Innovations

Financial Institutions Cyber Security Incidents and Economic Growth of Nigeria

Kemdi Lugard Okoroiwu
Accountancy Department, University of Nigeria, Enugu Campus, Nigeria

Chinwe R. Okoyeuzu
Department of Banking and Finance, University of Nigeria, Enugu Campus, Nigeria

Wilfred Isioma Ukpere
1Department of Industrial Psychology and People Management, University of Johannesburg, Johannesburg, South Africa

Correspondence Author: **Wilfred Isioma Ukpere**

Abstract : *This study investigated the impact of cybersecurity incidents on Nigeria's economic growth, focusing on the banking sector from 2002 to 2022.The study examined the impact of automated teller machine fraud (ATMF) and web-based fraud (WBF) on Nigeria's Gross Domestic Product (GDP), addressing key research questions about how these types of fraud influence the GDP. Utilizing an ex-post facto research design and time series data analysis, the research study analyzed data sourced from the Nigeria Deposit Insurance Corporation (NDIC) and the Central Bank of Nigeria (CBN). The descriptive statistics revealed positive and high values for both measures of cybersecurity incidents and economic growth, indicating the critical nature of cybersecurity issues for Nigerian banks. The findings show that ATM fraud and web-based fraud experience significant levels of variation, suggesting notable volatility; however, there is no statistically significant effect of these fraud types on Real GDP. This implies that, despite their volatility, ATMF and WBF do not significantly influence broader economic measures owing to the mitigating mechanisms present in the Nigerian economy. The study underscores the resilience of the Nigerian economy against certain cybersecurity threats, while emphasizing the necessity for targeted measures against specific fraud types that pose significant risks to economic stability. To address these concerns, the study recommends enhancing security measures for fraudulent transfers, developing comprehensive cybersecurity training programs,*

implementing robust regulatory frameworks, investing in advanced cybersecurity technologies, and promoting collaboration within the industry.

Keywords: *Financial Institutions, Cyber Security, Incidents, Economic Growth, Nigeria*

1. Introduction

Financial institutions have become more dependent on information and communication technologies (ICT) to conduct their operations and to provide services to clients in the current digital transformation age. However, this dependence has also made financial institutions attractive to cybersecurity. Cybersecurity incidents can be described as events that affect information systems, resulting in unauthorised access, disclosure, or disruption of data (Tatar et al., 2024). Cybersecurity threats pose a danger to a nation's economic growth, since these undermine the public's confidence in financial organisations, interrupt commercial operations, and stifle innovation. Cybersecurity has been directed towards critical financial infrastructure such as payment systems and clearing houses. These occurrences have affected financial operations and have interfered with firms' normal operations (Ma, 2021). The disruption has impacted the economy in a way that has seen companies unable to pay their suppliers or receive payments from their customers. The disruption has led to stoppages in production, disruption of the supply chain and a slowdown of the economy (Srinivas et al., 2019). It has also slowed down advancement of the financial industry by shifting attention and funding from research and development projects to cybersecurity measures (Pollmeier et al., 2023).

When financial institutions focus on the resolution of cybersecurity problems, they can devote less attention to the creation of new financial products and services. This hampers the pace of innovation and limits the availability of new financial products for businesses and customers. Lack of innovation hinders economic growth because it limits the number of new financial products and services that can enhance productivity and efficiency. The role of financial institutions in encouraging economic growth cannot be overemphasised, as they provide access to funds, facilitate monetary operations, and promote financial access. However, the increasing rate of cybercrimes, including different types of crimes such as ATM fraud and web-based fraud, poses a great threat to Nigeria's economic development.

ATM fraud victims lose their ability to use money for transactions and to purchase goods and services, as well as other essential financial activities (Wang et al., 2020). In addition, this disruption has led to corporate events being postponed, lost business, and reduced economic output (Wang et al., 2020). Furthermore, Web-based fraud, including phishing fraud, online identity theft, and e-commerce fraud,

has become more sophisticated, focusing on customers' financial data and interrupting online purchases (Mogaji& Nguyen, 2022). As a result, individuals have lost money, while financial institutions have lost customers' trust in online transactions, and the growth of e-commerce, a major driver of economic growth, has been hindered (Eboibi, 2017).

1.1 Research objectives

The current study's research objectives are outlined below:

- Examine the impact of ATM fraud on Nigeria's Gross Domestic Product (GDP).
- Ascertain the impact of web-based fraud on Nigeria's Gross Domestic Product (GDP).

2. Literature review

The nexus between cyber security breach in financial institutions and economic growth in Nigeria has, therefore, assumed a new perspective owing to the upsurge in the incidence of cyber threats. Being one of the biggest economy in Africa,Nigeria depends a lot on its financial institutions for economy stability and expansion. According to CBN and NDIC, there has been a rise in cybercrimes in Nigerian financial institutions, resulting in massive money losses, as well as customer confidence losses. Cybersecurity incidents have immediate consequences for these institutions, which include direct losses, disruptions of operations, and reputational losses that have led to reductions in investments, whilst also limiting overall development of the sector (Natalucci, Qureshi and Suntheim, 2024). Furthermore, the fragility of cybersecurity within the financial sector has larger implications for Nigeria's economic growth, as financial institutions play a vital role in facilitating investments and providing capital. In response, the Nigerian government has implemented initiatives such as the National Cyber Security Policy and Strategy to improve the nation's cybersecurity framework (OkeomaOnunka et al., 2023). However, challenges regarding policy enforcement and the necessity for continuous awareness and training, persist.

Akintoye et al.'s (2022) study examined how cybersecurity affected financial innovation in Nigerian Deposit Money Banks. Given that Nigeria is one of the most populatedBlack countries, with a reasonably high incidence of financial literacy, it aims to determine the impact of cybersecurity on the uptake and the efficacy of financial innovations. The current research study was restricted to the Deposit Money Banks in Nigeria, and of the 56 senior staff members from different departments that were identified in the sample frame, a total of 53 were selected, representing 93% of the market capitalization as at 31December 2021. The findings indicate that cybersecurity, especially, risk management and bank monitoring related positively to FI with an Adjusted $R^2 = 0.447$; $F = 23.274$; $p < 0.05$. Based on the

study's findings, it is suggested that Deposit Money Banks should review their risk management framework at least annually to address new risks that may emerge from the development of new products, and to enhance the credibility of e-banking channels for financial transactions.

Additionally, Juneja, Shankha, and Mondal (2024) examined the connection between hazards associated with the digital economy. This connection emphasized how important it is to safeguard against, recognize, and manage risks, including cyberattacks, data leaks, and idea and concept theft. The said authors concluded that although the digital economy has enormous opportunities for growth and innovation, the industry's sustainability and security depend heavily on investments in infrastructure, capacity, and awareness. Similarly, None et al.'s (2023) study on the challenges and cybersecurity threats in digital economic transformationhighlighted how technology has allowed global business to experience tremendous growth in the volume of international business; however, at the same time, organisations are facing several threats because of their over reliance on technology and GVCs. The most prominent of these risks is cybersecurity, which manifests in various forms, with negative effects on the affected individuals. This reality turns cybersecurity into a competitive advantage for organisations and into a prerequisite for sustainable economic growth. Using a large corpus of data, mostly from court cases, cybersecurity reports, and press releases, the study assumed an empirically informed theoretical approach and analyzed the primary cybersecurity risks, which were divided into three main categories: loss of trade secrets; loss of property; loss of stocks; and payment fraud. Examples from real-world situations were used to illustrate the main issues in each category. The study proposed that the state should strengthen its cybersecurity procedures, frameworks, and programs.

In addition, Vasiu and Vasiu (2018) outline cybersecurity as a prerequisite for sustained economic growth, accounting for global commerce, the utilization of digital services, and intricate supply chains. Using examples from court cases, cybersecurity reports, and press releases, the study categorized cybersecurity risks into three groups: financial fraud; harm; and theft of company secrets. In addition to their recommendations, the findings highlighted the importance of enhancing cybersecurity in enterprises by illustrating the extent of the suffering caused by such threats.

3. Research Methodology &Design

The current study's research methodology analyzed the collected data to determine the link between two or more factors without controlling the variables (Busk, 2017). Analysis of historical data on cyber security breaches in Nigeria's financial institutions and their effects on RGDP was conducted by using the ex-post facto research approach. This research design was useful for this study because it

involves the use of data to search for a relationship between two or more variables without manipulating the variables.

3.1 Population and Sampling

The population of the study comprised all the listed and trading financial institutions on the Nigerian Exchange Group (NGX) from 2002 to 2022 to obtain the required financial data, as well as the Central Bank of Nigeria to obtain the reported Real Gross Domestic Product (RGDP) from 2002-2022. This periodwould allow for deep and rich analysis and would present a data-driven and policy-relevant periodto examine the correlation between cyber security threats and economic development in Nigeria. It would also provide valuable analyses to help shape policies, enhance security measures, and foster economic growth in the context of emerging cyber threats

The study focused exclusively on annual bank fraud and forgery cases, as reported by the NDIC from 2002-2022, including all cybersecurity incidents reported by the NDIC during this period and the annual RGDP, as reported by the CBN from 2002-2022. Focusing solely on banks listed on the NGX would provide a well-defined, representative, and strategically relevant sample to assesscyber security occurrences in Nigeria's banking sector.

3.2 Model specification

The study developed the following model specifically to address the research objectives:

Real GDP=$\beta 0+\beta 1$ (AF) +$\beta 2$ (WBF) +ϵ.

Explanation of the variables

Dependent variable

Real Gross Domestic Product (Real GDP)

This refers to the dependent variable representing Nigeria’s overall economic growth. It can be measured by using various indicators such as RGDP growth, employment rate, poverty rate, or other relevant economic growth metrics. The current study adopted RGDPonly.

Independent Variables

ATM Fraud (AF)

This variable represents instances of fraud that occur through Automated Teller Machines (ATMs). It includes unauthorized withdrawals, card skimming, or any other fraudulent activity related to ATM transactions.

Web-based Fraud (WBF)

This variable refers to fraud that is conducted through web-based platforms. It encompasses a range of online fraudulent activities, including phishing, identity theft, online fraud, or any illicit activities that occur via the internet.

Error Term (ϵ)

This term captures the unobserved factors or errors in the model that are not explained by the included independent variables. It represents the difference between actual economic growth and predicted economic growth

4. Data presentation and results

Table1: Processed data of variables

	Independent Variables		Dependent Variables
YEAR	**AF (₦'bn)**	**WF(₦'bn)**	**REAL GDP(₦'bn)**
2002	342.39	23.63	136853
2003	2632.45	160.15	147136.7
2004	547.02	45.56	159937
2005	628.82	235.75	169527.3
2006	282	375	178666.2
2007	628.82	235.75	189250.8
2008	4028	235	200834
2009	1282	1355	216164.8
2010	2882	575	235823.1
2011	882	575	247478.6
2012	52	295	257718.9
2013	18	205	271271.8
2014	67	297	288384.2
2015	67	146	295632.7
2016	21	179	289870.5
2017	49	89	292447.6
2018	642	11	298162.6
2019	8	11	304958.6
2020	165	611	298925.9
2021	331	204	309046.4
2022	4	3068	318178.5

Source: Forgery and fraud cases reported byNDIC from 2002-2022 and RGDP reported by the CBN from 2002-2022

Table 1 above indicates that there is no relationship between the ATM fraud and GDP growth. Even though ATM fraud spiked significantly during certain years, theincreases do not always correspond with trends in the GDP. This inconsistency might be owing to various factors such as improvements in ATM security or the nature of ATM fraud itself, which may not always be tieddirectly to the overall state of the economy.

Table 2:Descriptive statistics on dependent and independent variables

Descriptive statistics			
Descriptives	**lnATMF**	**lnWBF**	**lnReal GDP**
Mean	2.311626858	2.279242486	5.3714509059
Std. Error of Mean	0.185761141	0.133548790	0.0258457837
Median	2.519827993	2.371067862	5.4111462353
Mode	1.826074802	1.041392685	5.1362543221
Std. Deviation	0.851264493	0.611997442	0.1184402605
Variance	0.725	0.375	0.014
Skewness	-0.391	-0.491	-0.692
Std. Error of Skewness	0.501	0.501	0.501
Kurtosis	-0.693	0.520	-0.936
Std. Error of Kurtosis	.972	.972	.972
Range	3.003029470	2.445462670	0.3664164533
Minimum	0.602059991	1.041392685	5.1362543221
Maximum	3.605089461	3.486855355	5.5026707754
Sum	48.54416403	47.86409222	112.80046902
Sum Square Deviation	14.49302	7.490871	0.280562
Jarque-Bera	1.036675	0.741608	2.315043
Probability	0.595510	0.690179	0.314264
Observations	21	21	21

Source: Researcher (2024) SPSS (v.25) and EViews (v.12) Outputs

According to the above table, ATM Fraud (lnATMF)shows high variability and a wide range of values. The distribution is slightly negatively skewed and flat (kurtosis is negative), with a significant difference between the minimum and maximum values.Web Fraud (lnWBF)hasa lower variability than ATM fraud but still shows a notable spread. It has a slightly negative skewness and a positive kurtosis, indicating a somewhat more peaked distribution.Real GDP (lnReal GDP)exhibits low variability and a narrow range. The distribution is also negatively skewed with a flat kurtosis, indicating that lower values are more frequent.

The descriptive statistics reveal distinct patterns in the data for ATM fraud, web fraud, and Real GDP. ATM fraud displays considerable variability and a wide range of values, with a slightly left-skewed and flatter distribution. Web fraud, while less

variable than ATM fraud, shows a moderate left skew and slightly peaked distribution. Real GDP values are stable, with low variability and a distribution that is close to normal.

Table 3: Results of correlation matrix

Correlation t-Statistic Probability	lnRealGDP	lnATMF	lnWBF
lnRealGDP	1.000000		
lnATMF	-0.610087 -3.356295 0.0033	1.000000	1.000000
lnWBF	0.122762 0.539187 0.05960	0.029268 0.127631 0.8998	1.000000

Source: Researcher (2024)Eviews (v.12) output

According to Table 3 above, there is a moderate negative relationship between the natural log of Real GDP and the natural log of ATM fraud. A correlation coefficient of -0.6101 indicates a significant inverse association. This illustrates that as the real GDP rises, ATM fraud falls, and vice versa. The t-statistic of -3.3563 and the p-value of 0.0033 show that this link is significant at the conventional levels of significance (0.05 or 0.01). This implies that, given the results obtained, it is not possible to attribute the negative correlation observed by chance alone.

When presented in natural log form, the link between Real GDP and web fraud is positive but weak, with a coefficient of 0.1228. This suggests a minor favorable association. Web fraud increases in tandem with real GDP, but the relationship is weak. The t-statistic of 0.5392 and the p-value of 0.0596 show that while not significant at the 0.05 level, this association is nearly significant. It means that the correlation is positive but weak, which does not imply a significant causal relationship.

Unit root tests for stationarity

To proceed with the analysis and data, the researcher investigated the stationary and order of integration of all study variables in the time series data set. To evaluate whether a given time series is stationary, the researchers utilized an econometric approach known as the unit root test. Some of the standard tactics include Augmented Dickey-Fuller (ADF), Dickey-Fuller (DF), and Phillips-Perron (PP). To

determine stationarity, the Augmented Dicky-Fuller Unit Root test was utilized. This is because the Augmented Dickey-Fuller Unit Root Test (ADF) use conventional least squares regression estimates at the 0.05 level. The test results indicated a negative augmented Dickey-Fuller (ADF) statistic. The lower the statistic's value, the stronger the evidence against the null hypothesis of the existence of a unit root at a certain level of significance.

H_0: There is a unit root (the series is not stationary).

H_1: There are no unit roots (the series is stationary).

Table 4: Augmented Dicky-Fuller unit root tests for stationarity

Variables	Level		1st Difference		2nd Difference	
	Intercept	Trend & Intercept	Intercept	Trend & Intercept	Intercept	Trend & Intercept
RealGDP	0.2009	0.9773	0.0982	0.1311	0.0029	0.0159
Web-based Fraud	0.1112	0.1674	0.0001	0.0005	0.0000	0.0000
ATM Fraud	0.0401	0.0200	0.0000	0.0000	0.0002	0.0012

Source: Researcher (2024)Eviews (v.12)

Table 4 above shows that the RealGDP data series was non-stationary at level and first difference for both intercept and trend but stationed at second difference for both intercept and trend and intercept. At level, the outright steal data series was non-stationary, but at first and second differences, it was stationary. The data set was deemed to be stationary, necessitating cointegration tests. These differences in the order of estimation (mixed order) show that the most suitable model of estimation would be Autoregressive Distributed Lag Model (ARDL) because of its ability to accept each of the variables, notwithstanding their integration order.

H_0: Cointegration does not exist.

H_1: Cointegration does exist.

ARDL Model Specification Tests

Since the degree of cointegration varies across the variables, the ARDL Model Specification Test was used to begin this process and to ascertain whether the variables are long-term and co-integrated with one another. To determine whether either or both the trend and the constant were statistically significant for the ARDL estimation, the test was conducted, using the Alaike info criterion (AIC), which is an estimator of the prediction error and, consequently, the relative quality of statistical models for a given set of data.

Table 5: ARDL model specification test (Constant & Trend)

Variable	Coefficient	St. Error	t-Statistic	Prob.
C	0.558309	0.303798	1.837762	0.1157
@Trend	0.000335	0.000995	0.336258	0.7481

Source: Researcher (2024) Eviews Output (v.12)

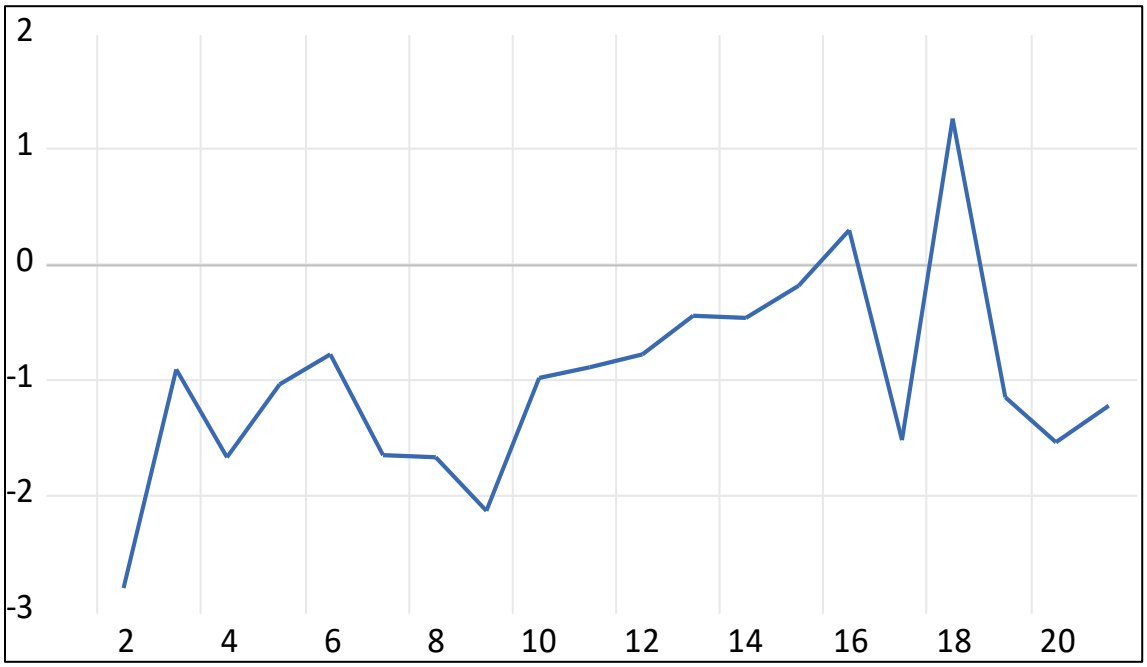
The result of the estimation showed that the constant (p = 0.1157) and the trend (p = 0.7481) values were not significant. Therefore, both constant and trend were not included in the ARDL specification model. To determine the model, the Error Correction measure (ECM) Test was conducted to determine the bound test results, as well as the short-run result of the ARDL.

Table6:Cointegration Tests

F-Bounds		Null hypothesis: No levels relationship			
Test Statistic	Value	Significance	I(0)	I(1)	
F-Statistic K	31.80802 6	10% 5% 2.5% 1%	1.75 2.04 2.32 2.66	2.87 3.24 3.59 4.05	
Variable	Coefficient	Std. Error	t-Statistic	Prob.	R^2
CointEq(-1)	-0.018978	0.001038	-18.27523	0.0000	0.843494

Source: Researcher (2024) Eviews Output (v.12)

Figure 4.1: Cointegration graph



Source: Researcher (2024) E-views (v.12) output

The F-Statistic value shown in Table 6 above is 31.80802 at the5% level of significance, which is higher than the upper bound of 3.24 and the lower bound of 2.04. This suggests that there is a long-term co-integration between the independent variables of financial institutions' cybersecurity and the dependent variable, economic growth (RealGDP). Given that it is cointegrated, this implies that the study's model passes the cointegration criteria. A further look at the results in Table 6 reveals that the one period lag error correction term (CointEq (-1)) is negative, less than one, and significant at the one percent level. The coefficient of error correction of 1.89%, however, shows that the rate of adjustment from the short run to the long run is negligible in the case of model disequilibrium. However, the coefficient of determination, or R-Squared, of 0.843494 shows that the model has an 84.3% good match.

Estimated ARDL results for long run and short run dynamics

This section contains the estimated ARDL results for analysis of the effects of financial institution cybersecurity incidents on Nigeria's economic growth between 2002-2022. The model shows that the short run effects of the independent variables of financial institutions' cybersecurity fraud found a statistically significant effect for fraudulent transfers on RealGDP (β = -0.005; $p < 0.05$). Long-term consequences revealed that web-based fraud (WBF) had no statistically significant impact on

RealGDP (β = -0.005; p > 0.05) and ATM fraud (PFC) had no statistically significant impact on RealGDP (β = 0.000; p > 0.05).

Table7: Long run and short run ARDL results

Results of the ARDL Long Run Relationship				
Variables	Dependent Variable: lnGDP			
	Coefficient	Standard Error	T-Statistic	Probability
InRealGDP(-1)	-0.120366	0.014699	-8.188771	0.0001
InWBF	-0.004956	0.002368	-2.092412	0.0747
InATMF	0.000309	0.001648	0.187255	0.8568
Results of the ARDL Short Run Relationship				
Variables	Dependent Variable: lnGDP			
	Coefficient	Standard Error	T-Statistic	Probability
InRealGDP(-1)	0.981022	0.003977	246.7047	0.0000
InWBF	-0.004956	0.001144	-4.331817	0.0034
InATMF	0.000309	0.000851	0.362548	0.7276

Source: Researcher (2024)Eviews (v.12) output

Model determination of Hypothesis One

Implicit model: RealGDP= f (ATMF):

Where: RealGDP is the overall real gross domestic product of Nigeria between 2002-2022;

ATMF refers to actual losses accruing from ATM fraud in banks.

Proposed model: RealGDP = $\beta o + \beta_1 ATMF + e$.

Step One: Statement of Hypothesis

H_0: ATM fraud does not have an effect on Nigeria's RealGDP.

H_1: ATM fraud has an effect on Nigeria's RealGDP.

Step Two: Statement of decision criteria

The decision criteria are to reject H0 if the p – value of the coefficient of ATM fraud (ATMF) is less than 0.05; do not reject H0, if otherwise.

Step Three: Conclusion

As shown in Table 7, ATM fraud (ATMF) was insignificant in relation to RealGDP (β = 0.000; p > 0.05). Since the probability value is greater than 0.05, then the null hypothesis is rejected. This implies that ATM fraud does not affect Nigeria's RealGDP, overall.

Model determination of Hypothesis Two

Implicit model: RealGDP= f (WBF)

Where: RealGDP is the overall real gross domestic product of Nigeria between 2002-2022;
WBF refers to actual losses accruing from web-based fraud suffered by banks.
Proposed model: RealGDP = $\beta o + \beta_1 WBF + e$
Step One: Statement of Hypothesis
H_0: Web-based fraud does not have an effect on Nigeria's RealGDP;
H_1: Web-based fraud has an effect onNigeria's RealGDP.

Step Two: Statement of decision criteria
The decision criteria are to reject the null hypothesis (H0) if the p – value of the coefficient of web-based fraud is less than 0.05; and not to reject the null hypothesis (H0) otherwise.
Step Three: Conclusion
Table 7 shows that WBF has no relationship with RealGDP as the coefficient is (-0.005) and the p-value is greater than 0.05. According to the calculated probability value, which is more than 0.05, the null hypothesis is rejected. It may, therefore, be concluded that,overall, web-based fraud does not affect Nigeria's RealGDP.

5. Discussion of findings

Hypothesis One: ATM fraud has a statistically significant effect on Nigeria's RealGDP

In the first hypothesis, the objective was to assess the impact of ATM fraud on Nigeria's RealGDP. The analysis of the above findings revealed that ATM fraud (ATMF) had a significant influence on RealGDP ($\beta = 0.000$; $p > 0.05$). This means that at the 5% level of significance, ATM fraud did not in any way determine the RealGDP levels between 2002 and 2022. This result could be because fraud may have a temporary effect on the economy, but after a while the negative effects of this fraud are supplemented by positive economic growth. This is evidenced by the statistically significant coefficients of the majority of the independent variables of the study on the RealGDP. Despite this result, evidence from extant literature is replete with mixed results on how ATM fraud can affect banks as well as the economies in which they operate. For instance, Adepoju and Alhassan (2010) highlight incidences of fraud across some banks that are operational in Minna, Niger State, and showed that reasons for ATM fraud include: location of the ATM at secluded and high-risk areas; PIN theft and shoulder surfing; and the use of ATMs outside banks. Kaur and Mokha (2022) found that there are positive impacts of the use of the ATM in the Indian economy and recommends its continual usage within the country. However, the study also highlighted that with the rising use of ATMs in India, there are also rising cases of ATM fraud, most poignant of which is skimming – a situation where

fraudsters steal information from customers' ATM cards by placing skimming devices in ATMs.

Hypothesis Two: Web-based fraud has a statistically significant effect on Nigeria's RealGDP

The second hypothesis was to assess the impact of web-based fraud on Nigeria's RealGDP. Analysis of the result in the study revealed that web-based fraud (WBF) had no significant impact on RealGDP ($\beta = -0.005$; $p > 0.05$). The impacts of fraud are diverse and may differ based on a country's political and financial institutions (Ahmad et al., 2021). Therefore, there might be other economic and political indicators within the economy that are more effective in affecting the GDP than the levels of fraud conducted online. This result is, however, contradicted by evidence from extant literature. Asokhia (2010) established that perceptions of cybercrimes, as rated by male and female respondents in local governments in Edo State, Nigeria, was different. According to Baker (1999), who examined fraud on the internet, there are three major areas that have potential to encourage fraudulent activities and conning people on the internet. Such areas are the growth of Internet companies, the development of electronic commerce, and the growth of securities and sales trading. But as these processes rise without proportionate measures to control and oversee activities on the internet, cases of internet fraud would increase and result in meager results for the economy. Manyika and Roxburgh (2011) argue that the internet has the capability to enhance the growth and development of a country's economy to the extent that the business, policy maker and government are willing to accept the great opportunities and prospects that the internet offers, whilst trying to manage various risks, which are associated with internet usage, particularly with reference to privacy, fraud and security threats.

6. Conclusion and recommendations

Analysis of the effect of cybersecurity incidents on Nigeria's economic growth, measured by RealGDP, yielded insightful findings on various forms of financial fraud. The study examined two hypotheses, focusing on several types of fraud and their impacts on RealGDP. The results indicate that automated teller machine fraud (ATMF) and web-based fraud (WBF) did not have a statistically significant effect on RealGDP, suggesting that despite their volatility, these types of fraud do not influence broader economic measures significantly owing to the economy's mitigating mechanisms.

Financial institutions should therefore implement enhanced security measures at ATM locations, including situating ATMs in well-monitored and secured areas, installing advanced surveillance systems, and promoting customer awareness programs on PIN protection and safe ATM usage practices.Policymakers and

financial institutions should focus on strengthening the overall cybersecurity infrastructure and regulatory framework, while simultaneously addressing broader economic and political factors that influence RGDP. This can include investing in advanced cybersecurity technologies, providing regular cybersecurity training for individuals and businesses, and enhancing legal measures to combat and deter web-based fraud effectively.

7. References

1. *Adepoju, A. S., & Alhassan, M. E. (2010). Challenges of automated teller machine (ATM) usage and fraud occurrences in Nigeria – A case study of selected banks in Minna Metropolis. Journal of Internet Banking and Commerce, 15(2), 1–11.*
2. *Ahmad, B., Ciupac-Ulici, M., & Beju, D.G. (2021). Economic and non-economic variables affecting fraud in European countries. Risks, 9(119), 1–17.*
3. *Akintoye, R., Ogunode, O., Ajayi, M. and Joshua, A.A. (2022). Cyber Security and Financial Innovation of Selected Deposit Money Banks in Nigeria. Universal Journal of Accounting and Finance, 10(2), pp.643–652.*
4. *Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. Journal of King Saud University - Computer and Information Sciences, 34(10), 8176–8206.*
5. *Asokhia, M. O. (2010). Enhancing national development and growth through combating cybercrime/internet fraud: A comparative approach. Journal of Social Sciences, 23(1), 13–19.*
6. *Baker, R. C. (1999). An analysis of advance fee fraud on the internet. Internet Research, 9(5), 348–360. Retrieved from ejournals.ebsco.com*
7. *Busk, P. L. (2017). Causal-Comparative Study. Wiley StatsRef: Statistics Reference Online, 1–2.*
8. *Eboibi, F. E. (2017). A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015. Computer Law & Security Review, 33(5), 700–717.*
9. *Juneja, A., Shankha Shubhra Goswami and Mondal, S. (2024). Cyber Security and Digital Economy: Opportunities, Growth and Challenges. Journal of Technology Innovations and Energy, 3(2), pp.1–22.*
10. *Kaur, J., & Mokha, K. A. (2022). Growth and impact of ATMs in India. Research Square, 1–12.*
11. *Ma, C. (2021). Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports, 7.*
12. *Manyika, J., & Roxburgh, C. (2011). The great transformer: The impact of the internet on economic growth and prosperity. In McKinsey Global Institute. Retrieved from www.iei.liu.se*
13. *Mogaji, E., & Nguyen, N. P. (2022). The dark side of mobile money: Perspectives from an emerging economy. Technological Forecasting and Social Change, 185,*

122045.

14. *Natalucci, F., Qureshi, M. and Suntheim, F. (2024). Rising Cyber Threats Pose Serious Concerns for Financial Stability. [online] IMF. Available at: www.imf.org*
15. *None Desta Lesmana, None Mochammmad Afifuddin and None Agus Adriyanto (2023). Challenges and Cybersecurity Threats in Digital Economic Transformation. International Journal of Humanities Education and Social Sciences, 2(6).*
16. *Okeoma Onunka, Ayoola Maxwell Alabi, Chiedozie Marius Okafor, Anwuli Nkemchor Obiki -Osafiele, Tochukwu Onunka and Chibuike Daraojimba (2023). Cybersecurity In U.S. And Nigeria Banking And Financial Institutions: Review And Assessing Risks And Economic Impacts. Acta Informatica Malaysia, 7(1), pp.54–62.*
17. *Pollmeier, S., Bongiovanni, I., & Slapničar, S. (2023). Designing a financial quantification model for cyber risk: A case study in a bank. Safety Science, 159, 106022.*
18. *Srinivas, J., Das, A. K., & Kumar, N. (2019). Government regulations in cyber security: Framework, standards and recommendations. Future Generation Computer Systems, 92(1), 178–188.*
19. *Tatar, U., Bilge Karabacak, Keskin, O. F., & Foti, D. P. (2024). Charting New Waters with CRAMMTS: A Survey-Driven Cybersecurity Risk Analysis Method for Maritime Stakeholders. Computers & Security, 104015–104015.*
20. *Vasiu, I. and Vasiu, L. (2018). Cybersecurity as an Essential Sustainable Economic Development Factor. European Journal of Sustainable Development, 7(4).*
21. *Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. International Journal of Law, Crime and Justice, 62, 100415.*