Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6, 4281-4290
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i6.2929

Does cybercrime affect brand loyalty to deposit money banks in Nigeria

Adedeji Daniel Gbadebo[1*]
[1]Walter Sisulu University, Mthatha, South Africa; agbadebo@wsu.ac.za (A.D.G.).

Abstract: The financial service industry, especially banking, has benefited greatly from the introduction of information technology. The technology has allowed them to offer a wide range of electronic banking services that have expanded scope of participants. This, however, has exposed the banks to cybercrime risk, posing serious threat to their survival. The study aimed to determine how the brand loyalty of the banks' customers is affected by cybercrime associated to the use of e-banking platforms. The study used self-structured and administered questionnaires to gather primary data from 200 clients from (10) deposit money banks (DMBs) and examine the effects of cybercrime on customers brand loyalty. A regression analysis was performed to investigate the relationship between customer brand loyalty and the considered cybercrime activities. The finding identifies a strong inverse association between brand loyalty and financial losses brought on by cybercrime. Also, the evidence shows that card theft significantly reduces brand loyalty. The study further discovers that recurring security vulnerabilities significantly reduce brand loyalty and lastly, the paper demonstrates that the most notable adverse effect on brand loyalty was caused by identity theft. The study's conclusions demonstrate a strong and unfavourable correlation between consumer brand loyalty and cybercrime. The article offers comprehensive recommendations, including policies, strategies, and interventions that show how cybercrime can be combated to reduce the risk of thefts in the banking sector.

Keywords: *Cybercrime, Customers brand loyalty, Deposit money banks.*

1. Introduction

The banking industry, which operates in a highly competitive and complex environment, has realized the benefits of providing its consumers with electronic banking services and products, which has led to a surge in popularity over the past three decades. The rapid technological advancements have revolutionized the global banking sector by enabling digital platforms to deliver better services and convenience. To improve client satisfaction and operational effectiveness, deposit money banks (DMBs) have embraced technology advancements. The DMBs are essential to the financial system by enabling payments, extending credit, and mobilizing.

The embracement of this technological advancement in the banking sector, however, is faced with several threats of cybercrimes (Dada, 2020). Hacking is thought to have served as the precursor to cybercrime in the 1960s. In the 1970s, privacy intrusions, phone tapping, trespassing, and the dissemination of illicit materials came after this. Viruses first appeared in the 1980s. The list of illicit online exploits has grown because of the rapid advancement of ICT from the 1990s and into the present. The internet is now a tool for global crimes and terrorism, as well as espionage. Customers and online buyers run a significant danger of inadvertently giving their personal information to scammers as e-banking becomes more popular. After obtaining the personal data of online shoppers, hackers create fictitious credit cards that they can use without being detected (Odulaja, 2023). Recently, economic crime has shifted to the digital sphere due to the expanding nature of e-transactions and e-commerce (Seema, 2016).

The situation is becoming endemic in Nigeria, as many banks and their clients have been reportedly faced with serious and multiple risks from cybercrimes. Nigeria has seen a substantial rise in

* Correspondence: agbadebo@wsu.ac.za

cybercrime-related cases in recent years. According to the Economic and Financial Crime Commission (2022), cybercriminals conspired with a bank employee to steal over six billion from a Nigerian bank. Dada (2020) states that corporate executives in Nigeria and other African countries are very concerned about crime and corruption. For example, crime and corruption, which account for 75% and 71% of all business-related barriers in Nigeria, are the biggest obstacles to economic activity and enterprise. After burglary, theft and fraud rank second in popularity (EFCC, 2009, 2010). The activities of these crimes can damage their brand loyalty and trust by exposing them to financial losses from fraud and unauthorized transactions. Consistent security breaches can cause customers to migrate to banks they believe to be more secure, eroding their faith in banks and decreasing their confidence in digital banking channels.

Due to increasing concern about the protection of personal and financial information of bank customers, cybersecurity has become a key factor in determining brand loyalty. Cybersecurity has become more important as banks depend more and more on digital platforms to supply services, raising the danger of cyberattacks. The prevention of this crimes highlights the need for banks to implement effective controls to prevent significant losses and operational risks brought on by cybercriminals' devious activities. It serves to uphold public trust in deposit money banks by encouraging bank customers to use online banking platforms (Olayemi, 2023).

Despite the threat that the cybercrime menace poses on the financial system in Nigeria, there is little research to demonstrate how the activities of cybercrime affect Nigerian bank customers' brand loyalty. Past literature, including Dada (2020), Akanji (2022), Ajibola (2023), and others, that investigated the issue of cybercrime activities and its effects on the banks performance in Nigeria concentrated primarily on cybercrime threats and challenges to financial operations, considering the kinds and nature of cybercrime that financial service operators face. This study closes this gap by examining how customer brand loyalty is impacted by cybercrime activity.

Specifically, paper attempts addressing four aims, including (i) to examine that extent at which financial losses to cybercrime affect customer brand loyalty (ii) to investigate the extent that card fraud by cybercriminal affect customer brand loyalty, (iii) to understand how persistent security breaches by cybercriminals affect customer brand loyalty and lastly, (iv) to demonstrate how identity thefts by cybercriminals affect customer brand loyalty. In attempting these to achieve the study aims, the article considers a survey-based approach using a closed-ended questionnaire. Two hundred (200) questionnaires and participants are examined, from 10 commercial banks in Ibadan Metropolis, Nigeria.

The finding identifies a strong inverse association between brand loyalty and financial losses brought on by cybercrime. Also, the evidence shows that card theft significantly reduces brand loyalty. The study further discovers that recurring security vulnerabilities significantly reduce brand loyalty and lastly, the paper demonstrates that the most notable adverse effect on brand loyalty was caused by identity theft. The article offers comprehensive recommendations, including policies, strategies, and interventions that show how cybercrime can be combated to reduce the risk of thefts in the banking sector. The study's remainder is structured as follows. Section 2, 3, 4, and 5, respectively, shows the literature, methods, results and conclusions.

2. Conceptual Review

2.1. Cybercrime and Financial Services Sector

Cybercrime includes any unlawful activity carried out via digital channels, including online fraud, phishing, mail hacking, identity theft, and identity theft (Dada, 2020). They are any type of misbehaviour in cyberspace (Odulaja, 2022), and representing illicit activity carried out using a computer, computer resource, or computer network (Sanchi, 2016). Raghavan and Latha (2014) consider cybercrime as computer-mediated actions carried out via international electronic networks that are either illegal or deemed illegitimate by some parties. Dada (2020) summed up cybercrimes as crimes involving the use of a computer and a network as a target, instrument, channel, source, or location.

Ankrah (2022) claims that computer-based applications and information technology are examples of modern banking technology. Convenience and easy access to funds and account information are two of the practical goals of banking from the standpoint of the banking consumer. He added that the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4281-4290, 2024
DOI: 10.55214/25768484.v8i6.2929

development of technology has made it possible to offer banking services and goods via electronic channels of distribution, or e-banking. The practice of conducting a bank's business using electronic devices is known as electronic banking. Ankrah (2022) provided instances of electronic equipment in use, such as computer systems, GSM phones, ATMs, Internet access points, optical character recognition (OCR), smart cards, and automated teller machines (ATMs).However, Danquah (2022) pointed out that the banking sectors' extensive use of information technology has also given rise to new risks and attacks, primarily in the form of computer crimes and fraud.

With its ease of use and accessibility, digital banking has drastically changed the financial services industry. Customers are now more vulnerable to the growing risk of cybercrime, which includes identity theft, card theft, continuous security breaches, and financial losses. These online dangers have the potential to significantly damage consumers' brand loyalty, which in turn has an effect on deposit money banks' overall profitability. Odulaja (2023) posit that financial losses due to cybercrime can lead to a decline in trust and confidence in a bank, negatively affecting customer loyalty. Customers who suffer financial losses due to cyber-attacks are more likely to switch banks or reduce their engagement with the affected bank.

Ajibola (2023) opined that card theft is a prevalent form of cybercrime that can lead to direct financial loss and inconvenience. The frequency of card theft incidents can erode customers' trust in a bank's security measures, leading to reduced brand loyalty. Persistent security breaches, such as unauthorized access to customer data, can have a lasting impact on a bank's reputation. Customers may perceive these breaches as a sign of incompetence or negligence, prompting them to switch to more secure alternatives. Identity theft is a severe form of cybercrime that can cause significant financial and emotional harm to customers (Imran,2022) . The long-term consequences of identity theft can diminish customers' trust in a bank, leading to a decline in brand loyalty.

2.2. Empirical Review

Wada (2021) analyzed the influence of electronic crime on the Indian banking industry . It became clear that customers are worried about security. The risks associated with identity theft, pharming, and deliberate disclosures of personal information are especially concerning. The results of the study showed that electronic crime related to banking transactions can be reduced by using updated technology and assigning reliable staff and equipment. Consumers worry about security; deliberate disclosures of personal information, including identity theft, and threats like phishing and pharming are of particular concern. The results of the study showed that electronic crime related to banking transactions can be reduced by using updated technology and assigning reliable staff and equipment. Imran (2022) Cybercrime has been shown to have several distinguishing features, such as anonymity, worldwide reach, the potential for widespread victimization, jurisdictional issues, and uneven criminal laws. the speed at which crimes are committed, Within electronic crime, there is a possibility for the deliberate exploitation of issues, differences, volatility, and dynamic nature.

Shewangu (2022) found that there was a negative relationship between the banking industry's performance and electronic fraud. The author examines the various forms of electronic fraud that are taking place in Zimbabwe's banking industry as well as the challenges faced in attempting to lower the risk in his analysis of the threat posed by this type of fraud. They carried out a descriptive analysis of the cyberfraud phenomenon using content analysis. Information was gathered from the selected informants from 22 banks using questionnaires and interviews. Convenience and judgmental sampling strategies were used. It was shown that bank staff are mostly responsible for the various types of electronic fraud stated. Concerns included a lack of resources (technology and detection techniques), inadequate cybercrime legislation, and a lack of awareness raised by awareness campaigns and educational initiatives.

Salami (2023) Key participants and features in another study that is based on a conceptual model for mitigating cyber-banking fraud risk submission include e-fraud victims, fraudster(s), guardians (banks), environmental conditions, and fraud kinds. The study employs the ontological tradition, emphasizing ideas that pinpoint the fundamental characteristics of the cyberfraud risk management phenomenon. It also seeks to investigate the perspectives of the banking sector on reality. To help financial institutions

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4281-4290, 2024
DOI: 10.55214/25768484.v8i6.2929

mitigate cyber fraud risk, the paper's conclusion integrated all relevant components of cyber fraud risk management into a proposed model. The model's development offers a fresh perspective on the phenomenon of cyber fraud risk management because it demonstrates a logical extension of current knowledge.

Ishmael, et al. (2023) investigated cybercrime as a new danger to Zimbabwe's financial services industry. In particular, the study looked into the prevalence of cybercrime in financial institutions. The study employed stratified random selection and purposive selection techniques to choose 48 participants from four commercial banks. The questionnaire and in-depth interviews served as the main research instruments. The investigation found that among the cybercrimes that happen at banks are malware, phishing, identity theft, and hacking. The researchers came to the conclusion that, despite the fact that financial institutions are putting cyber security systems in place to tackle the issue, technological innovation is surpassing the precautionary steps.

Inês & Alexandra (2023) in their paper titled Cybercrime and financial institutions: opportunities, challenges, and threats stated that the threats that cybercrime poses to the global financial system are demonstrated by recent high-profile incidents of financial institutions being the target of cybercriminals, such as the attack on the Bangladesh Central Bank in February 2016 that resulted in a loss of $81 million. Two categories of cybercrime pose a threat to financial institutions, according to their analysis. Hacking and denial-of-service assaults are examples of cyber-dependent crimes that are impossible to commit without internet access. Cyber-assisted, or cyber-enabled, On the other hand, crimes are traditional crimes like robbery, extortion, and fraud that are made easier and more convenient by technology but would still occur in the absence of it. Financial organizations must have plans in place that enable them to recognize and react to both kinds of threats.

According to the literature review, most researchers studying cybercrime focus more on conceptual modeling of the phenomenon, and very few of these studies examine the theoretical foundations of cybercrime or provide empirical analysis of the detrimental effects cybercrime can have on deposit money banks' ability to survive. Once more, most of these studies were carried out outside of Nigeria, which is not surprising given that the nation has reportedly lost billions of Naira to cybercrime, with its financial services industry being the main victim. This paper provides an empirical analysis of the hazards that cybercrime poses to deposit money banks, which serves as justification for the necessity of controlling cybercrime in Nigeria's financial services industry.

3. Methods

This study uses survey-based research designed. Using closed-ended questionnaire, the data are sourced from respondents from 10 commercial banks in Ibadan Metropolis, Nigeria. The respondents are grouped into strata based on shared features, according to the stratified random sample technique. The two hundred (200) questionnaires in total were given to study participants, who were selected from the ten (10) deposit money banks (DMBs). Of these, one hundred and seventy-six (176) questionnaires, or 88% of the total, were returned and completed correctly; fifteen (15) questionnaires, or 7.5% of the total, were returned but not properly completed, making them invalid; and nine (9) questionnaires, or 4.5% of the total, were not returned. The answers from the surveys that were received served as the basis for these analyses. Figure 2 above showed that one hundred and four (104) respondents, or 59% of the total respondents, are male and seventy-two (72) respondents, or 41% of the total respondents, are female. This suggests that gender is a major factor in this research.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4281-4290, 2024
DOI: 10.55214/25768484.v8i6.2929

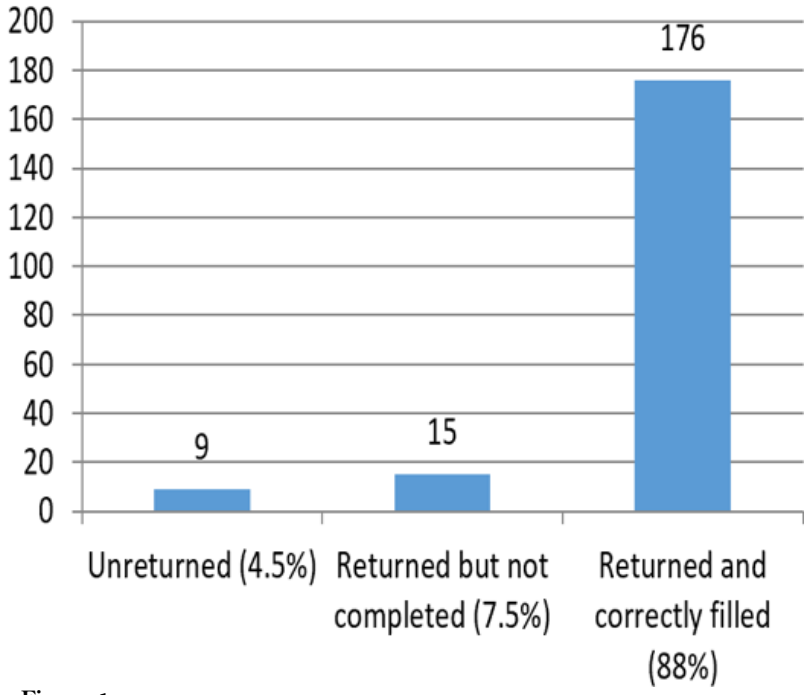

Figure 1.
Analysis of response rate.

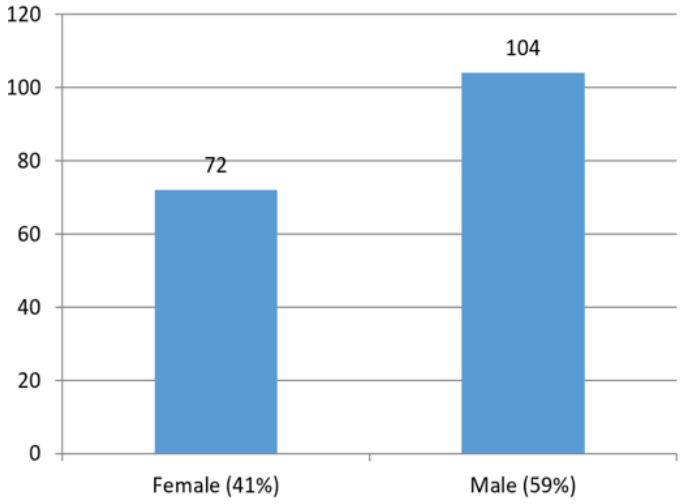

Figure 2.
Gender distribution of respondent.

To showing the relationship between customer brand loyalty and the associated considered cybercrime activities, the Lickert scale of responses represented on the designed questionnaire follows five scales involving, strongly agreed, agreed, indifference, disagree, and strongly disagreed, which respectively are coded 5, 4, 3, 2, and 1,

In completing the empirical analysis, the paper determines the appropriateness of the research instrument, using the Cronbach's Alpha method. Afterward, a regression analysis was performed to investigate the nature and strength of the relationship between customer brand loyalty and the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4281-4290, 2024
DOI: 10.55214/25768484.v8i6.2929

associated considered cybercrime activities. Equation 1 (functional form) and Equation 2 (linear form) are adopted to show the relationship between the customer brand loyalty and the cybercrime activities.

$$\mathrm{CBL}_i = f(\mathrm{FL}_i, \mathrm{CF}_i, \mathrm{PSB}_i, \mathrm{IT}_i) \quad (1)$$

$$CBL_i = \beta_0 + \beta_1 \mathrm{FL}_i + \beta_2 \mathrm{CF}_i + \beta_3 \mathrm{PSB}_i + \beta_4 \mathrm{IT}_i + \mu_i \quad (2)$$

Where CBL_i, the dependent variable is the customer brand loyalty, and the cybercrime activities, indicated by the independent variables as defined in (1) and (2), include financial losses (FL_i), card fraud (CF_i), persistent security breaches (PSB_i), identity theft (IT_i). β_0 is Intercept of the model, $\beta_1 (\text{for i} = 1, 2, 3)$ are the coefficients of the independent variables in the model, and μ_i = Error term. The data gathered from the questionnaire are used to complete the analysis using regression.

To ensure accuracy, efficiency, and completeness, the data gathered using questionnaires was edited, coded, and tallied. The data was presented using descriptive statistics, such as tables, and the qualitative data was gathered, which calls for a descriptive and content analysis. The investigation was divided into five stages, and a linear regression model was also employed to provide answers to the research questions.

4. Results

The paper completes some pre-estimation, to show the sample distribution and the reliability test. The data from the questionnaires were gathered, coded and transcribed according to the Lickert scale, and the distribution is presented. Table 1 (Panel A) shows the summary of the distributed questionnaires. Clearly, only 88%, that is 176 of the administered questionnaires were correctly filled, hence used for the analysis. The paper examines the reliability test using the Cronbach's Alpha (α) to ensure the validity of the instruments used to evaluate the aim. Accordingly, the outcome, reported in Table 1(Panel B), shows the overall Cronbach's Alpha is 0.99, which is higher than the theoretical benchmark (0.70). This indicates that the sixteen items on the study questionnaires appear to have a relatively good level of internal consistency and therefore deem sample is reliable.

Table 1.
Pre-estimation.

Panel A: Cases Process		
Cases	**N**	**%**
Valid	176	88.00%
Excluded[a]	24	12.00%
Total	200	100.00%
Panel B: Reliability test		
Statistic	#DF	α
Overall	16	0.99

Note: [a]Listwise deletion based on all variables in the procedure. The reliability rule for Cronbach's Alpha (α): $\alpha \geq 0.9$ (Excellence), $\alpha \geq 0.8$ (Good), $\alpha \geq 0.7$ (Acceptable), $\alpha \geq 0.6$ (Questionable), $\alpha \geq 0.5$ (Poor), $\alpha < 0.5$ (Unacceptable). #DF: Number of degrees of freedom.

The regression result of the model, which explicitly examined the impact of cybercrime activities on customer brand loyalty, is summarized in Table 2. The coefficient of financial losses was -0.342, which is statistically significant at 5%. This means that the client brand loyalty of the chosen banks will decrease by more than 34% for every percentage change in financial losses. The coefficient of card fraud was -0.113 and indicates that there will be a decrease of more than 11% in the client brand loyalty of the chosen banks for every percentage change in card fraud. However, this was not statistically significant.

The customer brand loyalty of the chosen banks will decrease by more than 60% for every percentage change in persistent security breaches, according to the coefficient of -0.608, which is statistically significant at 0.5%. The identity theft coefficient was -0.605, which is statistically significant at 0.5%. This means that for every percentage change in identity theft, the chosen banks' customers' brand loyalty will decrease by more than 60%. Considering the reported coefficient for constant, the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4281-4290, 2024
DOI: 10.55214/25768484.v8i6.2929

adopted variables are jointly significant at the 5% level of significance in explaining the dependent variables.

The dependent variable and predictors have significant association, as shown by the adjusted multiple correlation coefficients ($\bar{R}^2$) of 0.884, inferring that financial losses (FL_i), card fraud (CF_i), persistent security breaches (PSB_i), identity theft (IT_i) account for 88.4% of the variation in the customers' brand loyalty, leaving the remaining 11.6% as variations from the residuals.

Table 2.
Regression result for equation 2.

Variable	Coef.	Estimates	σ	t-stat	$pr(t$-stat$)$
Const.	β_0	-0.706	0.303	-2.330	0.005
FL_i	β_1	-0.342	0.084	-4.071	0.000
CF_i	β_2	-0.113	0.064	-1.766	0.118
PSB_i	β_3	-0.608	0.054	-11.259	0.000
IT_i	β_4	-0.605	0.225	-2.689	0.002
$\bar{R}^2$		0.884			
F-stat.		42.61			
Prob(F-stat.)		0.000			

Note: Const. is Constant term. Coef. is coefficient of each variable in equation (1). The reported coefficients are the Ordinary Least Squares (unstandardized) Estimates. σ is the standard error for each estimate, Pr (t-stat.) is the p-value for each t-statistic. $Coef$ & Apr (Coefficient and apriori sign). σ *is the* Standard deviation for each estimate. $\bar{R}^2$ is the R-square (Adjusted) and the figures in parenthesis are estimates are the p-values, using $prob|t| = 0$. *p ≤ 1%; **p ≤ 5%; ***p ≤10%.

Table 3 further displays the model summary describing the model's goodness of fit. The overall p-value is 0.000, which is less than the significance level of 0.05. Clearly, with the F-Statistics (320.120), the overall model is highly statistically significant at 1%, suggesting that the outcome is well predicted by the regression model. The study shows a good relationship between customer brand loyalty and the associated cybercrime activities, based on the reported coefficients for each of the adopted factors.

Table 3.
Model estimation summary (ANOVA).

Component	Σ^2	m^2	F-stat	$pr(F$-stat$)$
Regression $\left[n\sum_{i=1}^{k}(\bar{y}_{i.}-\bar{y}_{..})^2\right]$	73.106	30.137	320.120	0.000
Residual $\left[\sum_{i=1}^{k}\sum_{j=1}^{n}(y_{ij}-\bar{y}_{i.})^2\right]$	32.102	0.075		
Total $\left[\sum_{i=1}^{k}\sum_{j=1}^{n}(y_{ij}-\bar{y}_{..})^2\right]$	105.208			

Note: Predictors: (Constant), financial losses, card fraud, Persistent security breaches, identity theft. B. Dependent Variable: customer brand loyalty of the selected banks. F-stat; F-statistics, pr(F-stat): Probability of F-stat. Σ^2: Sum of square; $\bar{R}^2$-Adjusted R^2; m^2: Mean Square. $\sum_{i=1}^{k}\sum_{j=1}^{n}(y_{ij}-\bar{y}_{..})^2 = n\sum_{i=1}^{k}(\bar{y}_{i.}-\bar{y}_{..})^2 + \sum_{i=1}^{k}\sum_{j=1}^{n}(y_{ij}-\bar{y}_{i.})^2$

In summary, the result of the regression shows the following. First, the paper identifies a strong inverse association between brand loyalty and financial losses brought on by cybercrime. Clients who had financial setbacks were less likely to stick with their bank. Second, the evidence shows that card theft significantly reduces brand loyalty. Consumers who had their cards stolen were more likely to move banks. Third, the study discovered that recurring security vulnerabilities significantly reduce brand loyalty. The trust and loyalty of customers significantly declined because of repeated breaches. Forth, the paper demonstrates that the most notable adverse effect on brand loyalty was caused by identity theft. Customer loyalty was greatly diminished by identity theft's seriousness and enduring effects. Clients who were victims of cybercrime situations stressed how crucial the bank's response was in determining how loyal they would be.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4281-4290, 2024
DOI: 10.55214/25768484.v8i6.2929

The analysis shows how seriously cybercrime affects consumers' brand loyalty. Decreases in brand loyalty can have a negative impact on deposit money banks' overall performance, and they can be caused by a variety of factors, including financial losses, identity theft, card fraud, and security lapses. While these effects range in intensity, identity theft and security breaches have the biggest impact. The study also emphasizes how critical it is to respond to cybercrime situations effectively. If any security breaches, banks with a strong client base are those that can promptly detect and fix these problems.

5. Conclusions

Worldwide, electronic services present more prospects for corporate growth, and there are still a lot of uncharted territories to be discovered. Cybercrimes, however, pose a severe danger to corporate growth, especially in the online banking services sector. This article examines how the brand loyalty of the banks' customers is affected by cybercrime associated to the use of e-banking platforms. A regression analysis was performed to investigate the relationship between customer brand loyalty and the considered cybercrime activities. The empirical evidence discovered existence of a reciprocal relationship between the customer brand loyalty of the chosen banks and the adopted surrogates for cybercrime operations. The banking industry's clients' brand loyalty is seriously threatened by cybercrime. To lessen the negative effects of cybercrime on consumer loyalty and trust, deposit money banks need to give cybersecurity top priority and improve their reaction plans. They can protect their brand and keep customers loyal by doing this, which will eventually improve their performance. It follows that the money that banks should receive from e-banking services will inevitably decrease because of the public's diminished trust brought on by cybercrime operations, thereby endangering the banks' ability to remain financially stable.

Based on the findings, the paper offers some recommendations. First, the styd suggest the need to strengthen cybersecurity protocols. The Nigeria banks should make investments in cutting-edge cybersecurity procedures and tools to stop fraud and safeguard client information. Also, the paper offers there should be enhanced incident response. This will help to minimize the impact on client loyalty from cybercrime occurrences, banks should create and implement efficient incident response plans. Furthermore, there should be improvement in customer education amongst the banks, to help instruct their clientele on how to avoid becoming victims of cybercrime as well as the finest ways to defend themselves against it. Lastly, the paper offers the need for frequent audits. Doing this will help to find and fix system vulnerabilities, banks should carry out frequent security audits.

References

[1] Adeyemi, I (2021). Impact of ICT tools for combating cybercrime in Nigeria online banking: A conceptual Review. *International Journal of Finance*, 3(6), 180-188.

[2] Ahuja, A.V. (2010). Cybercrime in banking sector. Available at http://www.scribd.com/doc/28079943/Cyber-Crime-in-Banking-sector, p.6

[3] Ajibola, O. (2023). Impact of cybercrime on customer brand loyalty in Nigeria. *Journal of Policy and Development Studies*. 9 (1), 179-193.

[4] Akanji, O.O. (2022). The role of microfinance in empowering women in African. *International Journal of Business*, 2(2), 159-178.

[5] Central Bank of Nigeria (2015). Improving and securing the cyber-environment. *Nigerian e-Fraud Forum Annual report.*

[6] Chen, Y.S., Chen, T.J, & Lin, C.C. (2016). The Analyses of Purchasing Decisions and Brand Loyalty for Smartphone Consumers. *Open Journal of Social Sciences*, *04*(07), 108–116. https://doi.org/10.4236/jss.2016.47018

[7] Chuenban, P., Sornsaruht, P., & Pimdee, P. (2021). How brand attitude, brand quality, and brand value affect Thai canned tuna consumer brand loyalty. *Heliyon*, *7*(2). https://doi.org/10.1016/j.heliyon.2021.e06301

[8] Chung, Y., & Kim, A. J. (2019). Effects of mergers and acquisitions on brand loyalty in luxury Brands: The moderating roles of luxury tier difference and social media. *Journal of Business Research.*

[9] Dada, G. (2020). Organized cybercrime and bank account takeovers. *Federal Reserve Bank of San Francisco, Division of Banking Supervision and Regulation.*

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4281-4290, 2024
DOI: 10.55214/25768484.v8i6.2929

[10] Daily Post News (2017). Senate: Nigeria losses N127billion annually to cybercrime. Online at: *dailypost.ng/2017/03/08*.
[11] Florêncio, D. & Herley, C. (2010). Phishing and money mules. In Information Forensics and Security WIFS, *IEEE International Workshop*. 1-5.
[12] Fred, B., Brian, B. & Gene, L. (2014) Organized cybercrime and bank account takeovers. *International* Journal *of Finance*, 2(2) ,609-630.
[13] Imran, M. (2022). Impact of electronic crime in Indian banking sector – An overview. *International Journal of Business and Information Technology*. 1(2), 401-424.
[14] Inês, S. & Alexandra, S. (2023). Financial institutions and cybercrime: Threats, challenges and opportunities. *International Journal of Business* 1(4), 304-321.
[15] Ishmael, M., Shingirai, G., Martin, M. & Rufaro, C. (2023). Cybercrime - The emerging threat to the financial services sector in Zimbabwe. *Mediterranean Journal of Social Sciences*, 7(3), 500-522.
[16] Kataria, S., & Saini, V. (2020). The mediating impact of customer satisfaction in relation of brand equity and brand loyalty: An empirical synthesis and re-examination. *South Asian Journal of Business Studies*, *9*(1), 62–87. https://doi.org/10.1108/SAJBS-03-2019-0046
[17] Kaur, H., Paruthi, M., Islam, J. U., & Hollebeek, L. D. (2020). The role of brand community identification and reward on consumer brand engagement and brand loyalty in virtual brand communities. *Telematics and Informatics*, *46*, 101321.
[18] Khairi, A., Bahri, B., & Artha, B. (2021). A Literature Review of Non-Performing Loan. *Journal of Business and Management Review*, *2*(5), 366–373. https://doi.org/10.47153/jbmr25.1402021.
[19] Kim, J., Lee, H., & Lee, J. (2020). Smartphone preferences and brand loyalty: A discrete choice model reflecting the reference point and peer effect. *Journal of Retailing and Consumer Services*, *52*(May 2019), 101907. https://doi.org/10.1016/j.jretconser.2019.101907
[20] Muthukumaran, B. (2008). Cyber crime scenario in India. *Criminal Investigation Department Review*, January, pp.17-23.
[21] Nair, O.S. & Nair, E.G. (2022). Impact of cyber policies on customer satisfaction in India. *Journal of Research in International Business Management*. 1(4), 251-257.
[22] Ogbabu, T. & Usman, A. (2022). Impact cyber fraud on customer loyalty and banks profitability in Keyan. *Journal of Business Theory and Practic*. 3(1), 202-225.
[23] Olayemi, B. (2023). Cybercrimes in Nigeria: Analysis, detection and prevention. *FUOYE Journal of Engineering and Technology*, 1 (1).
[24] Olufunke, O.O. (2010). *Computer Crimes a*nd Counter Measures in the Nigerian Banking *Sector*. Journal of Internet Banking and Commerce, April, Volume 15, Issue no.1, p.2.
[25] Raghavan, R. & Latha, P. (2014). The effect of cybercrime on a Bank's finances. *International Journal of Current Research and Academic Review*, 2(2), 173-178.
[26] Salami, I. (2023). Cyber-banking fraud risk mitigation: Conceptual model. *Banks and Bank Systems*, 10 (2).
[27] Sanchi, A. (2016). Cybercrime in banking sector. *Research Journal of Management Sciences*. 3(4), 140-152.
[28] Seema, G. (2016), Cybercrime: A growing threat to Indian banking sector. *International Journal of Science Technology and Management*, *5* (12), 200-220.
[29] Sharma, A.K. & Nanda, G.L (2006). Frauds in Credit Card Business. Banking Finance, Volume, Issue no.7, p.15.
[30] Shewangu, D. (2022). Cyber-banking fraud risk mitigation: Conceptual model. *Banks and Bank Systems*, 10(2),180-201.
[31] Wada, F. (2022). Electronic banking and cybercrime in Nigeria - A theoretical policy perspective on causation. *African Journal of Computing and ICT*, 4(3),130-146.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4281-4290, 2024
DOI: 10.55214/25768484.v8i6.2929

Appendix

QUESTIONNAIRE
Instruction: Please tick (√) as appropriate in the space provided.

Section A: Demographic Data
1. Age: 18-29 ( ) 30 - 49 ( ) 50 and Above ( )
2. Gender: Male ( ) Female ( )
3. Marital status: Single ( ) Married ( )
4. Occupation: Civil servants ( ) Corporate employee ( ) Entrepreneur ( ) Student ( )

Section B: Operational Information

S/N	**STATEMENT**	**Strongly Agreed**	**Agreed**	**Indifference**	**Disagree**	**Strongly Disagreed**
	A. The relationship between financial losses to cybercrime and customer brand loyalty.					
1.	Financial losses to cybercrime reduce the level of customer confidence in banks.					
2.	Financial losses to cybercrime prevalence changes consumers' disposition to online banking.					
3.	I have changed my bank because of my financial losses to cybercrime.					
4.	Financial losses to cybercrime prevalence do not affect my disposition to using e-banking.					
	B. The effect of card fraud by cybercriminal on customer brand loyalty.					
5.	Card theft affects my loyalty to the brand associated with the card.					
6.	Card theft has a significant impact on customer disposition to e-banking usage.					
7.	Customers prefer to withdraw through the canter to ATM for the fear of Card theft.					
8.	I prefer not to have an ATM card for the fear of card theft.					
	C. The effects of persistent security breaches by cybercriminals on customer brand loyalty.					
9.	Persistent security issues reduce my trust in a brand's services.					
10.	I have changed my bank because of my cybercrime experience.					
11.	I am less likely to remain loyal to a brand that consistently faces security threats.					
12.	Continuous security breaches make me consider switching to another brand.					
	D. The relationship between identity theft by cybercriminal and customer brand loyalty.					
13.	I would stop using a brand's services if my card information was stolen in bank.					
14.	Identity theft by cybercriminal makes me question the reliability of the brand's security measures.					
15.	Identity theft cases make me doubt my bank ability to protect my information.					
16.	Cases of identity theft affect my disposition to using e-banking.					

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4281-4290, 2024
DOI: 10.55214/25768484.v8i6.2929