

## **CYBERSECURITY IN THE BANKING SECTOR: THE ROLE OF LAW IN ADDRESSING MOBILE BANKING CONCERNS IN NIGERIA.**

Obeta Ruth Oluchi, Atuegwu Wisdom Tochukwu, Ogbonna Angelica Chika, Azubuike Nmesoma Favour and Chukwuha Chinenye Vivian.

### **ABSTRACT**

It is axiomatic that the global banking sector is characterized by the rapid adoption of mobile banking, which has brought about significant benefits in terms of financial inclusion and convenience for bank customers/consumers. However, this technological advancement in banking has also introduced new cybersecurity risks that threaten the stability and integrity of various countries' banking sector. Following this backdrop, this paper examines the role of law in addressing emerging banking concerns with a particular focus on the Nigerian context. The paper begins by providing an overview of the mobile banking landscape in Nigeria, it then analyzes the cybersecurity challenges that have become common, including the prevalence of mobile banking fraud, data breaches, and unauthorized access to customers' accounts. The paper concludes by emphasizing the critical importance of a comprehensive legal framework to address the evolving cybersecurity challenges in the Nigerian banking sector. It also furnishes practical recommendations aimed at enhancing the resilience of the banking system and safeguarding the interests of bank customers and the broader economy.

**KEYWORDS:** Cybersecurity, Mobile Banking, Banking Sector, Challenges and Nigeria.

### **1.0 INTRODUCTION**

Now more than ever, there is an increasing need for banking institutions worldwide to fortify their defenses against an evolving and sophisticated threat landscape to protect the assets of

Bank customers/consumers from fraudsters both within and outside the bank.<sup>1</sup> In Nigeria, for instance, an NDIC publication indicates that about 1,914 bank staff of various banks were involved in bank fraud.<sup>2</sup> A 2023 survey conducted by the Financial Services Information Sharing and Analysis Center (FS-ISAC), shows that 89% of financial institutions are increasing their cybersecurity budgets in 2024. It is easy to claim that despite the availability of numerous

---

<sup>1</sup> Azeez O. Hasan, et Al. "Cybersecurity in Banking: A Global Perspective with a Focus on Nigerian Practices" Retrieved from <[www.fepbl.com/index.php/csitrj](http://www.fepbl.com/index.php/csitrj)> Accessed on 8th June, 2024.

<sup>2</sup> Ibid.

security measures, the need for additional investments is sacrosanct.<sup>3</sup> In this paper, the authors attempt to examine mobile banking opportunities and challenges within Nigeria's banking sector. The argument of the authors is that the law as an indispensable tool for regulating human conduct plays a crucial role in addressing the emerging cybersecurity threats and mobile banking concerns in Nigeria.

## **2.0 CONCEPTUAL FRAMEWORK**

To better understand this paper, let us succinctly analyze its keywords: Cybersecurity and Mobile Banking.

### **2.1 CYBERSECURITY**

Cybersecurity in the banking sector refers to the measures and technologies employed by financial institutions to protect against unauthorized access, cyber threats, and data breaches. The cybersecurity system, guidelines, and techniques are designed to protect against threats, potential harm, computer viruses, malware, hacking, information theft, and unauthorized access to networks, computers, applications, and documentation. The main objective and importance of cybersecurity in banking is to protect the user's assets.<sup>4</sup>

### **2.2 MOBILE BANKING**

Mobile banking falls within the definition of "Electronic banking". "Electronic banking", or "E-banking" includes the provision of retail and small value banking products and services through electronic banking channels as well as large value electronic payments, and other wholesale banking services delivered electronically. In other words, e-banking is the use of electronic delivery channels for banking products and services. It is a subset of e-finance. The most important electronic delivery channels are the Internet, wireless communication networks, automated teller machines (ATMs), telephones and mobile phones. Mobile banking is a form of electronic banking (e-banking) delivered via mobile networks and performed on a mobile phone. It is also referred to as Internet banking.<sup>5</sup> The mobile banking system gained popularity during the peak of COVID-19 when it was impossible to visit public places. Before the introduction of this, SMS banking was prevalent in most countries. Even at present, several

---

<sup>3</sup> Artur Nesternenko, "Cybersecurity in Banking: Main Threats and Challenges in 2024" Retrieved from <<https://dashdevs.com/blog/cybersecurity-in-banking-main-threats-and-challenges-in-2023/>> Accessed on 8th June, 2024

<sup>4</sup> Ibid

<sup>5</sup> Vivienne Lawack-Davids, "The Legal and Regulatory Framework of Mobile Banking and Mobile Payments in South Africa" Retrieved from: *Journal of International Commercial Law and Technology*, Vol 7, Issue 4 (2012) Accessed on 8th June, 2024.

banks offer both SMS and mobile banking to their customers.<sup>6</sup>

### 3.0 EXAMINING THE CONCEPT OF MOBILE/INTERNET BANKING IN NIGERIA AND ITS ASSOCIATED RISKS.

Nigeria has been investing heavily in the development of information technologies. It was estimated in December 2017 that more than 50% of its population now use the internet. This is almost 100 million individuals,<sup>7</sup> making it the 8th largest globally with the highest number of Internet users. Internet banking was first introduced to Nigeria in 2003.<sup>8</sup> The event was marked by the introduction of Guidelines on Electronic Banking in Nigeria (CBN, 2003) by the Central Bank of Nigeria (CBN). A recapitalization of the Nigerian banking industry took place soon afterwards, with only 25 banks out of the previous 89 banks in Nigeria surviving this recapitalization. Those who survived were known to have engaged in the use of internet technologies for the effective and efficient delivery of banking services.<sup>9</sup>

In the last few years, customers' appetite in Nigeria for internet banking has grown rapidly. Internet banking services have also developed rapidly with banks expanding their delivery channels online, providing almost all offline banking services via the Internet.<sup>10</sup> Despite these benefits, however, its adoption remains remarkably low in Nigeria, with just over 40% of customers having used online banking platforms for one or more banking activities.<sup>11</sup> Studies reveal that the main barriers to a greater acceptance of Internet banking in Nigeria, have proved to be the lack of security and trust, limited privacy, and an inadequate telecommunications infrastructure; along with a low literacy level, and an unreliable electricity supply.<sup>12</sup> Yet of all these factors, security emerged as the most significant factor in Auta's (2010) research, which used an exploratory 'principle component factor analysis' to identify the underlying factors determining the success of internet banking in Nigeria. The revolutionary service changes in

---

<sup>6</sup> Supra, note 3.

<sup>7</sup> Internet World Stats, 2018a, b. "[Internet Penetration in Africa](https://www.internetworldstats.com/stats1.html)" – December 31, 2017. Retrieved from <https://www.internetworldstats.com/stats1.html>. Accessed on 12<sup>th</sup> June, 2024.

<sup>8</sup> Oni, A.A., Ayo, C.K., 2010. "[An empirical investigation of the level of users' acceptance of e-banking in Nigeria](#)". Retrieved from: *Journal of Internet Banking and Commerce*. 15, 1-13. Accessed on 12<sup>th</sup> June, 2024.

<sup>9</sup> Akanbi, P.A., Ayodele, T.D., Adedipe, O.A., 2014. "[An Investigation into Some Factors Influencing the Intention to Use Internet Banking among Undergraduates in Nigeria](#)". Retrieved from: *Research Journal of Finance and Accounting*. 5, 1-9. Accessed on 12<sup>th</sup> June, 2024.

<sup>10</sup> Tarhini, A., Mgbemena, C., Trab, M.S.A., Masa'deh, R., 2015. "[User adoption of online banking in Nigeria: A qualitative study](#)". Retrieved from: *The Journal of Internet Banking and Commerce*. 20 (3). Accessed on 12<sup>th</sup> June, 2024.

<sup>11</sup> KPMG, 2017. "[How can Nigerian banks start to improve Internet banking penetration?](https://home.kpmg.com/ng/en/home/insights/2017/11/how-can-nigerian-banks-start-to-improve-internet-banking-penetra.html)" Retrieved from: <https://home.kpmg.com/ng/en/home/insights/2017/11/how-can-nigerian-banks-start-to-improve-internet-banking-penetra.html> Accessed on 12<sup>th</sup> June, 2024.

<sup>12</sup> Agboola, A. A., 2006. "[Electronic Payment Systems and Tele-banking Services in Nigeria](#)". Retrieved from: *Journal of Internet Banking and Commerce*. 11 (3), 1-7. Accessed on 12<sup>th</sup> June, 2024

the Nigerian banking industry have brought about a new wave of security problems.<sup>13</sup> Cybersecurity breaches have become a key phenomenon affecting the Nigerian banking industry (both the banks and their customers).<sup>14</sup>

According to the report in 2013 of the Nigerian Inter-Bank Settlements Systems (NIBSS Plc), Nigerian banks lost 159 billion Nigerian Naira between 2000 and the first quarter of 2013 to cyber security breaches.<sup>15</sup> Moreover, more than half of the loss occurred in 2010 when the internet became a popular banking tool.<sup>16</sup> Nigeria had, more generally, lost around 500 billion Nigerian Naira between 2010 and 2017 on reported and unreported cases of online fraud/cybercrime across major sectors of the economy, which included both the banking and telecommunications sectors.<sup>17</sup> Besides financial loss, the reputational loss brought about by security breaches, while not quantifiable, maybe even harder for banks to recover. The biggest cost of a data breach is indeed reputation in terms of the erosion of brand value.<sup>18</sup> The reputational loss of a bank may reverberate through the whole banking system by increasing the reputational risk of other banks.<sup>19</sup>

### 3.1 ANALYSING THE RISKS AND CHALLENGES

The most prominent types of cyber security threats and challenges in the global banking sector include; Phishing, cyber terrorism, malware attacks, Bank Verification Number (BVN) scams, fraud identity theft, password sniffing, and theft of bank cards.<sup>20</sup>

To start with, Nigerian banks grapple with sophisticated phishing attacks that attempt to trick individuals into revealing sensitive information. Social engineering tactics prey on human vulnerabilities, making awareness crucial. The surge in mobile banking introduces new risks, with threats such as mobile malware and SIM swapping attacks targeting users' devices and

---

<sup>13</sup> Ehimen, O.R., Bola, A., 2010. “Cybercrime in Nigeria”. Retrieved from: *Business Intelligence Journal*. 3 (1), 93-98. Accessed on 12<sup>th</sup> June, 2024.

<sup>14</sup> Tade, O., 2013. “A spiritual dimension to cybercrime in Nigeria: The ‘yahoo plus’ phenomenon”. Retrieved from *Human Affairs*. 23 (4), 689-705. Accessed on 12<sup>th</sup> June, 2024.

<sup>15</sup> Akwaja, C., 2014. “Nigeria: Banks lose N159 Billion to Cyber Crime”. Retrieved from <https://allafrica.com/stories/201406230436.html>. Accessed on 14<sup>th</sup> June, 2024.

<sup>16</sup> Ojeka S.A., Ben-Caleb E., Ekpe, E-O.I., 2017. “Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee Effectiveness”. Retrieved from: *International Review of Management and Marketing*. 7 (2), 340-346. Accessed on 14<sup>th</sup> June, 2024.

<sup>17</sup> Okamgba, J., 2017. “Online Fraud Drains Nigeria over N500 billion in 7 years”. Retrieved from <https://cfatech.ng/online-fraud-drains-nigeria-over-n500-billion-in-7-years/> Accessed on 14<sup>th</sup> June, 2024.

<sup>18</sup> Ponemon Institute, 2017. “The impact of data breaches on reputation & share value”. Retrieved from [https://www.centrif.com/media/4772757/ponemon\\_data\\_breach\\_impact\\_study\\_uk.pdf](https://www.centrif.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf). Accessed on 19<sup>th</sup> June, 2024.

<sup>19</sup> Pennathur, A.K., 2001. “Clicks and bricks”: e-Risk Management for banks in the age of the Internet”. Retrieved from: *Journal of banking & finance*. 25(11), 2103-2123. Accessed on 14<sup>th</sup> June, 2024.

<sup>20</sup> Reyes, A., Britton, R., O'Shea, K., Steele, J., 2011. “Cyber-crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors”. Syngress, Rockland, MA. Accessed on 20<sup>th</sup> June, 2024.

phone numbers. The country's evolving digital infrastructure poses challenges, as outdated systems and inadequate cybersecurity measures in some instances become potential points of vulnerability.<sup>21</sup> Secondly, misconfiguration is a type of human error that exposes sensitive data or systems to unauthorized access. Misconfigurations can occur due to a lack of awareness, training, or proper security policies. Misconfigurations can lead to data breaches, identity theft, or sabotage. Credential stuffing is a type of brute force attack that uses stolen or leaked usernames and passwords to access online accounts. Credential stuffing can result in account takeover, fraud, or identity theft. Credential stuffing relies on the reuse of passwords across multiple platforms. Ransom ware is a type of malware that encrypts the victim's files and demands a ransom for their decryption. Ransomware can cause significant disruption and financial losses to individuals and organizations. Ransomware attacks often start with phishing, social engineering, or web application attacks. Malicious software encrypts data, demanding a ransom for its release, crippling banking operations and compromising customer information. Data Breaches in which unauthorized access to customer databases can result in the exposure of personal and financial information, leading to identity theft and financial fraud.<sup>22</sup>

#### **4.0 THE ROLE OF LAW IN ADDRESSING MOBILE BANKING CONCERNS IN NIGERIA**

While the cybersecurity challenges that affect mobile banking in Nigeria are profound, the law as a fundamental instrument of regulating human actions and conducts, stands as a beacon of hope in addressing the emerging challenges. The major roles the law plays include the regulation of mobile banking activities and imposition of sanctions in cases of breach of the provisions.

In many countries, a critical regulatory prerequisite for launching mobile banking is adopting a risk-based approach for combating money laundering and terrorist financing.<sup>23</sup> In Nigeria, the main legislation for the regulation of banks is the Banks and Other Financial Institutions Act (BOFIA). Another law which regulates banking activities in the country is the Central Bank of Nigeria (Establishment) Act 2007(CBN Act). These two laws give the Central Bank of Nigeria (CBN) powers to supervise and regulate banks and other financial institutions in Nigeria. Section 68 of the BOFIA ACT specifically made provisions covering cyber security.

#### **5.0 RECOMMENDATIONS AND CONCLUSION**

---

<sup>21</sup> Azeez O. Hassan, *supra*.

<sup>22</sup> *Ibid*.

<sup>23</sup> *Ibid*.

It is recommended that the existing laws that regulate banking activities in Nigeria should step up more and be more encompassing in issues relating to matters like cyber security since laws are dynamic and are meant to change according to the social and economic situations of the society. Further, adhering to regulatory frameworks, such as those outlined by the Central Bank of Nigeria (CBN) and other industry regulators, adds a layer of complexity, necessitating banks to maintain robust compliance practices. Additionally, while awareness is growing, there is still a need for heightened cybersecurity education and training, both within banking institutions and among customers, to mitigate the risk of falling victim to cyber threats.<sup>24</sup> Indeed, mobile banking systems help improve the ease of banking, however, it also pose significant cybersecurity challenges. These challenges are complex and profound but they are not over our heads. By implementing the recommendations analyzed in this paper, we can create a sane banking ecosystem where ease of transactions thrives without any form of jeopardy or threats on the finances of either the banks or bank customers.

---

<sup>24</sup> Catia Ballista et Al. “International Experiences of Mobile Banking Regulation” Retrieved from<[www.theigc.org](http://www.theigc.org)> Accessed on 8th June, 2024.