

---

## EFFECT OF BANK CUSTOMERS' PRIVACY CONCERN ON INTENTION TO ADOPT OPEN BANKING

**OLOVEZE**, Ambrose Ogbonna

Department of Marketing

Michael Okpara University of Agriculture, Umudike

emrysoloveze@gmail.com

**AHAIWE**, Emmanuel Onyedikachi

Department of Marketing

Michael Okpara University of Agriculture, Umudike

**OKEKE**, Damian Chibuike,

Department of Economics

Michael Okpara University of Agriculture, Umudike

Chibuikeokeke@yahoo.com

**OGBONNA**, Chinweike

Regional Manager, Peace Mass Transit, Aba, Nigeria

### ABSTRACT

Privacy concerns are critical considerations in consumers' relationship with businesses. Consumers consider it an exclusive area that they should control and scarcely reveal without some level of assurances. Innovations like open banking face challenge of success because customers' permissioned data are a pre-requisite to its success. Rising data breaches, customers fear for loss of privacy and finance, exposure to risk are major challenges to the success of open banking. This study examined the effect of customers' privacy concern on intention to adopt open banking. Privacy concern was approached as a multi-dimensional construct consisting perceived risk, perceived security and perceived trust. 478 test units were pooled from students with operational bank accounts using structured questionnaire. Confirmatory factor analysis and structural equation modeling was adopted. The result reveals that perceived security is the strongest antecedent to adoption of open banking. The study recommends that strict regulations with extreme punitive measures are required to ensure strict compliance by banks and third parties.

**Keywords:** Open banking, data protection, privacy concerns, bank innovation, digitalisation

### INTRODUCTION

The banking sector has been undergoing transformations in Nigeria with the intention to improve banks' ability to deliver superior services to customers. The transformations have gone from liberalization of banking license that encouraged new entrants, to bank consolidations with increase in bank capitalization, and to the implementation of information and communication technologies (ICT) to facilitate bank processes. One of the intentions is to improve customer service delivery and make the system robust and competitive.

Several technologies such as the use of automated teller machines (ATM) have created profound effect on customers. Customers seek convenience, easier access to their money and reduction in waiting time in banking halls. This progression attracted more adoption of technologies in the banking industry with customer-centric goals. Other disruptive innovations within the banking industry encompass cardless cash

---

on ATMs (Oloveze et al., 2022), internet banking, m-banking, point of sale terminal for cash deposits, withdrawals, bills payment and transfer options, biometric authentication provisions on ATM.

These innovations created room for competitiveness in the bank industry as banks sought to attract and retain customers, and make retained customers loyal ones. But they also pose security issues in the minds of customers; as technology has allowed bank frauds and in huge financial losses (NIBSS, 2020; The Nilson Report, 2019).

Recently, reports identified existence of huge financial exclusion and large number of unbanked population in Nigeria. This led to involvement of financial technology firms known as fintechs that sought to bridge the gap between the banked and unbanked population. These fintechs engaged massively in financial activities such as offering loans to customers. They have rapidly introduced innovative payment platforms, including mobile wallets and e-payment applications (Liébana-Cabanillas et al., 2020) in order to reduce the level of financial exclusion in Nigeria, which was put at 40% (Demirgüç-Kunt et al., 2018).

However, the involvement of these fintechs has raised increased concern for data privacy violations and distrust, as they are frequently accused of breaching customers' privacy (Ochojila, 2022). Recently, banks and fintechs have been sanctioned due to non-compliance to guidelines on data protection, data breach and violation of confidentiality (Tunji, 2023). With fintechs involvement in Nigeria it is suggested that only the paranoid survive because of customers' concern in trusting third parties with bank details and private information (Matuluko, 2016).

Currently, the planned enrolment of open banking is generating positive expectations after its development in United Kingdom that arose from poor competitive level of retail banking sector. The projection for developing nations where there is high rate of unbanked and under-banked population is on offer of accessibility, affordability, improvement on financial inclusion through fintechs and strengthening the financial market (Hoganlovells, 2018). The underlying factor is its potential to utilize available customers' data to revolutionize financial markets.

Nigeria launched open banking and supported it with data protection laws, regulations and operational guidelines. Notably, open banking allow banks to grant third parties, the access to customers' personal data and financial information following the customers' consent. The drive is to promote and deepen building of customer-centric products and competitiveness among financial service providers.

The function of open banking system requires the involvement of central bank of Nigeria; Application Programming Interface providers like banks and insurance companies; Application Programming Interface consumers like fintechs; and the bank customers who own the data and financial information, and whose consent is a determinant to the success of open banking. Accordingly, third parties like Paystack, banks like Sterling bank, and big firms like PriceWaterCoopers have adopted open banking (Onyango, 2023).

However, there is concern customers' privacy and data security. The debate over e-consumer protection has been an ongoing discourse since the advent of e-commerce because e-consumer protection is an important issue for online sellers and buyers (Ateke & Ogbuji, 2017). Consumers want to be sure that their personal data shared on online are protected, while firms argue the extent to which they should be responsible for safeguarding personal data of customers (Ateke & Ogbuji, 2017). Privacy concerns in this study encompass security worries, risk issues and trust concerns. Data security and protection are key

---

customer concerns (Nigerian Communication Commission, 2021). Omoruyi (2023) reports that data breaches rose to 64% in the first quarter of 2023).

Thus, data breaches are high with 91% success rate of all fraudsters' attack in 2020 (Guardian, 2023); and this is not reducing, given the rising data breaches between January and March 2023 (Oloruntade, 2023). With the failure of several innovations in history, the success potential of open banking hangs on customers' consent. This makes the adoption success of open banking to be massively dependent on customers' permission over their financial data. Therefore, this study focuses on the effect of bank customers' privacy concerns on intention to adopt open banking.

### LITERATURE REVIEW

Open banking is an emerging discourse in literature following its nascent stage in enrolment and application in developed and developing countries. It is a process that involves banks (regarded as application programming interface providers) providing access to customer private data and financial information to third parties (regarded as application programming interface consumers) to enable designing of customer-centric products; as well as reshape innovation in the industry and promote competitiveness.

Open banking thrives in sharing of customer-permissioned data between banks and third parties to facilitate customized financial products (Onyango, 2023). It drives innovation and efficiency (Hoganlovells, 2018), competition and accessibility to financial services (Onyango, 2023), give customers increased control over personal data (PwC, n.d.), promises to expand the financial ecosystem, provides customers with needed digital experiences (Accenture, n.d.), and chance of promoting tailored financial products (GoCardless, 2023). Also, open banking promises to lower transaction costs, boost conversion rates, improve acceptance e-payments, promote instant settlement by expanding payment methods, improve customer experience, deepen security by ensuring that third parties meet higher security standards, enhance transfer of customer data, and promote new financial technologies and collaboration between banks and fintechs (Kevin 2023).

Studies suggest that open banking is an emerging area in literature with most appearing as discussion papers. Goga (2020) evaluated digitalisation, data and open banking with focus on South Africa and suggests that customer data that banks hold have the power to deliver immense benefits to the consumer though customer consent and regulations are fundamental to the application. The study of Castañeda et al. (2007) highlighted customers' privacy concern majorly on control of personal information in online settings and its subsequent usage in e-market system. This captures customers demand for privacy in handling their personal data and financial information.

Privacy concerns have been present in online settings. Ateke and Isaac (2020) provides that customers are concerned about security and privacy of online transactions; they fear that their personal information might be misused or that they might become victims of cybercriminals, especially, as threats of credit card fraud and password theft create substantial problems for netizens and e-tailers.

The concept of privacy establishes customers' desire to control information emanating from them as a fundamental requirement to maintain relationship (Rachels, 1975). It is evaluated in terms of risks (Ashworth & Free, 2006) while being linked to data security (Bellman et al., 2004) and trust. It is argued as one-dimensional construct (Buchananet et al., 2007) despite its multi-dimensional context (Milne, 2000; Castañeda et al., 2007). The underlying factor is on customers' desire to know the purpose for using their personal data, and exercising control over its collection and use. Thus studies accessed privacy

---

concern from control (Olivero & Lunt, 2004), knowledge (Pollach, 2005) and security (Bellman et al. 2004) perspectives. This study approached privacy as a multi-dimensional construct consisting perceived risk, perceived security and perceived trust.

### **Perceived Risk**

Customers perceive certain levels of risk with every action. The levels of risk depend on the level of knowledge and attitude towards the risk. It deals with customers' behavioural uncertainties on the type and level of loss they might incur when they enact certain behaviours. Thus, it is a component of customers' uncertainty and consequences of action (Peter & Rayan, 1976). The perception of risk increases where customers' perceive insufficient security (Naiyi, 2004), inappropriate usage of personal data (Nyshadham, 2000) and situations where there is lack of trust (McCorkle, 1990). In open banking context, customers are one of the parties to its success. Their consent to the use of private information is a fundamental requirement for open banking. Studies have indicated that risk influences customers' behavioural response to online offerings (Ateke & Isaac, 2020; Kalinic et al., 2019; Naiyi, 2004) while indirectly impacting consumer behaviour through its negative impact on trust (Liebana-Cabanillas et al., 2018). Therefore, the following hypotheses were formulated:

H<sub>1</sub>: Customers' perceived risk negatively relates to trust towards open banking

H<sub>2</sub>: Customers' perceived risk negatively relates to intention to adopt open banking

### **Perceived Security**

Security of personal information is a critical concern to customers; and their perception of security is formed by experience, antecedents in the field, and natural behavioural tendencies to be preserved and protected against harm and risk. It is highlighted in areas of risk, safety and privacy (Oloveze et al., 2022). In open banking context, stringent security measures, protective regulations and operational guidelines are necessary to protect customer data and generate confidence, especially when users are unfamiliar with an innovation (Kim et al., 2010). The critical concerns of customers in security context encompass privacy concerns, customer personal data, the transaction itself (Shah et al., 2014), and desire to have control over sharing of their data (Naiyi, 2004). These are often inhibitors to adoption of products (Lee, 2009). Studies suggest that security issues need to be controlled (Schierz et al., 2010) to achieve significant adoption success. Extant literature indicates that security positively influence consumer behaviour (Oloveze et al., 2022; Liebana-Cabanillas et al., 2018). Further, because of its significance in this study and rising data breaches in Nigeria, it is suggested to be related to trust. The notion is that where customers perceive adequate security of an innovation it can impact their trust towards the innovation. Thus, we hypothesize that:

H<sub>3</sub>: Perceived security is positively related to trust in adopting open banking.

H<sub>4</sub>: Perceived security is positively related to intention to adopt open banking.

### **Perceived Trust**

Perceived trust is an attribute that is seen from cognitive and behavioural dimensions. Cognitive aspect explains the expectation of one party on another fulfilling an obligation in a relationship while behavioural dimension explains the willingness of one party to be vulnerable to risk (Oloveze et al. 2022). In online settings, it contributes to reduction in privacy concerns and data breaches (Blut et al., 2015) while having competition, security and privacy concerns as its antecedents (Yousafzai et al., 2003). Trust levels are affected by risk involvement when adoption of innovation is at the early stage though it mitigates with time (Liebana-Cabanillas et al., 2018). With innovations, initial trust is essential because customers' perceived risk impacts adoption. Practically, trust in firms reduces risk while encouraging continuous adoption (Yang et al., 2015). However, regulations and stringent customer protections in online transactions are necessary to improve trust at the initial stage of innovation (Liebana-Cabanillas et

al., 2018). Extant literatures show that security increases the intention to adopt innovations (Oloveze et al. 2022; Liebana-Cabanillas et al. 2018). Therefore, we hypothesize that:

H<sub>5</sub>: Perceived trust is positively related to trust in adopting open banking.

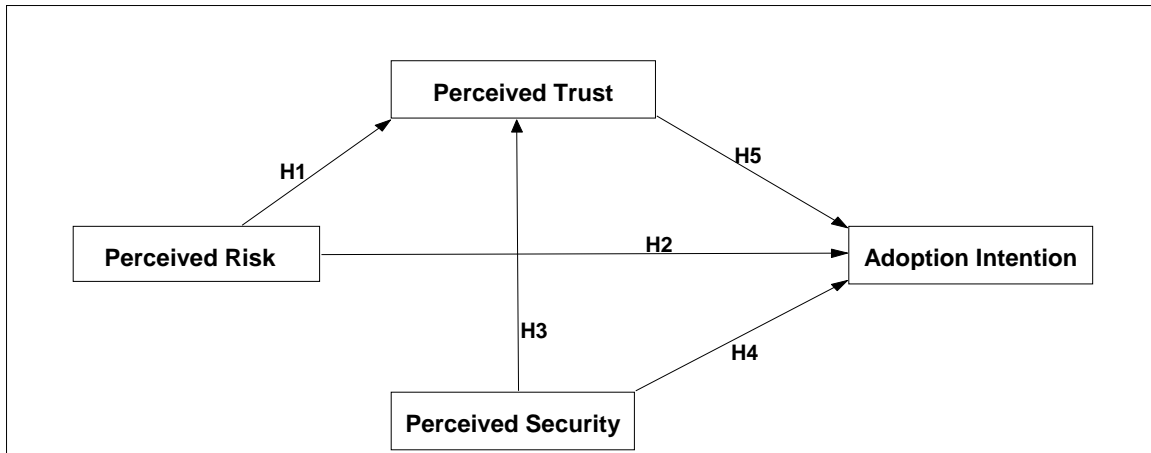


Fig 1. Proposed Conceptual Model

**METHODOLOGY**

This study is a cross-sectional survey that adapted questionnaire as research instrument. The items in the questionnaire were scaled on 5-point Likert. The preliminary test on the instrument was done using experts’ experience in banking system and technology. Purposive and snowball sampling was adopted because of the focus which was on bank customers with operational account. Having a bank account that is functional is a pre-requisite for participation in the study. This was used as a screening question. The sample consisted mainly of students of higher institutions in South East Nigeria. Data was collected using Google-form-designed questionnaire. The link was shared to undergraduate and post-graduate students. Confirmatory factor analysis was adopted for reliability and validity using SPSS v23 and AMOS 23.

**RESULTS AND DISCUSSION**

478 samples were collected after three weeks with the screening question indicating that all the students that participated in the survey have functional bank accounts. The demographic profile revealed that 63% were female, 37% were male. 66% were undergraduates, 34% were postgraduate students. Common method bias (CMB) was assessed through Herman’s single factor technique by adjusting all items to single factor. With 46.647, CMB was not a problem. Kaiser-Meyer-Olkin value of 0.777 confirmed the sampling adequacy for factor analysis. Further, with 4522.003 Bartlett’s test of sphericity at p=0.00, the null hypothesis of no difference in variances of the responses was rejected.

**Table 1: Confirmatory Factor Analysis**

Variable	Factor items	Factor loads	CA	CR	AVE	Mean
Perceived Trust	Trust1	.871	.843	.845	.647	3.30
	Trust2	.809				
	Trust3	.726				
Perceived Risk	Risk1	.887	.853	.904	.758	3.33
	Risk2	.890				

Perceived security	Risk3	.833				
	Security1	.852	.860	.801	.575	3.36
	Security2	.717				
	Security3	.696				
Adoption intention	Adopt_Int1	.792	.919	.893	.737	2.73
	Adopt_Int2	.895				
	Adopt_Int3	.885				

Reliability of the scale was checked through Cronbach alpha and composite reliability, with threshold of 0.6 and 0.7 respectively (Hair et al., 2006). The values of Cronbach alpha and composite reliability for each of the constructs on Table 1 were above the thresholds thereby confirming the reliability. Validity was performed through convergent validity and discriminant validity. The convergent validity was assessed through factor loadings. All the factor loadings on Table 1 were above the threshold of 0.6 (Bagozzi & Yi, 1988) thereby proving the validity. This was also confirmed through the average variance extracted (AVE) which is higher than the 0.5 threshold for each of the constructs (Fornell & Larcker, 1981).

Further, the discriminant validity confirmed the validity as revealed on Table 2. This was done through the correlations between the dimensions which must be below the root of AVE (Fornell & Larcker, 1981) while the correlations must not be more than 0.9 (Hair et al. 1995). These conditions were met. The values of  $R^2$  indicated on table 1 revealed that for perceived trust, perceived risk and security accounted for 40.4% variance while for adoption intention, perceived risk, trust and security accounted for 57% variance. The proposed model for privacy concerns on open banking system was evaluated through the goodness-of-fit model indicators against their recommended thresholds shown on table 2. The results confirm that the model is good given that the vital respective values were above the thresholds in literature.

**Table 2: Correlation Matrix, Discriminant Validity, and Model Evaluation**

Variable	Perceived trust		Perceived risk		Perceived security		Adoption intention			
Perceived trust	<b>.804</b>									
Perceived risk	.017		<b>.871</b>							
Perceived security	.618		-.141		<b>.758</b>					
Adoption intention	.491		-.273		.743		<b>.858</b>			
Model indicators	CFI	TLI	IFI	RFI	NFI	SRMR	RMSEA	AGFI	GFI	CMIN/DF
Model values	.987	.922	.987	.914	.986	.061	.134	.902	.990	9.556
Recommended thresholds	$\geq 0.90$	$\geq 0.90$	$\geq 0.90$	$\geq 0.90$	$\geq 0.90$	$\leq 0.08$	$\leq 0.08$	$\geq 0.80$	$\geq 0.90$	$\leq 5.00$
Variable	$R^2$					Explanation				
Perceived trust	0.404					Weak				
Adoption intention	0.570					Moderate				

Note: Main diagonal – (**in bold**) square root of AVE

The analysis of the paths was done using structural equation modeling through maximum likelihood, estimates and p-values. As revealed on Table 3 and figure 2, all the paths were significant. The direct and indirect paths revealed that perceived security is the most significant factor that influences intention to adopt open banking. Therefore, bank customers consider this aspect of their privacy to be the strongest concern in adopting open banking.

With  $H_1$  and  $H_2$  that was formed from perceived risk,  $H_1$  ( $\beta=0.089$ ,  $p \leq 0.003$ ) confirms the significant effect of perceived risk on perceived trust but with a positive effect. The implication is that risk do not



decrease trust in open banking despite its significant role. This is not consistent with literature (Liebana-Cabanillas et al., 2018) but can be deduced from three key areas. The sample unit who consisted mainly of undergraduate students that tends to be educated with risk involvements in innovation. Education and knowledge of risks associated with related innovations has the potency to mitigate the drawbacks of risk. Secondly, the class of the sample unit consists youth that are most likely innovators. Innovators have the tendency to adopt innovations at its early risky stage before the massive roll out. Thirdly, the sample consists youths in Nigeria with abilities in technological skills that could imagine the benefits against the risk involvement and decide to adopt it. Notably, this is an important contribution because literature conceptualizes a negative relationship between risk and trust in all circumstances.

H<sub>2</sub> ( $\beta = -0.202, p \leq 0.000$ ) confirms that perceived risk has significant negative relationship with open banking adoption intention. This is consistent in literature (Kalinic et al. 2019). The result reveals that it has the least effect on open banking. Theoretically, the finding implies that with the negative relationship, perceived risk decreases open banking adoption intention, following associated fears with rising data breaches, prevailing knowledge of charges against banks' fraudulent activities on customers' financial accounts, fear of losing control of personal data, fear of misuse by fintechs who have been found guilty of misusing customer data, and general negative consequences of consenting to open banking system.

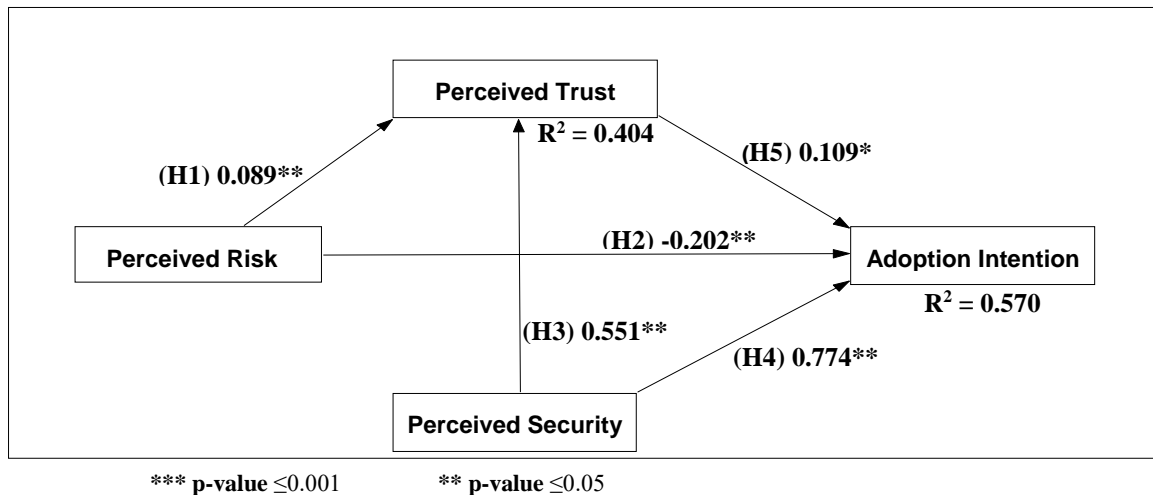
H<sub>3</sub> ( $\beta = 0.551, p \leq 0.000$ ) confirms that perceived security relates positively and significantly to trust in open banking. The relationship between security and trust is often ignored in literature and empirical studies. This study confirms the positive effect of security on customers' trust to innovation. The theoretical implication is that security perception of bank customers on open banking increases their trust level towards adopting the innovation. Essentially, it is the most important indirect predictor on customers' privacy concerns to open banking. This is also an important contribution to literature because literature conceptualizes security majorly as a direct effect on innovation.

H<sub>4</sub> ( $\beta = 0.774, p \leq 0.000$ ) confirms that perceived security positively and significantly relates to intention to adopt open banking. This is consistent with earlier results (Oloveze et al. 2022; Liebana-Cabanillas et al. 2018). The theoretical implication is that increases in security measures and stringent guidelines, and regulations that promises customer protection increases bank customers' adoption intention. Therefore bank customers' consideration of security of the financial information demands that banks must provide firm assurances on right use of personal information and stronger protection of their information while sharing it with third parties.

H<sub>5</sub> ( $\beta = 0.109, p \leq 0.031$ ) confirms that perceived trust is positively and significantly related to intention to adopt open banking. This is consistent with empirical results on innovations that are similar to this type of innovation (Kalinic et al. 2019; Oloveze et al. 2022). Theoretically, the implication is that trust increases the intention of bank customers to adopt open banking thereby making trust factor a necessary variable despite the low value estimate/coefficient.

**Table 3: Hypothesized relationships**

Hypotheses	B	S.E	C.R.	Std. B	P	Decision
H1: Perceive risk→ Perceived trust	.089	.030	2.978	.105	.003	Yes
H2: Perceive risk→ Adoption intention	-.202	.033	-6.053	-.184	.000	Yes
H3: Perceived security→ Perceived trust	.551	.031	17.717	.627	.000	Yes
H4: Perceived security→ Adoption intention	.774	.044	17.530	.679	.000	Yes
H5: Perceived trust→ Adoption intention	.109	.050	2.156	.084	.031	Yes



**Fig 2.** Result of Conceptual Model

### CONCLUSION AND RECOMMENDATIONS

Generally, privacy concerns of customers' indicates that security, risk and trust are the multi-dimensional perspectives to evaluate privacy concern about open banking. These three dimensions are important despite not having same level of effect. In this instance, what bank customers consider to be the strongest signal is security concern. Security concerns cover their concern on safety, protection of personal data and financial information and the desire not to be exposed to risk.

Both security and risk reveals direct and indirect roles on customers' intention to adopt open banking. The role of trust and risk reveals that despite their low effects on adoption intention, they are important considerations for customers in consenting to open banking system. Among the multi-dimensional constructs, risk is the only variable with negative influence thereby making it capable of decreasing the intention to adopt open banking.

The study calls for caution in application because of design adopted. The use of cross-sectional survey implies there is need for a longitudinal study that spans longer periods. Secondly, the sample size of 478 bank customers calls for a larger sample size as this might not represent the total population of bank customers in South East Nigeria. Thirdly, a probability sampling approach is encouraged as future lines of study while the path of moderating effects of students' gender, age and bank patronage can be studied. Future studies can integrate the dimensions of risk given to understand the key risk aspect that has major effect on adoption intention. This will help have deeper understanding on direction of privacy concerns from the sample units.

With the revealed findings, strict regulations with extreme punitive measures are required to ensure strict compliance by banks and third parties. Operational guideline needs not be compromised. It should be made clearer and strictly met by all parties involved in handling customers' data. To mitigate the privacy concerns' effect, bank customers must be given priority attention by designing legal frameworks that is 100% customer-centric, provide efficient avenue at no cost for easier and faster customer redress, and raise the punishment to an extreme level that makes it near impossible for the defaulting bank or third party to function thereafter. Lastly, aggressive marketing campaigns needs to be undertaken by the apex



bank and commercial banks to create sustained awareness on the operation and the workable measures taken to protect customer information and punish offenders.

## REFERENCES

- Accenture. (n.d.). *Open banking: Highlighting the change around the world*. Retrieved from <https://www.accenture.com/us-en/insights/banking/open-banking>
- Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics*, 67, 107-123.
- Ateke, B. W., & Isaac, H. A. (2020). Online consumer protection initiatives and e-loyalty. *International Academic Journal of Management and Marketing*, 6(5), 59-73.
- Ateke, B. W., & Ogbuji, C. N. (2017). An exploratory study of online consumer protection concerns: The Nigerian case. *FUO Journal of Business and Finance*, 7(2), 92-100.
- Bagozzi, R.P. & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science*, 16(1), 74-94.
- Blut, M., Chowdhry, N., Mittal, V. & Brock, C. (2015). E-service quality: A meta-analytic review. *Journal of Retailing*, 91(4), 679-700.
- Bellman, S., Johnson, E.J., Kobrin, S.J. & Lohse, G.L. (2004). International differences in information privacy concerns: a global survey of consumers. *The Information Society*, 20(5), 313-324.
- Buchanan, T., Paine, C., Joinson, A.N. & Reips, U. (2007). Development of measures of online privacy concern and protection for use on the internet. *Journal of the American Society for Information Science and Technology*, 58(2), 157-165.
- Castañeda, J.A., Montoso, F.J. & Luque, T. (2007). The dimensionality of customer privacy concern on the internet. *Online Information Review*, 31(4), 420 – 439.
- Demirgüç-Kunt, A. Klapper, L. Singer, D. Ansar, S. & Hess, J. (2018). *The global finindex database, 2017: Measuring financial inclusion and the fintech revolution*. Worldbank Publications. The World Bank Group.
- Fornell, C., & Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39–50.
- GoCardless. (2023). *Open banking benefits for customers, businesses and banks*. Retrieved from <https://gocardless.com/guides/posts/what-are-the-benefits-of-open-banking/#:~:text=Open%20banking%20enables%20customers%20to%20financial%20services%20to%20underserved%20populations>
- Goga, S. (2020). *Digitalisation, data and open banking: A South African perspective*. Discussion paper 3, Discussion paper for expert panel on regulating digital platforms for economic development.
- Guardian (2023). Alleged data breach: NDPB investigates two Nigerian banks, *Guardian Nigeria*, 30 January. Retrieved from <https://guardian.ng/news/nigeria/alleged-data-breach-ndpb-investigates-two-nigerian-banks/>
- Hair, J. F., Anderson, R. E., Tatham, R. L., & William, C. B. (1995). *Multivariate data analysis with readings*. Prentice-Hall, Inc.
- Hair, J. F., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. (2006). *Multivariate data analysis (6th edition)*. Pearson Educational International
- Hoganlovells. (2018). *Open banking in Africa – the power of data*. Retrieved from <https://www.hoganlovells.com/en/publications/open-banking-in-africa>

- Kalinic, Z., Marinkovic, V., Molinillo, S. & Liébana-Cabanillas, F. (2019). A multi-analytical approach to peer-to-peer mobile payment acceptance prediction. *Journal of Retailing and Consumer Services*, 49, 143-153. <https://doi.org/10.1016/j.jretconser.2019.03.016>
- Kevin. (2023). *What are the benefits of open banking?* Retrieved from <https://www.kevin.eu/blog/benefits-of-open-banking/>
- Kim, C., Tao, W., Shin, N., & Kim, K.S. (2010). An empirical study of customers' perceptions of security and trust in e-payment systems. *Electronic Commerce Research and Applications*, 9(1), 84-95.
- Lee, M. (2009). Factors influencing the adoption of internet banking: an integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, 8, 130-141.
- Liébana-Cabanillas, F. García-Maroto, I. Muñoz-Leiva, F. & Ramos-de-Luna, I. (2020). Mobile payment adoption in the age of digital transformation: The case of ApplePay, *Sustainability*, 12, 5443.
- Liebana-Cabanillas, F., Higuera-Castillo, E., Molinillo, S. & Ruiz Montañez, M. (2018). Assessing the role of risk and trust in consumers' adoption of online payment systems. *International Journal of Information Systems and Software Engineering for Big Companies*, 5(2), 99-113.
- Liebana-Cabanillas, F., Marinkovic, V., Ramos-de-Luna, I., & Kalinic, Z. (2018). Predicting the determinants of mobile payment acceptance: A hybrid SEM-neural network approach. *Technological Forecasting & Social Change*, 129, 117-130.
- Matuluko, M. (2016). Fintech security in Nigeria: only the paranoid survive, *Techpoint*, 27 June. Retrieved from <https://techpoint.africa/2016/06/27/fintech-security-nigeria/>
- Milne, G. R. (2000). Privacy and ethical issues in database/interactive marketing and public policy: a research framework and overview of the special issue. *Journal of Public Policy and Marketing*, 19(1), 1-6.
- Naiyi, Y. E. (2004). Dimensions of consumer's perceived risk in online shopping. *Journal of Electronic Science and Technology of China*, 2(3), 178-182
- NIBSS. (2020). *NIBSS Insight: Fraud in the Nigerian financial services (2<sup>nd</sup> edition)*. Retrieved from <https://www.nibss-plc.com.ng>
- Nigerian Communication Commission (2021). *Emerging role of data and fintech in the development of digital economy*. Retrieved from <https://www.ncc.gov.ng/documents/985-emerging-role-of-data-and-fintech-in-the-development-of-digital-economy/file>
- Nyshadham, E. A. (2000). Privacy policies of air travel web sites: a survey and analysis. *Journal Air Transport Management*, 6, 143-152
- McCorkle, D. E. (1990). The role of perceived risk in mail order-catalog shopping. *Journal of Direct Marketing*, 4, 26-35.
- Ochojila, A. (2022). Individuals should have authority to decide whether to share sensitive data, legal experts view. Retrieved from <https://guardian.ng/features/individuals-should-have-authority-to-decide-whether-to-share-sensitive-data-legal-experts-argue/>
- Olivero, N., & Lunt, P. (2004). Privacy versus willingness to disclose in e-commerce exchanges: the effect of risk awareness on the relative role of trust and control. *Journal of Economic Psychology*, 25(2), 243-262.
- Oloruntade, G. (2023). *Nigeria is witnessing a disturbing surge in data breaches*. Retrieved from <https://techcabal.com/2023/05/23/nigeria-is-witnessing-a-disturbing-surge-in-data-breaches/>
- Oloveze, A.O., Chukwuoyims, K., Oteh, O.U., Aliu, K.A., Oko, R.A. & Ogbonna, C. (2022). Customer intention toward m-PoS adoption in gas stations: Gender perspective. *AKSU Journal of Administration and Corporate Governance (AKSUJACOG)*, 2(2), 15-30
- Oloveze, A.O., Okonkwo, R.V.O., Oteh, O.U., Nwachukwu, C.P., & Chukwuoyims, K. (2022). Cardless cash and consumer psychology in a cashless society: Structural equation model (SEM) approach, *Journal of Psychology and Allied Disciplines (JPAD)*, 1(1), 19-34.

- 
- Omoruyi, O. (2023). *Nigeria sees 64% increase in data breaches, recording an outstanding 82,000 episodes in Q1 2023*. Retrieved from <https://technext24.com/2023/05/23/nigeria-records-82000-data-breach-in-q1/>
- Onyango, C. (2023). *After Nigeria launched open banking, 3 African countries follow*. Retrieved from [https://primeprogressng.com/posts/after-nigeria-launched-open-banking-3-african-countries-follow-319?\\_s=www.google.com](https://primeprogressng.com/posts/after-nigeria-launched-open-banking-3-african-countries-follow-319?_s=www.google.com)
- Peter, J. P., & Rayan, N.J. (1976). An investigation of perceived risk at the brand level. *Journal of Marketing Research*, 13, 184-188
- Pollach, I. (2005). A typology of communicative strategies in online privacy policies: ethics, power and informed consent. *Journal of Business Ethics*, 62, 221-35
- PwC. (n.d.). *The case of open banking in Nigeria*. Retrieved from <https://www.pwc.com/ng/en/publications/the-case-for-open-banking-in-nigeria.html>
- Rachels, J. (1975). Why privacy is important. *Philosophy and Public Affairs*, 4, 323-333
- Schierz, P. G., Schilke, O., & Wirtz, B. W. (2010). Understanding consumer acceptance of mobile payment services: An empirical analysis. *Electronic Commerce Research and Applications*, 9(3), 209–216.
- Shah, M. H., Peikari, H. R., & Yasin, N.M. (2014). The determinants of individuals' perceived e-security: evidence from Malaysia. *International Journal of Information Management*, 34, 48–57.
- The Nilson Report. (2019). *Card fraud losses reach \$27.85 Billion*. Retrieved from <https://nilsonreport.com/mention/407/1link/>
- Tunji, S. (2023). *FG probes banks, fintechs over data privacy violation*. Retrieved from <https://punchng.com/fg-probes-banks-fintechs-over-data-privacy-violation/>
- Yang, Q., Pang, C., Liu, L., Yen, D. C., & Tarn, J. M. (2015). Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation. *Computers in Human Behavior*, 50, 9-24.
- Yousafzai, S., Pallister, J. & Foxall, G. (2003). A proposed model of e-trust for electronic banking. *Technovation*, 23(11), 847-860.