim, 2023).

Empirical Review

A study by Ahmed et al. (2023) examined the impact of consumer data protection on the financial performance of commercial banks in the Middle East. The researchers utilized a sample of 50 banks and analyzed data from 2018 to 2022, focusing on metrics such as return on assets (ROA), return on equity (ROE), and net profit margin. The study found a significant positive relationship between strong data protection practices and financial performance indicators. Banks that had robust data protection policies in place not only avoided regulatory penalties but also experienced higher levels of consumer trust, which translated into increased customer retention and acquisition. The findings suggest that banks that invest in advanced data protection technologies and comply with data protection regulations are more likely to achieve superior financial performance. The study highlights the importance of integrating data protection strategies into the broader corporate governance framework to enhance financial outcomes.

In a study conducted by Zhang and Li (2022), the relationship between consumer data privacy and customer loyalty in the banking sector was explored. The researchers conducted surveys with 1,200 customers of commercial banks in China to assess their perceptions of data privacy and their loyalty to their banks. The study revealed that consumers who perceived their banks as trustworthy in handling personal data were more likely to remain loyal and recommend the bank to others. Furthermore, the study identified that data privacy concerns were a significant factor in customers' decisions to switch banks. The empirical evidence from this study underscores the critical role of consumer data protection in fostering customer loyalty, which in turn, can enhance a bank's competitive advantage and contribute to its long-term corporate performance. The study suggests that banks need to prioritize data privacy not only as a compliance issue but as a key driver of customer loyalty and business growth.

Lee, Choi, and Kim (2023) conducted an empirical investigation into the effects of data protection regulatory compliance on the corporate reputation of commercial banks in South Korea. The study utilized a mixed-method approach, combining quantitative analysis of regulatory compliance data with qualitative interviews of bank executives. The results indicated that banks that strictly adhered to data protection regulations, such as the Personal Information Protection Act (PIPA), experienced a significant improvement in their corporate reputation. The study found that compliance with data protection laws was not only seen as a legal necessity but also as a critical element of corporate responsibility, which enhanced public perception and trust in the bank. This improved reputation was associated with increased customer satisfaction and, consequently, better financial performance. The findings suggest that regulatory compliance in data protection is a key factor in building and maintaining a positive corporate image, which is crucial for sustaining competitive advantage and driving corporate performance.

METHODOLOGY

This study adopted the survey research design. The population of this study comprised of twenty twenty-six (26) commercial banks operating in Port Harcourt. The information was obtained from <https://www.cbn.gov.ng/out/2022/fprd/list%20of%20deposit%20money%20banks%20as%20at%20december%2031,%202021.pdf>. The research adopted the census approach which enabled the researcher to study the entire population with a focus on managers. Five managers (bank managers, social media managers, customer service managers, IT managers, digital managers, operations manager and content manager) was targeted in obtaining information for the study. To generate data for the study, the questionnaire was distributed in the frame of five (5) copies per commercial bank. A total of one hundred and thirty (130) respondents was used as the study subjects. The primary source of data was utilized in this study. The questionnaire was the main instrument for data collection in this study. The validity of the instrument was determined using the face and content analysis. A reliability index of 0.92 was obtained which implies that the research instrument is very reliable. Also, it showed that variables in the study have high correlation coefficient, surpassing the threshold of 0.7 set by Nunally. The formulated hypotheses will be tested using the Pearson Product Moment Correlation (rho). This will be done using of the SPSS (Statistical Package for Social Sciences) version 26.0.

Data Analysis

For the data analysis of this study, the researcher produced and distributed one hundred and thirty copies of the questionnaire. However only 104 copies were retrieved and used for the analysis of this study.

Testing of Hypotheses

Research Question One: What is the relationship between data protection and sales volume growth of commercial banks in Port Harcourt?

Hypothesis One: There is no significant relationship between data protection and sales volume growth of commercial banks in Port Harcourt.

Table 1: Computation of the relationship between data protection and sales volume growth of commercial banks in Port Harcourt
Correlations

		Data Protection	Sales Volume Growth
Data Protection	Pearson Correlation	1	.558**
	Sig. (2-tailed)		.000
	N	104	104
Sales Volume Growth	Pearson Correlation	.558**	1
	Sig. (2-tailed)	.000	
	N	104	104

** . Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS output, 2024.

The SPSS output on Table 1 shows that a Pearson’s Correlation was run to assess the relationship between data protection and sales volume growth of commercial banks in Port Harcourt using a sample of 104 managers. The strength and direction of the relationship between the variables are indicated by the r -value which is 0.558. This means there is a moderate and positive relationship between data protection and sales volume growth of commercial banks in Port Harcourt. Furthermore, significance of the relationship is shown by the probability value which is 0.000 less than the threshold of 0.05 indicating that the relationship between the variables is statistically significant. In other words, there is a moderate, positive and statistically significant relationship

between data protection and sales volume growth of commercial banks in Port Harcourt ($r = 0.558$, $N = 104$, $p = 0.000 < 0.05$).

Research Question Two: What is the relationship between data protection and profit growth of commercial banks in Port Harcourt?

Hypothesis Two: There is no significant relationship between data protection and profit growth of commercial banks in Port Harcourt.

Table 2 Computation of the relationship between data protection and profit growth of commercial banks in Port Harcourt

		Correlations	
		Data Protection	Profit Growth
Data Protection	Pearson Correlation	1	.635**
	Sig. (2-tailed)		.000
	N	104	104
Profit Growth	Pearson Correlation	.635**	1
	Sig. (2-tailed)	.000	
	N	104	104

** . Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS output, 2024.

The SPSS output on Table 2 shows that a Pearson’s Correlation was run to assess the relationship between data protection and profit growth of commercial banks in Port Harcourt using a sample of 104 managers. The strength and direction of the relationship between the variables are indicated by the r -value which is 0.635. This means there is a strong and positive relationship between data protection and profit growth of commercial banks in Port Harcourt. Furthermore, significance of the relationship is shown by the probability value which is 0.000 less than the threshold of 0.05 indicating that the relationship between the variables is statistically significant. In other words, there is a moderate, positive and statistically significant relationship between data protection and profit growth of commercial banks in Port Harcourt ($r = 0.635$, $N = 104$, $p = 0.000 < 0.05$).

Research Question Three: What is the relationship between access control and sales volume growth of commercial banks in Port Harcourt?

Hypothesis Three: There is no significant relationship between access control and sales volume growth of commercial banks in Port Harcourt.

Table 3: Computation of the relationship between access control and sales volume growth of commercial banks in Port Harcourt

		Correlations	
		Access Control	Sales Volume Growth
Access Control	Pearson Correlation	1	.941**
	Sig. (2-tailed)		.000
	N	104	104
Sales Volume Growth	Pearson Correlation	.941**	1
	Sig. (2-tailed)	.000	
	N	104	104

** . Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS output, 2024.

The SPSS output on Table 3 shows that a Pearson’s Correlation was run to assess the relationship between access control and sales volume growth of commercial banks in Port Harcourt using a sample of 104 managers. The strength and direction of the relationship between the variables are indicated by the r -value which is 0.941. This means there is a very strong and positive relationship between access control and sales volume growth of commercial banks in Port Harcourt. Furthermore, significance of the relationship is shown by the probability value which is 0.000 less than the threshold of 0.05 indicating that the relationship between the variables is statistically significant. In other words, there is a very strong, positive and statistically significant relationship between access control and sales volume growth of commercial banks in Port Harcourt ($r = 0.941$, $N = 104$, $p = 0.000 < 0.05$).

Research Question Four: What is the relationship between access control and profit growth of commercial banks in Port Harcourt?

Hypothesis Four: There is no significant relationship between access control and profit growth of commercial banks in Port Harcourt.

Table 4 Computation of the relationship between access control and profit growth of commercial banks in Port Harcourt
Correlations

		Access Control	Profit Growth
Access Control	Pearson Correlation	1	.667**
	Sig. (2-tailed)		.000
	N	104	104
Profit Growth	Pearson Correlation	.667**	1
	Sig. (2-tailed)	.000	
	N	104	104

** . Correlation is significant at the 0.01 level (2-tailed).

Source: SPSS output, 2024.

The SPSS output on Table 4 shows that a Pearson’s Correlation was run to assess the relationship between access control and profit growth of commercial banks in Port Harcourt using a sample of 104 bank managers. The strength and direction of the relationship between the variables are indicated by the r -value which is 0.667. This means there is a strong and positive relationship between access control and profit growth of commercial banks in Port Harcourt. Furthermore, significance of the relationship is shown by the probability value which is 0.000 less than the threshold of 0.05 indicating that the relationship between the variables is statistically significant. In other words, there is a strong, positive and statistically significant relationship between access control and profit growth of commercial banks in Port Harcourt ($r = 0.667$, $N = 104$, $p = 0.000 < 0.05$).

CONCLUSIONS

The study conducted on the relationship between consumer data privacy and corporate performance of commercial banks in Port Harcourt reveals critical insights that underscore the importance of robust data protection measures in driving corporate success. Specifically, the analysis shows that data protection, as a dimension of consumer data privacy, has a positive and significant relationship with both sales volume growth and profit growth of commercial banks. This indicates that when banks implement strong data protection practices, they not only safeguard consumer information but also enhance their overall corporate performance. Similarly, access control, another dimension

of consumer data privacy, also exhibits a positive and significant relationship with sales volume growth and profit growth. This suggests that stringent access control mechanisms that regulate who can access consumer data contribute to the banks' financial growth by fostering consumer trust and loyalty.

The findings affirm that consumer data privacy is not just a regulatory compliance issue but a strategic business driver. Commercial banks that prioritize and invest in robust data protection and access control measures can expect to see tangible improvements in their sales and profitability. This reinforces the notion that safeguarding consumer data is integral to sustaining long-term corporate performance in the competitive banking sector of Port Harcourt.

RECOMMENDATION

- i. Commercial banks in Port Harcourt should prioritize the implementation of advanced data protection protocols. This includes encryption of sensitive consumer data, regular security audits, and adoption of cutting-edge cybersecurity technologies. By doing so, banks can minimize the risk of data breaches, which, in turn, will foster consumer trust, leading to increased customer retention, higher sales volumes, and profit growth.
- ii. It is recommended that commercial banks invest in robust access control systems to ensure that only authorized personnel can access sensitive consumer data. This can include multi-factor authentication, biometric verification, and role-based access controls. Such measures will not only comply with data privacy regulations but also contribute to a secure environment that encourages consumer confidence and loyalty, ultimately driving sales and profitability.
- iii. Banks should implement regular training and awareness programs for employees on the importance of consumer data privacy and the specific protocols in place. Educated employees are more likely to follow best practices, reducing the risk of data mishandling. Additionally, banks should engage in transparent communication with customers regarding how their data is protected, which can further enhance customer trust and contribute to sales and profit growth.
- iv. Banks should establish a continuous monitoring system to regularly assess the effectiveness of their data protection and access control measures. This should include regular reviews of security policies, updates to technology infrastructure, and adaptation to emerging threats. By continuously improving their consumer data privacy strategies, banks can maintain a competitive edge in the market, ensuring sustained growth in sales volume and profitability.

REFERENCES

- Ahmed, M., Li, J., & Xu, Z. (2023). The impact of consumer data protection on the financial performance of commercial banks in the Middle East. *Journal of Financial Regulation and Compliance*, 31(2), 102-119. <https://doi.org/10.1108/JFRC-05-2023-0067>
- Chen, X., & Lu, Y. (2023). Enhancing cybersecurity through advanced access control mechanisms: A focus on multi-factor authentication and role-based access control. *Cybersecurity Journal*, 8(3), 145-160. <https://doi.org/10.1016/j.cyberj.2023.101022>
- Dimitrieska, S. (2023). The role of consumer trust in online banking: Implications for data privacy and bank performance. *International Journal of Bank Marketing*, 41(1), 45-62. <https://doi.org/10.1108/IJBM-07-2022-0284>
- Frydlinger, D., & Hodge, J. (2023). Navigating data protection regulations: Insights from GDPR and NDPR implementations. *Information Security Journal: A Global Perspective*, 32(2), 89-105. <https://doi.org/10.1080/19393555.2023.1197824>

- Grewal, D., Roggeveen, A. L., & Nordfält, J. (2023). Consumer data protection in the digital age: Balancing privacy and personalization. *Journal of Retailing*, 99(1), 26-42. <https://doi.org/10.1016/j.jretai.2023.01.003>
- Jones, R., & Robinson, G. (2023). Corporate performance metrics: A holistic approach to financial and non-financial indicators. *Journal of Business Strategy*, 44(2), 55-70. <https://doi.org/10.1108/JBS-11-2022-0191>
- Kowatsch, T., & Maass, W. (2023). Consumer awareness and data privacy: Implications for digital banking. *Journal of Consumer Affairs*, 57(2), 311-328. <https://doi.org/10.1111/joca.12438>
- Kumar, R., Gupta, S., & Sharma, A. (2023). Strategies for driving sales volume growth in competitive markets: The role of customer relationship management. *Marketing Intelligence & Planning*, 41(3), 345-359. <https://doi.org/10.1108/MIP-04-2022-0178>
- Kumar, S., Singh, V., & Choudhary, P. (2023). Advanced access control mechanisms for enhanced organizational security: A comprehensive review. *Information Systems Management*, 40(1), 24-38. <https://doi.org/10.1080/10580530.2023.1207382>
- Lee, H., Choi, S., & Kim, J. (2023). The role of regulatory compliance in enhancing corporate reputation: Evidence from South Korean banks. *Corporate Reputation Review*, 26(2), 90-108. <https://doi.org/10.1057/s41299-023-00125-7>
- Li, X., Wang, J., & Zhao, Y. (2023). Sales volume growth strategies in the digital era: Insights from the Chinese retail sector. *Journal of Business Research*, 156(1), 200-212. <https://doi.org/10.1016/j.jbusres.2023.05.012>
- O'Connor, S., & O'Leary, K. (2023). Data privacy in a digital world: Exploring consumer expectations and organizational responses. *Journal of Information Privacy and Security*, 19(2), 67-82. <https://doi.org/10.1080/15536548.2023.1193276>
- Smith, P., Brown, D., & Lee, M. (2023). Rethinking corporate performance: The integration of ESG factors in performance evaluation. *Journal of Corporate Finance*, 78(4), 203-220. <https://doi.org/10.1016/j.jcorpfin.2023.101967>
- Venkatesh, V., & Davis, F. D. (2023). Revisiting the Technology Acceptance Model: Current perspectives and future directions. *MIS Quarterly*, 47(1), 123-143. <https://doi.org/10.25300/MISQ/2023/16512>
- Wang, H., Li, C., & Li, Z. (2023). Consumer data protection: Legal frameworks and their impact on business practices. *International Journal of Information Management*, 70(2), 101729. <https://doi.org/10.1016/j.ijinfomgt.2023.101729>
- Westin, A. F., Alhadeff, E. A., & Dourado, E. (2023). Evolving concepts of consumer data privacy in the digital age. *Journal of Law, Technology & Policy*, 2023(2), 45-70. <https://doi.org/10.1016/j.techlaw.2023.102034>
- Zhang, T., Huang, Y., & Chen, H. (2023). Profit growth strategies in emerging markets: Balancing innovation and cost management. *Emerging Markets Review*, 54(1), 123-138. <https://doi.org/10.1016/j.ememar.2023.101715>

Zhang, X., & Li, Y. (2022). The impact of data privacy on customer loyalty: Evidence from the banking sector in China. *Journal of Financial Services Marketing*, 27(1), 60-75.
<https://doi.org/10.1057/s41264-021-00090-8>