Scan to know paper details and
author's profile

Cybersecurity Threats and Their Impact on Financial Inclusion Drivers in Nigeria

Ajibare, Adedayo Oluyemi & Oguntuase, Oluwaseun James

ABSTRACT

This research examined the intricate relationship between cybersecurity threats and financial inclusion in Nigeria, providing novel insights into their dynamic interplay. Considering the staggering growth of cyber frauds targeting financial inclusion drivers in Nigeria, it has become critical to understand the impact of cybersecurity threats on financial inclusion, as inclusive finance is paramount for fostering comprehensive economic development. This study examined the relationship between cybersecurity threats and the demand/supply sides of financial inclusion. The data used were sourced from reputable institutions like the Nigeria Electronic Fraud Forum (NeFF) and the World Bank Development Indicator. The hypotheses of the study were robustly tested using three estimation techniques, which include Ordinary Least Squares (OLS), Two-Stage Least Squares (2SLS), and Generalized Method of Moments (GMM). Key findings challenged conventional wisdom, revealing unexpected relationships between cybersecurity threats and financial inclusion. Contrary to prior assumptions, a positive long-run relationship is revealed between cybersecurity threats and the demand side of financial inclusion. Additionally, the cybersecurity threat has a significant influence on the supply side of financial inclusion. The study thus recommended a revised, robust, and innovative cybersecurity framework for the Nigerian financial sector.

Keywords: cybersecurity threats, demand/supply side of financial inclusion, nigeria, and OLS/2SLS/GMM.

Classification: JEL Code: 21, O16, C36

Language: English

Great Britain
Journals Press

LJP Copyright ID: 146443
Print ISSN: 2633-2299
Online ISSN: 2633-2302

London Journal of Research in Management & Business

Volume 25 | Issue 4 | Compilation 1.0

Cybersecurity Threats and Their Impact on Financial Inclusion Drivers in Nigeria

AJIBARE, Adedayo Oluyemi[α] & OGUNTUASE, Oluwaseun James[σ]

ABSTRACT

This research examined the intricate relationship between cybersecurity threats and financial inclusion in Nigeria, providing novel insights into their dynamic interplay. Considering the staggering growth of cyber frauds targeting financial inclusion drivers in Nigeria, it has become critical to understand the impact of cybersecurity threats on financial inclusion, as inclusive finance is paramount for fostering comprehensive economic development. This study examined the relationship between cybersecurity threats and the demand/supply sides of financial inclusion. The data used were sourced from reputable institutions like the Nigeria Electronic Fraud Forum (NeFF) and the World Bank Development Indicator. The hypotheses of the study were robustly tested using three estimation techniques, which include Ordinary Least Squares (OLS), Two-Stage Least Squares (2SLS), and Generalized Method of Moments (GMM). Key findings challenged conventional wisdom, revealing unexpected relationships between cybersecurity threats and financial inclusion. Contrary to prior assumptions, a positive long-run relationship is revealed between cybersecurity threats and the demand side of financial inclusion. Additionally, the cybersecurity threat has a significant influence on the supply side of financial inclusion. The study thus recommended a revised, robust, and innovative cybersecurity framework for the Nigerian financial sector. It also suggested a review of the theory of production to validly include digital/financial technology as the latest (fifth) factor of production to enable academia, practitioners, and indeed all other stakeholders to understand its features, merits, and demerits, and therefore be able to combat its inherent risks safely.

Keywords: cybersecurity threats, demand/supply side of financial inclusion, nigeria, and OLS/2SLS/GMM

I. INTRODUCTION

The pervasiveness of cybersecurity crime has been well documented in the literature. This crime is seen as a threat, unwaveringly reducing the rate of participation in the digital financial market. In recent years, the financial service sector has undergone significant changes due to the widespread integration of digital technologies. This has created fresh opportunities for global financial access and participation. Innovations like online payment systems and mobile banking apps have enabled millions, particularly those in remote or underserved areas, to access basic financial services. However, alongside these developments comes an escalating risk of cybersecurity breaches and digital scams, posing significant challenges to achieving widespread financial inclusion.

According to Cook (2023), if cybercrime were a country, it would have been the third largest economy in the world behind the US and China, with a currently staggering value of $8 trillion, which is expected to climb to $10.5 trillion by 2025. This is an indication that cyber-fraudsters are winning the war despite the array of risk management measures being periodically deployed by experts and professional bodies. If this trend continues without the right orientation and actions, over one-tenth of the global GDP, which is currently estimated at $99trillion (Rao, 2023) may soon be under the control of criminals and fraudsters; and if technologically advanced economies suffer cyberfraud in large magnitude, then critical attention must be paid to the developing economies to avoid a skewed tech progress or overdependence in the nearest future.

As the rate of cybercrime increases, the unbanked may assume that the risk involved in using electronic financial services and products is higher than the benefits and may deliberately choose to be excluded. Africa has had one of the fastest growth rates in cybercrime activities among emerging nations; in fact, the World Economic Forum has identified cybercrime as one of Africa's top challenges for 2019. An estimated value of $650 million and $210 million in losses came from Nigeria and Kenya, respectively, and $3.5 billion in losses were incurred throughout Africa in 2019 (World Bank, 2020).

Unequivocally, the issue of cybersecurity threats and financial inclusion calls for an urgent examination. This is why Ozili (2018) and, more recently, Sambuli and Grossman (2022) examined this relationship and explained that the lack of consumer trust in digital finance services leads to the readoption of informal mechanisms. A similar study was also conducted by David, Nicholas, and Emma (2021); they revealed that to reduce cyberattacks and their effects, firms are required to build in-house cybersecurity (human) measures and give proper training to their employees instead of using only basic software protection and strong passwords. They, however, did not consider the impact of cybercrime on the firms' customers; rather, they focused on the protection of the firms. Gustavo (2023) also stated that the adoption of Digital Financial Services (DFS), which are made possible by digital technologies, is a crucial factor in financial inclusion and has been significantly hampered by security and privacy concerns.

Fadairo-Cokers and Ibrahim (2021) reported that cybercrime and the usage of some financial institutions' services and products are negatively related. Similarly, Durai and Stella (2019) explained that security has a negative influence on digital financial inclusion, meaning the measured variables are inversely related. There are a series of studies relating to cybercrime with some other variables. For instance, Aribake (2015) analyzed the impact of Information and Communication Technology (ICT) tools for fighting cybercrime on online banking activities in Nigeria, and the findings revealed that cybercrime and ICT tools are inversely related since the improvement in ICT can be used to forestall internet crime. Attamah (2019) also examined the effect of cybercrime on the online banking system, and he discovered that there is widespread cybercrime in Nigeria, and this has an inverse impact on online banking activities.

So far, however, there is no concrete study that relates cybersecurity threats to financial inclusion, simultaneously emphasizing the safety of both the users (clients) and the suppliers (financial institutions). Another uniqueness of this study is to examine the role of cybersecurity threats on financial inclusion to establish findings on the long and short-run relationships between the variables, using a more robust technique such as a dynamic multivariate framework with the capability to explain temporal breaks or shocks. Also, this study is rooted in the Theory of Technology-Enabled Crime and one of the Theories of Financial Inclusion, known as the Technology Acceptance Model (TAM). In light of this, the study has thus significantly extended the existing literature. This study will consider how cybersecurity threats influence financial inclusion in the context of Nigeria. Unlike the study of Aribake (2015) which analyzed the impact of ICT tools for fighting cybercrime on online banking in Nigeria.

II. LITERATURE REVIEW

The impact of cybercrimes on online banking transactions and Automated Teller Machine (ATM) usage among bank customers in the Federal Capital Territory (FCT) has been documented by Fadairo-Cokers and Ibrahim (2021). The authors used primary data that was collected from nine (9) different banks in the Federal Capital Territory (FCT) region of the country and descriptive statistics for analyzing their hypotheses. The study highlights a notable prevalence of banking cybercrime activities in the FCT. While the online protocols implemented by banks to counteract such activities are deemed adequate, the effectiveness of efforts by related agencies in combating banking cybercrimes in the FCT falls short of expectations. Poor financial literacy and limited knowledge of internet operations are identified as major contributors to banking cybercrimes in the FCT. Despite this, the study acknowledges that awareness initiatives on banking cybercrimes by related agencies are adequate (Fadairo Cokers and Ibrahim 2021). Considering these findings, they recommended intensified awareness campaigns by related agencies to mitigate the occurrence of online banking and ATM cybercrimes in the FCT. Furthermore, it suggests that various banks reassess their online protocols aimed at curbing banking cybercrime activities in the Federal Capital Territory to minimize instances of such crimes.

Before the work of Fadairo-Cokers and Ibrahim (2021), Durai and Stella (2019) analysed how digital finance impacts financial inclusion. The authors underscored that the proliferation of digital technologies has facilitated an expanded array of financial services, encompassing online banking, mobile banking, and various e-payment methods such as e-wallets, mobile wallets, and credit and debit cards. These technological advancements offer numerous advantages to consumers, including enhanced convenience and streamlined financial transactions. However, the looming threat of cyberattacks presents a critical concern, particularly in tandem with the ongoing evolution of the economy towards cashless transactions. Despite the growing acceptance of cashless payment methods, there persists a range of apprehensions, including concerns regarding security vulnerabilities, inadequate network coverage, merchant reluctance, elevated transactional costs, and limited user proficiency with technology (Durai and Stella 2019). These factors collectively impede the widespread adoption of the new payment ecosystem. The result of the One-way ANOVA shows that digital finance has a significant and positive influence on inclusive finance, however, digital finance has several negative influences on matters bordering on security, affordability, and adaptability, which collectively impair the safety, acceptance, and growth of financial inclusion (Durai and Stella 2019).

Iwedi, Owakah, and Wofuru-Nyenke (2023) investigated the impact of financial technology on financial inclusion within Nigeria. Utilizing quarterly secondary data sourced from the Central Bank of Nigeria (CBN) Statistical Bulletin (2021) spanning from 2009 to 2019, the study assessed various indicators of financial technology, including point of sale, automated teller machine (ATM), web banking technology, and mobile banking technology. Financial inclusion in Nigeria was assessed using the deposit ratio as a proxy. Employing the vector autoregression (VAR) estimation technique, the study analyzed the time series data. The findings indicate that web banking technology exhibits a positive and statistically significant effect on financial inclusion in Nigeria. However, point of sale, automated teller machines, and mobile banking technology demonstrate positive effects on financial inclusion, albeit not statistically significant. In the same vein, Attamah (2019) examines the effect of cybercrime on the online banking system in Nigeria. The author discovered that there is widespread cybercrime in Nigeria, and this negatively impacts online banking activities.

Several empirical studies (Bouveret, 2018; Faccia and Petratos, 2021; Johri and Kumar, 2023; Ohiani, 2020; and Onunka et al., 2023) have shed light on the devastating repercussions of cybercrime on banking institutions, prompting increased efforts to implement cybersecurity measures aimed at mitigating its impact and fortifying existing defenses. Banks have emerged as direct targets of cybercrime, particularly evident in India, where numerous financial institutions have succumbed to large-scale malware attacks (Acharya and Joshi 2020). These attacks not only result in the compromise of valuable and sensitive data but also inflict substantial financial losses on the affected banks. Acharya and Joshi (2020) studied how cyberattacks affect banking institutions in India. This study aims to delineate the business domains most vulnerable to cyberattacks and to devise tailored strategies for the enhancement and refinement of cybersecurity protocols. The study used secondary data that were sourced from various online platforms, which include government websites, scholarly articles, and research papers. The secondary data analysis was supported using a case study relating to notable cyber threats and criminal incidents, resulting in significant financial consequences in the past.

The study underscores the exponential proliferation of cybercrime and its profound ramifications as a formidable menace to the integrity of banking and financial institutions. It advocates for a comprehensive approach to combating cyber insecurities, asserting that Indian banks must not only confront external threats but also address internal attitudinal barriers and cultivate a mindset conducive to proactive engagement with cyber threats and criminals. Furthermore, the authors advocate for the abandonment of traditional methodologies in favour of adopting cutting-edge technologies and agile, proactive approaches to cybersecurity. They emphasized the imperative of continually assessing the cybersecurity landscape and anticipating emerging threats to effectively safeguard against cyber vulnerabilities.

The inability to curb the increasing cybercrime will result in a decrease in the use of financial products and services. The rising prominence of risk control issues, including data security, privacy protection, and information disclosure, presents a significant challenge to the global expansion of digitally inclusive finance. While developing digitally inclusive banking services, numerous commercial banks and financial service providers have introduced new systems, established online platforms, and engaged in partnerships with numerous third-party entities simultaneously. Any disruptions in the transaction process can severely impact the operations of these businesses or platforms. Such disruptions not only tarnish the reputation of banks and financial service providers but also raise concerns about the potential unauthorized access to and disclosure of user data by third-party entities (Zuo, 2020).

Nevertheless, some studies are focused on how the digitalization of banking services influences the economy. The study on the intricacy of the Fintech era's digital service transformation was carried out by Truong (2022). The study's findings unmistakably supported FinTech's rapidly expanding responsibilities in contemporary economics and offered benchmarks for digitizing the current corporate culture. Wonglimpiyarat and Khaemasunun (2017) analyzed FinTech and its dynamic shifts within the banking sector. The findings' analyses demonstrate the systemic traits of FinTech-based innovations in the banking sector, both globally and in the context of Thailand. Similarly, Iwedi, Kocha, and Wike (2022) studied how the Nigerian economy was affected by the digitalization of financial services. This study made use of 12-year aggregate yearly digital banking service data from the Central Bank of Nigeria (CBN) Statistical Bulletin. The significance of the link between Nigeria's economic performance and digital banking service channels was ascertained through the application of Ordinary Least Squares (OLS). The outcome demonstrates that there is a high correlation between Nigeria's economic growth and both WEB Pay and Mobile Pay. They also found that Nigeria's economic growth is positively and significantly correlated with the digitalization of banking service channels.

From the various scanned literature, there appears to be little empirical research that directly relates cybersecurity threats to either the demand (users') side or supply (financial institutions') side of financial inclusion. One of these studies was conducted by Khan, Mubarik, and Naghavi (2021), who examined how cybersecurity helps limit the negative effects of cybercrimes on financial inclusion. They used a closed-ended questionnaire to gather data from Pakistan's banking industry, and they analyzed the collected data using partial least squares structural equation modeling. They provided evidence that robust cybersecurity lessens the effects of online risks on financial inclusion.

Adeyemi and Festus (2022) evaluated how technology adoption influences financial inclusion in Nigeria and China. The authors used internet usage, Automated Teller Machines, and mobile cellular subscriptions to proxy the adoption of technology, and financial inclusion was proxied by the number of depositors with commercial banks per 1,000 adult population. They adopted the Pooled OLS and Generalized Least Squares estimators. Their study revealed that all the independent variables (internet usage, Automated Teller Machines, and mobile cellular subscriptions) have an insignificant but positive influence on financial inclusion in the two countries (China and Nigeria).

III. METHODS

3.1 Data Collection

The design/plan of this study is in different stages, starting from the secondary data collection, intuitive specification of underlying relationships, hypothesis testing/verification, methods of estimation, and robustness checks. Financial inclusion is classified into two, namely the demand side and the supply side. Specifically, the demand (clients) side's proxy is the deposit rate to the cost of intermediation ratio, which is considered because customers' main obligation to the banks is deposit, and can therefore be used as a measurement of financial inclusion. The supply (banks) side is represented by ATM per 100,000 and bank branches per 100,000 persons; these are considered because they constitute how banks financially include customers.

In the notion of Nwobia, Adigwe, Ezu, and Okoye (2020), cybersecurity threats emanate from the amount of losses associated with the use of financial technology such as ATM, POS, e banking, etc. Therefore, this study proxies cybersecurity threats by the amount of losses resulting from ATM and POS. The raw data on these variables were collected from the Nigeria Electronic Fraud Forum (NeFF), and the World Bank Development Indicator through https://databank.worldbank.org/, over a sample period from 2013 to 2023 on an annual scale. The choice of this period is influenced by the scarcity of data. However, the data are decomposed into monthly figures to increase the quality of the regression outputs.

3.2 Estimation Techniques

A linear dynamic multivariate time-series relationship is introduced to show a causal influence from cybersecurity threats to inclusive finance. This provides an avenue to test the hypotheses that cybersecurity threats negatively impact the supply side and demand side of financial inclusion.

Additionally, a unit root test is conducted to establish the order of integration and purported co-integration to confirm whether a long relationship exists between financial inclusion and cybersecurity threats. Again, the estimation of the long-run and short-run dynamic relationships between the variables of interest using the OLS method is conducted. Robustness checks are conducted by further using the 2SLS and GMM methods to facilitate results comparability and subsequently establish their integrity.

Finally, to account for confounding effects or Simpson's paradox, the study controls for secure internet servers and individuals using the internet. Controlling for these two variables can enhance the quality of regression outputs.

3.3 Model Specification

Thus, econometrically and in the spirit of Nwobia, Adigwe, Ezu, and Okoye (2020), the underlying methodological relationship is defined in two blocks.

Block One- This refers to the supply side of financial inclusion. It comprises ATM per 100,000 persons and bank branches per 100,000 persons. Thus:

$$atmp_t = \alpha_0 + \alpha_1 lossatm_t + \alpha_2 losspos_t + \alpha_3 sis_t + \alpha_4 iui_t + u_t; \quad 3.1$$

$$bbp_t = \phi_0 + \phi_1 lossatm_t + \phi_2 losspos_t + \phi_3 sis_t + \phi_4 iui_t + w_t; \quad 3.2$$

Block Two- This concerns the demand side of financial inclusion. It is restricted to only one variable deposit rate to the cost of intermediation ratio. Thus:

$$dcir_t = \theta_0 + \theta_1 lossatm_t + \theta_2 losspos_t + \theta_3 sis_t + \theta_4 iui_t + v_t; \qquad 3.3$$

Where: $atmp_t$ ATM per Persons 100000 bbp_t -bank branch per 100,000 persons, $dcir_t$ *-ratio of* deposit rate to cost of intermediation, $lossatm_t$ -loss associated with ATMs as a source of threat to customers, $losspos_t$ loss associated with POS as a source of threat to customers, sis_t -secur internet server and $iuis_t$ -individual using the internet.

In general form, the model can be restated using the VAR specification of lag 1:

$$y_t = \lambda + \rho y_{t-1} + \varepsilon_t; \varepsilon_t \square IID(0, \delta_\varepsilon^2) \qquad 3.4$$

Where: y_t is the vector of all the variables of interest in each equation specified above, ε_t is t the contemporary disturbances that is normally distributed with zero mean and constant variance.

Scaling equation 3.4 gives rise to VECM, as shown below.

$$\Delta y_t = \eta + \psi \Delta y_{t-1} + \varphi y_{t-1} + \mu_t; \qquad 3.5$$

Where: The vector Ψ are the coefficients of the short-run dynamics and the vector ϕ are the long-run elaasticity coefficients.

The study proposes to estimate the weights or coefficients of equation 3.5 using the OLS, 2SLS, and GMM estimation procedures.

IV. RESULTS

The variables employed for this study are described using descriptive statistics. These variables are ATM per 100,000 persons (ATM), bank branch per 100,000 persons (BBP), ratio of deposit rate to cost of intermediation (DCIR), loss associated with ATM as a source of threat to customers (LOSSATM), loss associated to POS as a source of threat to customers (LOSSPOS), secure internet server (SIS), and individual using the internet (% of population) (IUI). Table 1 reports the outputs of the results obtained.

Table 1: Descriptive Statistics

Variable	Mean	Std. Dev.	Skewness	Kurtosis
ATM	16.30480	0.678575	-2.395444	9.871839
BBP	4.727456	0.453806	1.320423	3.511589
DCIR	1.000244	0.264830	-0.273598	1.845968
LOSSATM	4.31E+08	1.11E+08	-1.832106	5.332971
LOSSPOS	2.19E+08	92580777	-0.450461	1.998983
SIS	16717.33	12303.95	0.334944	2.346912
IUI	38.39442	12.44011	-0.126493	1.475448

Source: E-View 12 Output

In the table above, the descriptive statistics of the variables used in this study are explained. The average value, standard deviation, skewness value, and kurtosis value are presented.

Table 2: Normality Test Result

Variable	Jarque Bera	Lilliefors (D)	Cramer-von Mises (W2)	Watson (U2)	Anderson Darling (A2)
ATM	35.80(0.00)	0.31(0.00)	1.77(0.00)	1.56(0.00)	9.82(0.00)
BBP	36.48(0.00)	0.18(0.00)	1.60(0.00)	1.37(0.00)	9.26(0.00)
DCIR	8.22(0.02)	0.12(0.00)	0.29(0.00)	0.28(0.00)	2.09(0.00)
LOSSATM	95.13(0.00)	0.33(0.00)	3.68(0.00)	3.36(0.00)	18.67(0.00)
LOSSPOS	9.14(0.01)	0.20(0.00)	0.89(0.00)	0.85(0.00)	4.67(0.00)
SIS	4.41(0.11)	0.12(0.00)	0.47(0.00)	0.46(0.00)	3.31(0.00)
IUI	12.04(0.002)	0.15(0.00)	0.66(0.00)	0.65(0.00)	4.43(0.00

Source: E-View 12 Output.

Table 2 shows the normality results of all the variables using the Jarque-Bera, Lilliefors, Cramer- Mises (W2), von, Watson (U2), and Anderson Darling (A2). The tests were conducted under the null hypothesis that the series follows a normal distribution. From these results, only the secure internet server (sis) series is normally distributed when considering the output of the Jarque-Bera statistics. All the other variables series do not follow a normal distribution. Nevertheless, according to the Central Limit Theorem (CLT), rejection of normality does not matter in this study since the sample size is asymptotically large.

4.2 Unit Root Test

The test for unit root is conducted using the Augmented Dickey-Fuller (ADF), Philip-Peron (PP), and Kwiatkowski-Phillips-Schmidt-Shin test statistic (KPSS) method on the variables of interest. The summary of the results is presented in Table 3 below:

Table 3: Unit Root Test Result

Variable	ADF	PP	KPSS
ATM	2.99(1.94)	2.99(1.94)	0.14(0.15)
BBP	2.05(1.94)	2.12(1.94)	0.09(0.15)
DCIR	2.44(1.94)	2.56(1.94)	0.13(0.46)
LOSSATM	2.83(1.94)	2.83(1.94)	0.37(0.46)
LOSSPOS	3.14(1.94)	3.24(1.94)	0.24(0.46)
SIS	2.16(1.94)	2.16(1.94)	0.16(0.46)
IUI	1.05(1.94)	1.05(1.94)	0.30(0.46)

Source: E-View 12 Output.

Note: The critical values are enclosed in parentheses to indicate their significance levels.

The stationarity test results for all the variables of the study are presented in Table 3 above. The Augmented Dickey-Fuller (ADF) test, Phillips-Perron (PP) test, and Kwiatkowski Phillips-Schmidt-Shin (KPSS) tests were employed to assess stationarity. The test statistics are provided together with their respective critical values in parentheses. The values of the ADF statistics and PP statistics for all the variables are greater than their critical statistics at a 5% alpha value. Thus, the null hypothesis is rejected, meaning the series are all stationary. This is supported by the result of the KPSS. Therefore, there is a strong indication that all the variables of interest in this study are I(1) variables. In this regard, we proceed to conduct a multivariate co-integration test by Johansen.

4.3 Co-integration Test

The three models of this study are tested thus; 1, whether there is a long-run relationship between the number of ATM per 100,000 persons and cyber security threat (loss associated to ATM as a source of threat to customers, and loss associated with POS as a source of threat to customers). 2, whether there is a long-run relationship between bank branches per 100,000 persons and cyber security threat (loss associated with ATM as a source of threat to customers, and loss associated with POS as a source of threat to customers). 3, if there is a long-run relationship between the ratio of deposit rate to cost of intermediation and cybersecurity threats (loss associated with ATM as a source of threat to customers, and loss associated with POS as a source of threat to customers). The following are the test results, which are based on trace statistics and maximum Eigen statistics.

Table 4: Test Results of no Cointegrating Relationship between the number of ATMs per 100,000 people and cyber security threat

Hypothesized no CE's	Eigenvalue	Trace-Stat	5% Critical	Max-Eigen	5% Critical
		Stat	Value	Stat	Value
None *	0.147106	42.08415	35.19275	18.77612	22.29962
At most 1 *	0.113991	23.30803	20.26184	14.28133	15.8921
At most 2	0.073645	9.026701	9.164546	9.026701	9.164546

Source: E-View 12 Output. Note: To each statistic, there is a correspondent critical value at 5%, and start rejecting until you do not reject. Also, the Trace test indicates 1 cointegrating eqn(s) at the 0.05 level and the Max eigenvalue test indicates no cointegrating eqn(s) at the 0.05 level.

In Table 4 above, the variables tested for their cointegrating relationship are the supply side of financial inclusion (the number of ATMs per 100,000 persons) and cybersecurity threat (loss associated with ATM as a source of threat to customers, and loss associated with POS as a source of threat to customers). As reported above, the Eigenvalue is respectively less than one, meaning that the system containing these three variables is stable. The eigenvalues indicate system stability, this supports a cointegrating relationship. Further tests by trace statistic also confirm that the null hypothesis of no cointegration is rejected at a 5% level of significance because the trace statistic is larger than the corresponding 5% critical value. There is also evidence of one cointegrating equation and one cointegrating rank. This means that cybersecurity threat maintains a long-run relationship with the supply side of financial inclusion.

Table 5: Test Results of No Cointegrating Relationship between the Bank Branches per 100,000 Persons and Cyber Security Threat

Hypothesized no CE's	Eigenvalue	Trace-Stat	5% Critical	Max-Eigen	5% Critical
		Stat	Value	Stat	Value
None *	0.133886	29.31556	24.27596	16.96119	17.7973
At most 1 *	0.099318	12.35437	12.3209	12.34313	11.2248
At most 2	9.53E-05	0.011244	4.129906	0.011244	4.129906

Source: E-View 12 Output. Note: To each statistic, there is a correspondent critical value at 5%, and start rejecting until you do not reject. Also, the Trace test indicates 1 cointegrating eqn(s) at the 0.05 level and the Max eigenvalue test indicates no cointegrating eqn(s) at the 0.05 level.

Table 5 shows that the trace statistic under the assumption of at most 1 cointegrating equation is approximately 12.35 and the associated critical value of 12.32. This implies that the null hypothesis of no cointegration is rejected. However, under the Maximum Eigen statistics, we do not reject the null hypothesis of no cointegration, thus, we go with the result of the trace statistics. There is therefore a long-run relationship between the supply side of financial inclusion (bank branches per 100,000 persons) and cybersecurity threats (loss associated to ATM as a source of threat to customers, and loss associated with POS as a source of threat to customers).

Table 6: Test Results of no Cointegrating Relationship between the Ratio of Deposit Rate to Cost of Intermediation and Cyber Security Threat

Hypothesized no CE's	Eigenvalue	Trace-Stat	5% Critical	Max-Eigen	5% Critical
		Stat	Value	Stat	Value
None *	0.271784	56.18261	35.01090	35.20456	24.25202
At most 1 *	0.172132	20.97806	18.39771	20.96806	17.14769
At most 2	9.01E-05	0.009997	3.841465	0.009997	3.841465

Source: E-View 12 Output. Note: To each statistic, there is a correspondent critical value at 5%, and start rejecting until you do not reject. Also, the Trace test indicates 1 cointegrating eqn(s) at the 0.05 level and the Max eigenvalue test indicates 1 cointegrating eqn(s) at the 0.05 level.

The variables of cybersecurity threat and the demand side of financial inclusion, cointegrating relationship loss associated to ATM as a source of threat to customers, and loss associated to POS as a source of threat to customers, and ratio of deposit rate to cost of intermediation. As seen above the Eigenvalue is respectively less than one, this implies that the system containing these three variables is stable. Additionally, the test of no cointegration is rejected because the trace statistic (56.18) is larger than the 5% critical value (35.01). At the same time, the maximum Eigen statistic (35.21) is larger than the 5% critical value (24.25). However, we cannot reject the hypothesis that there is only one cointegrating vector because the trace statistic and the maximum Eigen statistic are respectively smaller than their associated critical values. This indicates that the null hypothesis of no cointegration is refuted. Based on the result of the trace statistic and the maximum Eigen statistic, we can equally state that for the null hypothesis, there is only one cointegrating vector that cannot be rejected. Therefore, there is a presence of a long-term relationship between the demand side of financial inclusion (ratio of deposit rate to cost of intermediation) and loss associated with ATM as a source of threat to customers, and loss associated with POS as a source of threat to customers proxies for cybersecurity threat.

4.4 Testing the Nature of the Long-Run Relationship

The co-integration test conducted earlier has shown that financial inclusion and cybersecurity threats have a long-term relationship. Therefore, there is a need to investigate the nature of this long-run relationship. When referring to the nature of a relationship, we mean that a rise in any one of the losses associated with ATM or POS causes the supply side/demand side of financial inclusion to change in one or the other direction by a specific percentage. Therefore, three methods were employed in this study, these methods are OLS, 2SLS, and GMM. The essence of employing these three methods is to establish a robustness check or to confirm the certainty of the nature of the long-run relationship. The results are presented in Tables 7, 8, and 9 for the three equations/models.

Table 7: The Nature of the Long Run Relationship between the Number of ATMs per 100,000 Persons and Cyber Security Threat

	OLS		2SLS		GMM	
Variable	Coeff	PV	Coeff	PV	Coeff	PV
LOSSATM	0.110421	0.000	0.110421	0.000	0.110421	0.000
LOSSPOS	0.017795	0.0001	0.017795	0.0001	0.017795	0.0175
IUI	-0.054328	0.000	-0.054328	0.000	-0.054328	0.000
SIS	-0.001252	0.4738	-0.001252	0.4738	-0.001252	0.5817
C	0.203716	0.000	0.203716	0.000	0.203716	0.0085
Adjusted R-squared	0.894331		0.894331		0.894331	

Source: E-View 12 Output. Note: PV is the probability value. Also, because this is a time series analysis, the instruments used for 2SLS and GMM estimator are predetermined variables (lag/previous value of the dependent variable)

Table 7 displays the results of the long-run relationship between the number of ATMs per 100,000 persons and cyber security threats (loss associated with ATM (LOSSATM) and loss associated with POS (LOSSPOS). The coefficient of LOSSATM is approximately 0.11 or 11% with a corresponding probability value of 0%. This implies that there is a positive and significant relationship between these variables, this relationship is significant at a 1% alpha value. This result shows that despite the loss recorded from using ATMs, the number of ATMs per 100,000 persons is still increasing. Banks' customers are still using the ATM (an instrument of financial inclusion). The coefficient of LOSSPOS is also positive, which suggests that this threat factor moves in the same direction as the supply side of financial inclusion (the number of ATMs per 100,000 persons). It is noted that the three estimators yielded the same outcome, thus, the cybersecurity threat has a direct relationship with the supply side of financial inclusion.

Table 8: The Nature of the Long-Run Relationship between the Bank Branches per 100,000 Persons and Cyber Security Threat OLS 2SLS GMM

	OLS		2SLS		GMM	
Variable	Coeff	PV	Coeff	PV	Coeff	PV
LOSSATM	-0.08646	0.000	-0.08646	0.000	0.08646	0.0001
LOSSPOS	0.023349	0.0002	0.023349	0.0002	0.023349	0.0795
IUI	-0.078466	0.000	-0.078466	0.000	-0.078466	0.0002
SIS	-0.029107	0.000	-0.029107	0.000	-0.029107	0.000
C	1.460583	0.000	1.460583	0.000	1.460583	0.000
Adjusted R-squared	0.951233		0.951233		0.951233	

Source: E-View 12 Output. Note: In the study, the results yielded by the OLS were confirmed using the 2SLS and the GMM. The reason for this confirmation is to see if the parameter for these methods changes or remains the same. Since the parameter remained the same, there is strong evidence that the relationship exists. If the parameter had changed, the inconsistency would have been reported.

One output of the test on the nature of the long-run relationship between the supply side of financial inclusion (bank branches per 100,000 persons) and cyber security threats is reported in the above table. The results of the three estimators reveal that LOSSATM has a negative and significant influence on bank branches per 100,000 persons, this implies that loss associated with the use of ATM moves in the opposite direction with bank branches per 100,000 persons; meaning a 1% decrease in ATM losses will lead to about 0.1 or 10% increase in bank branches per 100,000 persons. The three-estimation techniques produced the same output, for variable LOSSPOS has a positive coefficient of approximately 0.02 or 2% and this shows that this variable has a weak but positive impact on the supply side of financial inclusion. As the loss from POS increases, bank branches per 100,000 persons also increase in the long run. The results from OLS and 2SLS methods show that LOSSPOS has a significant influence on bank branches per 100,000 persons at a 1% alpha value while the GMM method shows that these variables are significantly related at a 10% alpha value.

Therefore, these results reveal that as the threat of using POS increases, people prefer to use the bank, so branches' transactions increase. Furthermore, as loss in ATM usage increases, banks' customers withdraw from the bank which in the long run will lead to a decrease in the number of bank branches.

Table 9: The Nature of the Long Run Relationship between the Ratio of Deposit Rate to Cost of Intermediation and Cyber Security Threat

	OLS		2SLS		GMM	
Variable	Coeff	PV	Coeff	PV	Coeff	PV
LOSSATM	0.064104	0.5719	0.064104	0.5719	0.064104	0.6251
LOSSPOS	0.097933	0.1471	0.097933	0.1471	0.097933	0.2971
IUI	-0.928349	0.000	-0.928349	0.000	-0.928349	0.0003
SIS	0.079538	0.0039	0.079538	0.0039	0.079538	0.0661

C	-0.245075	0.7191	-0.245075	0.7191	-0.245075	0.6843
Adjusted R-squared	0.420563		0.420563		0.420563	

Source: E-View 12 Output

The coefficients for loss associated to ATM as a source of threat to customers (LOSSATM), and loss associated to POS as a source of threat to customers (LOSSPOS) are approximately 0.06, and 0.10 respectively. ATM and POS losses are positively impacting the ratio of deposit rate to cost of intermediation, this is contrary to a-priori expectation, nevertheless, this positive impact is very weak and insignificant in the long run.

4.5 Testing the Short-Run Dynamic Relationship between the supply and demand sides of Financial Inclusion and Cybersecurity threat

Examining the short-run dynamic influence from loss associated with ATM as a source of threat to customers (LOSSATM), and loss associated with POS as a source of threat to customers (LOSSPOS) to supply and demand sides of financial inclusion is another crucial aspect of this study. The findings summary is reported in Tables 10, 11, and 12 respectively.

Table 10: Short Run Dynamic on the Relationship between the Number of ATMs per 100,000 Persons and Cyber Security Threat

	OLS		2SLS		GMM	
Variable	Coeff	PV	Coeff	PV	Coeff	PV
DATM(-1)	0.73542	0.000	0.73542	0.000	0.73542	0.000
DLOSSATM	0.255674	0.000	0.255674	0.000	0.255674	0.0001
DLOSSATM(-1)	-0.200008	0.000	-0.200008	0.000	-0.200008	0.0006
DLOSSPOS	0.007944	0.000	0.007944	0.000	0.007944	0.0469
DLOSSPOS(-1)	0.00011	0.9233	0.00011	0.9233	0.00011	0.9674
DIUI	-0.042583	0.0129	-0.042583	0.0129	-0.042583	0.012
DSIS	-0.002022	0.0242	-0.002022	0.0242	-0.002022	0.067
C	0.000101	0.5651	0.000101	0.5651	0.000101	0.4607
Adjusted R-squared	0.955815		0.955815		0.955815	

Source: E-View 12 Output

The changes in the number of ATMs per 100,000 persons (DATM(-1)), DLOSSATM, DLOSSATM (-1), DLOSSPOS, DLOSSPOS(-1) are approximately 0.74, 0.26, -0.20, 0.01, and 0.00011 respectively. This means that ATM at lag one has a positive short-run effect on the current ATM. Similarly, loss associated with POS as a source of threat to customers (LOSSPOS) at lag one, current LOSSPOS, and current LOSSPOS have a positive short-run effect. That is, there is a dynamic short-run positive influence from LOSSPOS at lag one, current LOSSPOS, and current LOSSATM to the supply side of financial inclusion. Nevertheless, LOSSATM at lag one has a negative coefficient. This indicates that there is a short-run dynamic from previous LOSSATM to the supply side of financial inclusion. Furthermore, only the short-run dynamic effect from LOSSPOS at lag one to the supply side of financial inclusion is not significant across the three techniques.

Table 11: Short Run Dynamic on the Relationship between Bank Branches per 100,000 Persons and Cyber Security Threat

	OLS		2SLS		GMM	
Variable	Coeff	PV	Coeff	PV	Coeff	PV
DBBP(-1)	0.898039	0.000	0.898039	0.000	0.898039	0.000
DLOSSATM	0.040837	0.4213	0.040837	0.4213	0.040837	0.5254
DLOSSATM(-1)	-0.043026	0.3275	-0.043026	0.3275	-0.043026	0.4481
DLOSSPOS	0.002706	0.3988	0.002706	0.3988	0.002706	0.3888
DLOSSPOS(-1)	0.000663	0.7428	0.000663	0.7428	0.000663	0.7689
DIUI	-0.051404	0.1173	-0.051404	0.1173	-0.051404	0.2928
DSIS	0.001405	0.4112	0.001405	0.4112	0.001405	0.4586
C	0.000201	0.5381	0.000201	0.5381	0.000201	0.4889
Adjusted R-squared	0.836663		0.836663		0.836663	

Source: E-View 12 Output

As shown in the table above, the value of bank branches per 100,000 persons (DBBP (-1)), loss associated to ATM as a source of threat to customers, (DLOSSATM), loss associated with ATM as a source of threat to customers (DLOSSATM(-1)) at lag one, loss associated to POS as a source of threat to customers (DLOSSPOS), and loss associated to POS as a source of threat to customers at lag one (DLOSSPOS(-1)) are approximately 0.90, 0.04, -0.04, 0.003 and 0.001 respectively. All these variables except LOSSATM at lag one have a positive short-run effect on bank branches per 100,000 persons (supply side of financial inclusion). Thus, in the short run, these variables play a positive role on the supply side of inclusive finance.

Table 12: Short Run Dynamic on the Relationship between Ratio of Deposit Rate to Cost of Intermediation and Cyber Security Threat

	OLS		2SLS		GMM	
Variable	Coeff	PV	Coeff	PV	Coeff	PV
DDCIR(-1)	0.847403	0.000	0.847403	0.000	0.847403	0.000
DLOSSATM	0.066841	0.8679	0.066841	0.8679	0.066841	0.9313
DLOSSATM(-1)	-0.016604	0.9622	-0.016604	0.9622	-0.016604	0.9806
DLOSSPOS	-0.053316	0.037	-0.053316	0.037	-0.053316	0.0646
DLOSSPOS(-1)	0.019199	0.2366	0.019199	0.2366	0.019199	0.2223
DIUI	-0.471442	0.073	-0.471442	0.073	-0.471442	0.1492
DSIS	0.013654	0.2893	0.013654	0.2893	0.013654	0.5044
C	0.002498	0.3424	0.002498	0.3424	0.002498	0.4454
Adjusted R-squared	0.783919		0.783919		0.783919	

Source: E-View 12 Output

The changes in cybersecurity threats to the demand side of financial inclusion are observed at lag one only. In the above table, the coefficient of the ratio of deposit rate to cost of intermediation at lag one DDCIR(-1) is approximately 0.85 with a probability value of zero. This implies that within the short-run dynamic, changes in the ratio of deposit rate to cost of intermediation respond positively to the previous ratio of deposit rate to cost of intermediation. Loss associated with ATM as a source of threat to customers (LOSSATM) at lag one and loss associated with POS as a source of threat to customers (LOSSPOS) have negative coefficients, while the coefficients of loss associated with POS as a source of threat to customers (LOSSPOS) at lag one and loss associated to ATM as a source of threat to customers (LOSSATM) are positive, indicating a system that is not stable. In the same view, LOSSPOS at lag one and LOSSATM have a positive short-run effect on the demand side of financial inclusion. However, LOSSATM at lag one and LOSSPOS have negative short-run influence on the demand side of financial inclusion. The value of the Adjusted R-square is approximately 0.78. This suggests that the regressors have a joint effect of about 78% on the regressands.

V. CONCLUSION

There exists a long-run relationship between cybersecurity threats and both the supply and demand sides of financial inclusion. The research sheds light on the nuanced dynamics between cybersecurity threats and financial inclusion, revealing both expected and unexpected relationships. Contrary to prior assumptions, for example, the studies of Demirgüç-Kunt et al., 2018, Bouveret, 2018; Faccia and Petratos, 2021; Johri and Kumar, 2023; Ohiani, 2020 and Onunka, et al. 2023) claimed that cybercrime has a negative impact on users of financial products. Also, the study of Malladi et al., (2021) showed that inclusive finance can be hindered because of unguarded digital platforms. This study however finds a positive long-run relationship between cybersecurity threats and the demand side of financial inclusion, challenging conventional wisdom that human beings naturally tend to avoid whatever exposes them to financial or economic losses, thus prompting a re-evaluation of existing frameworks. This unexpected finding underscores the complexity of the relationship between cybersecurity and financial inclusion, highlighting the need for a more nuanced understanding of the underlying mechanisms at play.

The nature of the long-run relationship between cybersecurity threats and the supply side of financial inclusion is significant, this practically implies that the more the banks roll out financial inclusion tools, the higher the spate of fraud. This indicates that financial institutions need to allocate resources to enhance cybersecurity infrastructure**.** Moreover, the importance of considering cybersecurity threats in the context of financial inclusion, particularly in emerging economies like Nigeria is demonstrated in this study. With the rapid digitization of financial services and the increasing prevalence of cyberattacks, understanding the implications of cybersecurity threats on financial inclusion is paramount for ensuring the resilience and stability of the financial system.

Also, the nature of the short-run relationship between cybersecurity threats and both the supply and demand sides of financial inclusion varies, with a positive relationship observed for the supply side and an insignificant relationship for the demand side.

Therefore, based on the reality of modern business processes, especially with digital technology warehousing vast data for the provision of products and services to customers, it is indeed crucial to reassess the continuous relevance of the Theory of production. The traditional goal of the firm is to efficiently combine the factors of production to create products and services that will continually meet the ever-changing needs of customers; a role digital technology has now unconsciously sneaked into. Digital and/or financial technology has obviously dwarfed the essence of land and labour as factors of production, clearly revealing the outdatedness of the Theory of production.

This study recommends a review that will recognize digital technology as the fifth and indeed, a very critical factor of production to identify its characteristics and dynamics, understand its merits and demerits, and ultimately be able to devise measures that will safely alleviate its ravaging intrinsic threats on people’s welfare, financial sector’s survival and economic development generally.

REFERENCES

1. Acharya, S. and Joshi, S. (2020) “Impact of cyber-attacks on banking institutions in India: A study of safety mechanisms and preventive measures”, *Palarch’s Journal of Archaeology of Egypt/Egyptology 17(6)*, pp. 4656-4670, ISSN 1567-214x
2. Adeyemi, W. A. and Festus, O. O. (2022) “The effect of technology adoption on financial inclusion: a cross-country panel analysis between China and Nigeria”, *European Journal of Business and Management Research*, 7(2), 1-11 DOI: http://dx.doi.org/10.24018/ejbmr.2022.7.2.1314
3. Aribake, F O. (2015) “Impact of ICT tools for combating cybercrime in Nigeria online banking: A conceptual review”, *International Journal Trade, Economics and Finance* 6, pp. 272-277.
4. Attamah, N. (2019) “Effect of cybercrime on Nigeria’s online banking system”, *Journal of Applied Sciences* 5(1), pp. 72-79, www.iaajournals.org IAA
5. Bouveret, A. (2018) “Cyber risk for the financial sector: a framework for quantitative assessment”, IMF Working Papers, 18 (143), Pp.1. https://doi.org/10.5089/9781484360750.001
6. Cook, J. (2023) *‘If cybercrime was a country, it would be the world’s third-largest economy after the U.S. and China’ - Business Leader News, Business Leader.* Available at: https://www.businessleader.co.uk/interview-raluca-saceanu-ceo-smarttech247/.
7. David B.-G, Nicholas, L, and Emma, B. (2021) “The dynamics of business, cybersecurity, and cyber-victimization: foregrounding the internal guardian in prevention, victims & offenders”, 16(3), 286-315, DOI: 10.1080/15564886.2020.1814468
8. Davis, F. D. (1989) “Perceived usefulness, perceived ease of use, and user acceptance of information technology”, MIS Quarterly, 13(3), pp. 319-340.
9. Demirgüç-Kunt, A., Klapper, L., Singer, D., Ansar, S., and Hess, J. (2018) “The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution”, The World Bank.
10. Durai, T, and Stella, G. (2019) “Digital finance and its impact on financial inclusion”, *Journal of Emerging Technologies and Innovative Research* (JETIR), 6(1), pp. 122-127.
11. Faccia, A., and Petratos, P. (2021) “Blockchain, Enterprise Resource Planning (ERP) and Accounting Information Systems (AIS): Research on e-Procurement and System Integration”, https://scite.ai/reports/10.3390/app11156792
12. Fadairo-Cokers, O A and Ibrahim, G U. (2021) “Impact of Cybercrime on Selected Deposit Money Banks (DMBs) in the Federal Capital Territory (FCT)”, *International Journal of Advanced Research in Statistics, Management, and Finance.* 8(1), pp. 176-188, 10.48028/iiprds/ijarsmf.v8.i1.12
13. Gustavo M V B A. (2023) “The effect of national cybersecurity commitment on financial inclusion”, MSc Thesis, Georgetown University.
14. International Telecommunication Union (ITU). (2019), Global Cybersecurity Index (GCI) 2018. Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GlobalCybersecurityIndex.aspx
15. Iwedi, M., Kocha, C., and Wike, C. (2022) “Effect of digitalization of banking services on the Nigerian economy”, *Contemporary Journal of Banking and Finance*, 2(1), pp. 1-9.
16. Iwedi M., Owakah N. F., and Wofuru-Nyenke O. K. (2023) “Effect of financial technology on financial inclusion in Nigeria”, *African Journal of Accounting and Financial Research* 3(1), pp.21-36. DOI: 10.52589/AJAFR-A7LQZBE9
17. Johri, A., and Kumar, S. (2023) “Exploring Customer Awareness towards Their Cyber

Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation", https://scite.ai/reports/10.1155/2023/2103442

18. Khan, A., Mubarik, M. S., and Naghavi, N. (2021) "What matters for financial inclusions? Evidence from emerging economy", *International Journal of Finance and Economics*, Pp. 821838 https://doi.or HYPERLINKn"https://doi.org/10.1002/ijfe.2451"g HYPERLINK "https://doi.org/ 10.1002 ijfe.2451"/10.1002/HYPERLINK "https://doi.org/10.1002/ijfe.2451"ij HYPERLINK "https://doi. org/10.1002/ijfe. 2451"fe.2451
19. Malladi, C. M., Soni, R. K., and Srinivasan, S. (2021) "Digital financial inclusion: Next frontiers —Challenges and opportunities". CSI Transactions on ICT, 9(2), pp. 127-134.
20. Nwobia, C.E., Adigwe, P. A., Ezu, G. K. and Okoye, J. N. (2020) "Electronic fraud and performance of deposit money banks in Nigeria: 2008-2018", *International Journal of Business and Management*, 15(6), pp. 126-136, doi:10.5539/ijbm.v15n6p126
21. Ohiani, A.S. (2020) "Technology innovation in the Nigerian banking system: prospects and challenges", *Rajagiri Management Journal*, 15 (1), Pp. 2-15. https://doi.org/10.1108/ramj-05- 2020-0018
22. Onunka, O., Alabi, A. M., Okafor, C. M., Obiki-Osafiele, A. N., Onunka, T. and Daraojimba, C. (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
23. Ozili, P K. (2018) "Impact of digital finance on financial inclusion and stability", *Borsa Istanbul Review*, 18(4), 329–340, https://doi.org/ 10.1016/j.bir.2017.12.003
24. Rao, P. (2023) *Visualizing the $105 Trillion World Economy in One Chart*, *Visual Capitalist*. Available at: https://www.Visualcapitalist.com/visualizing-the-105-trillion-world-economy in-one-chart/.
25. Sambuli, N, and Grossman, T. (2022) "Introducing CyberFI: Perspectives on cybersecurity, capacity development, and financial inclusion in Africa. Carnegie Endowment for International Peace", https://carnegieendowment.org/2022/05/02/introducing-cyberfi-perspectives-on cybersecurity-capacity-development-and-financial-inclusion-in-africa-pub-87001
26. Truong, Q. N. (2022) "Management strategies for digital transformation thrive in constant change", Master of Business Administration Thesis for a Master of Digital Business Management (UAS) - Degree Vaasa 2022.
27. Wonglimpiyarat, J and Khaemasunun, P. (2017) "Strategies of remodelling China towards an innovation-driven economy", *International Journal of Business Innovation and Research*, 12(2), pp. 175-188
28. World Bank Group. (2020) Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution. Retrieved from htt HYPERLINK "https://globalfindex.worldbank.org/"pHYPERLINK https://globalfindex.worldbank.org/"s://HYPERLINK"https://globalfindex.worldbank.org/"gHYPERLINK "https://globalfindex.worldbank.org/"lobalfindex.worldbank.orHYPERLINK "https://globalfindex.worldbank.org/"g HYPERLINK "https://globalfindex.worldbank.org/"/
29. Zuo, W. (2020) "The analysis of digital finance and digital inclusive finance discussion on impact, problems and suggestions", *Advances in Economics, Business and Management Research*, vol. 203, pp. 2151-2154.