# A Critical Review of Payment Card Data Security Standard Implementation in Nigeria

Ali Thomas Gaga
*Department of Information Technology*
*Faculty of Computing*
*Bingham UniversityKaru,*
*Nasarawa State, Nigeria*
ali-gaga.thomas@binghamuni.edu.ng

Musa Yusuf
*Department of Cybersecurity*
*Faculty of Computing*
*Bingham University*
*Karu, Nasarawa State, Nigeria*
https://orcid.org/0000-0002-7893-9531

Ann Hassan Brijik
*Department of Information Technology*
*Faculty of Computing*
*Bingham University Karu,*
*Nasarawa State, Nigeria*
annebjk@binghamuni.edu.ng

Onu Egena
*Department of Cybersecurity*
*Faculty of Computing*
*Bingham University Karu,*
*Nasarawa State, Nigeria*
onu.egena@binghamuni.edu.ng

***Abstract*—The crux of this study is on the adoption of E-payment system in Nigeria: Its economic benefits and challenges. The arrival of the internet has taken electronic payments and transactions to an exponential growth level. Consumers could purchase goods and services from the internet and send unencrypted credit card numbers across the network, which did not provide much security and privacy. But a wide variety of new secure network payment schemes have been developed as consumers became more aware of their privacy and security. In January 2012, the Nigeria Apex Bank, Central Bank of Nigeria (CBN) rolled out guidelines for the transition of Nigeria's mainly cash-based economy and payment system to cashless and electronic payment (e-payment) system ending over 50 years of mainly cash-based operated economy and payment system. This announcement elicited mixed reactions firstly excitement due to the enormous benefits this transition will impact on Nigeria economy and at the same time elicited panic due to unpreparedness of the economy to transit successfully to electronic payment in a system hitherto filled with bobby trap of security challenges. Ten months later after the introduction of the policy, only a handful of the major stakeholders are fully compliant mainly because of the complexity and the high prohibitive cost of implementation of CBN adopted security framework, the Payment Card Industry Data Security Standard (PCI DSS). This research survey the security challenges facing the implementation of the cashless e-payment policy of Nigeria and at the end recommended a framework to ensure implementation issues in the payment card data security standard in Nigeria is mitigated where all stakeholders can be compliant for a safe electronic payment experience.**

***Keywords*—Cashless economy; electronic payment security; CBN; Nigeria; PoS; ATM; Bank Server; PCI DSS. Electronic payment, e-commerce, e-banking.**

## I. INTRODUCTION

Over the last decade, the Nigerian payments system has evolved from manually processed cash transactions to online and real-time electronic payments system [1]. This evolution is in response to the penetration of the broadband internet services and advanced in technology in the country which facilitates the growth on online business transactions, such as e-commerce, electronic fund transfer, bill payments, etc.

This development eventually required an effective, efficient, timely and secure means of cash settlement for business transactions. Since the conventional means of cash settlement of payment has become inefficient and time consuming. Consequently, the financial sector in Nigeria ventured into this new goldmine of opportunities and began to provide solutions and services to meet the changing needs of the customers. This marked the beginning of a new era in Nigeria's payments system [2]

To ensure secured electronic payment transactions, Central Bank of Nigeria (CBN) had to develop the technical and human capacity necessary to regulate the industry and to put in place necessary regulatory frameworks to achieve these goals [3]. To provide safe and efficient mechanisms for paying and receiving electronic payments with minimum risks, the Payment Card Industry Data Security Standards (PCI DSS) was introduced [4]

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle cardholder information [5]. It was developed by Card companies such as: MasterCard, Visa Card, PayPal and Microsoft in 2009 to address security challenges arising from use of credit, debit and pre-paid cards on payment terminals such as ATM, POS, Online.

The PCI DSS are operational and technical requirements for organizations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in electronic transactions [6]. It is a unified set of security requirements aimed at keeping the cardholder's data secure from data breaches and financial fraud [7]. It is a requirement for any business that processes credit or debit card transactions. Payment Card Industry certification is also considered the best way to safeguard sensitive data and information, thereby helping businesses to build long lasting and trusting relationships with their customers (CBN's Payment System Vision 2020, 2013)

The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and to facilitate the broad adoption of consistent data security measures globally [8]. PCI DSS applies to all entities

involved in payment card processing including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data and/or sensitive authentication data (SAD).

According to Omoniyi, (2020), the PCI DSS are set by the Payment Card Industry Security Standards Council (PCI SSC), founded by American Express, Discover, JCB International, MasterCard and Visa Inc. and they assist merchants and financial institutions achieve the following:

i. Understand and implement standards for security policies.

ii. Understand technologies and processes that protect their payment systems from breaches and theft of cardholder data; and

iii. Understand and implement standards for creating secure payment solutions.

### *A. PCI DSS Requirements*

The PCI DSS is divided into 6 goals and the entity must achieve each goal to be PCI DSS compliant. To achieve the goals, 12 requirements must be met.

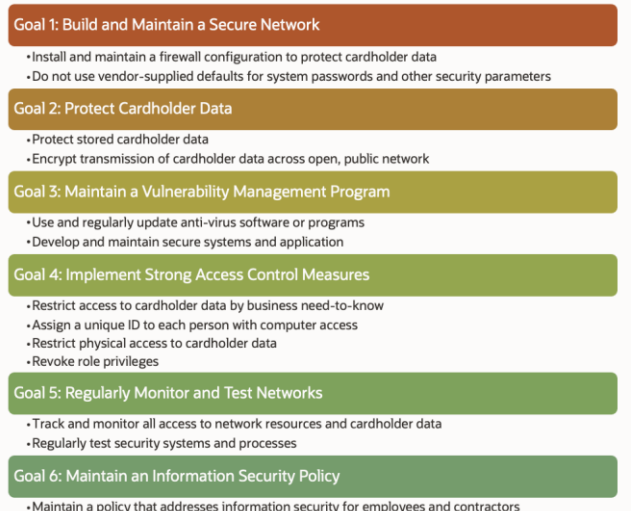


Figure 1: Source: Blogs.Oracle.com (Niddagatta, 2021)

The PCI SSC recommends that entities should not treat compliance as an annual event; rather they should monitor compliance continuously to maximize the security of the cardholder data the entity possesses. In Nigeria, non-compliance with the PCI DSS attracts appropriate sanctions from the CBN. Therefore, to avoid such penalties, merchants and entities should ensure they are compliant with the standards.

### *B. Consequences of Breaching the PCI DSS*

A data breach by any stakeholder that reveals sensitive customer information is likely to have severe consequences (Imperva, 2021). Some of the consequences are as below:

**Fines:** Major payment processors or Card Schemes like MasterCard or Visa have a schedule of fines that are meted out to entities that are non-compliant with the PCI DSS. Also, non-compliance or a breach of the standards in Nigeria will attract fines from CBN. Barrister

**Costs:** where a data breach occurs by any entity, the entity will be required to carry out an audit of PCI DSS compliant. Audit costs are quite expensive and small merchants may suffer a huge amount of loss due to the audit costs.

**Significant penalties:** If a company is found to be incompetent, it will be subject to substantial non-compliance fines, regardless of the size of the company.

**Legal costs, settlements, and judgments:** If a client's data has been compromised, he or she can sue, which can be extremely expensive. If a company does not meet the PCI guidelines, credit card companies can take legal action against it.

**Brand reputation**: A data breach can significantly jeopardize a company's reputation and customer loyalty due to credit card information insecurity. Customers are less likely to trust the company's brand after a data breach, particularly if there is negative publicity surrounding it.

**Unemployment:** If a company is found to be subjected to a breach that would make PCI DSS compliance preventable, reputational damage could result in a sudden drop in sales, with incredibly high fines, penalties, and potential legal costs, which may result in loss of job in the company. (Baykara, 2021)

## II. LITERATURE REVIEW

### *2.1 Electronic Payment System In Nigeria*

The electronic payment system consists of many stakeholders, the major stakeholders of Nigeria electronic payment system include the followings: Consumer or customer, Switching Companies (E payment processors eg, interswitch and E-Transact), Card processing companies (e.g. Value Card), Merchants or retailers, Mobile Money providers (Mobile Payment Providers), Commercial Banks and The financial regulatory agency (the Central Bank of Nigeria)

The electronic payment system handles different transactions such as: Business-to-Business (B2B) transactions mostly involves Bank-to-Bank electronic fund transfer (ETF) and Electronic Cheque Clearing System (ECCS) while Business-to-Customer (B2C) transactions involves the use of payment terminals by consumers/customers such as Point-Of-Sale (PoS) terminals, Mobile payment terminals, Mobile/Internet Banking terminal, Automated Teller Machine (ATM) terminal and Online Merchant portals/e-commerce platforms. Also, there are Customer-to-Customer (C2C) and Customer-to-Business (C2B).

Figure 2 depicts the electronic payment system architecture in Nigeria. The electronic payment switching is handled by the switching companies (e-payment processors) such as Interswitch and e-Transact while the Mobile payment providers, authorized by CBN, handle electronic payment such as e-Purse,

e-Money, Pocket Money etc, using the Telecommunication platforms (GSM) and electronic switching services.

Figure 2: Nigeria's current electronic payment architecture


The Nigerian electronic payment architecture offers about five (5) different models of payment transactions as depicted below and the process flow as shown in Figure 3 to Figure 7:

**Model 1**. Consumer to Merchant e-payment model using PoS terminal (owned by the merchant) and bank issued credit/debit cards (owned by the consumer), Consumer's ATM payment model using the bank issued credit/debit cards and ATM terminal installed in banks' premises to pay customers.

**Model 2:** Consumer to Merchant e-payment model using online portals and bank issued credit/debit cards (owned by consumers),

**Model 3.** Consumer to Merchant e-payment model using online portals and bank issued credit/debit cards (owned by consumers),

**Model 4**. Bank to Bank Electronic Payment System model using Electronic Fund Transfer (ETF) and Electronic Cheque Clearing system (ECCS),

**Model 5**: Mobile Payment/Internet Banking model using consumer's mobile equipment, third-party e-payment software and Bank's Transaction Server to pay consumers using telecommunication gateway and switching platform.

*2.2 Security Challenges Affecting Nigeria Electronic Payment System*

The Nigeria Electronic Payment System is confronted with a lot of security challenges; these challenges are affecting the successful implementation of cashless economy policies in Nigeria. Some of the challenges include:

Identity threats: Fraud committed by inside-outside collusion by fraudsters and corrupt banks' employee in order to defraud the bank or their customers,

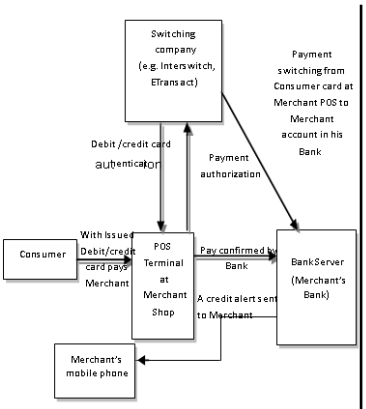


Figure 3: Model 1

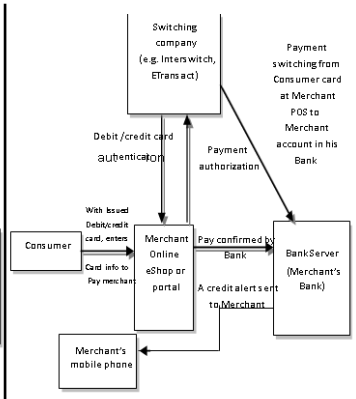


Figure 4: Model 2

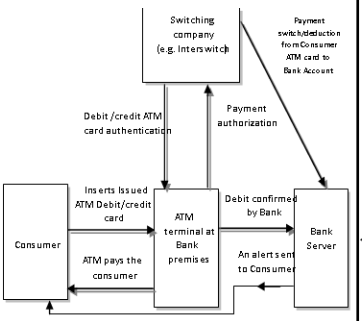


Figure 5: Model 3

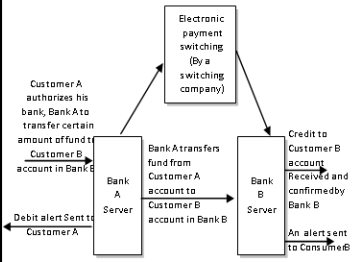


Figure 6: Model 4

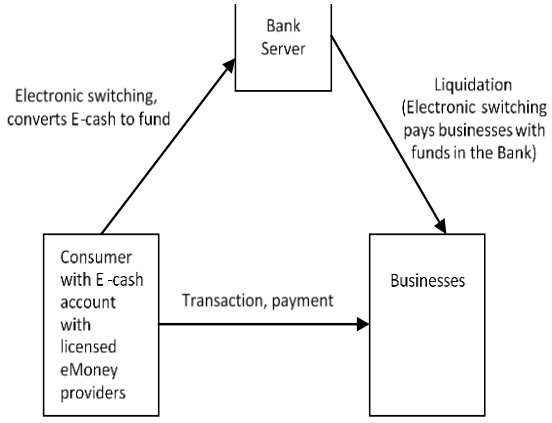


Figure 7: Model 5

Forgery: Armed robbers blowing up ATM terminals installed in Bank premises with explosives and dynamites to cart away physical cash,

Cloning of credit and debit cards of bank customers' cards by hackers through various social engineering tactics to unsuspecting Nigerians to reveal their cards pin ids to enable the hackers withdraw funds from customers' bank accounts using ATM terminals.

Online criminals and hackers exploit security vulnerabilities in merchant websites to receive products or airline tickets for free or at reduced prices without paying a dime.

Customers' privacy invasion and threats: Dearth of technical and security awareness and knowledge by most users which make them gullible to the antics of e-payment and online fraudsters.

Lack of legal or legislative bill to sanction offenders or e-payment criminals to serve as deterrent.

The security challenges identified above fall into three categories of security challenges: physical, data/information and operational security challenges. Any security system designed for Nigeria's e-payment system must take into full account of these security vulnerabilities and challenges identified above as well as the loopholes identified in the current Nigeria e-payment security models to be successful.

### *2.3 Payment Card Industry Data Security Standard*

Prior to the release of PCI DSS, the payment card industry comprising of Master card, Visa, American Express, JCB and Discover, they relied upon their individual policies regarding the security processes and storage of payment card data. This have created significant challenges as regards to an integrated approach to the issues surrounding PCI. Therefore, the Payment Card Industry Security Standards Council combined these individual policies resulting in the released of PCI DSS version 1.0 in December 2004 (Roebuck, 2012). The Council ensure procedures were put in place to mitigate the breach of sensitive payment card data by ensuring merchants that accept this data are both aware of and enforce the necessary security measures (Chuvakin & Williams, 2011).

Early documentation from the American Bar Association (2008) and some more recent research from Chuvakin and Williams (2011) and Bakay et al, (2014) suggested that a climate of growing concern surrounding the protection of sensitive credit card data led to the PCI DSS being devised by MasterCard and Visa to alleviate concerns surrounding the safe handling of cardholder data in a practical step by step process (American Bar Association, 2008, Bakay et al, 2014). An important feature driving the initial stages of the standard's creation was the need for compliance and the importance of clarity within its process and documentation. This early phase of the standards creation contained numerous flaws subsequently rectified by version 1.2.1, this version had many requirement additions to address these issues, providing more guidance on wireless technologies, virtualisation and encryption methods, resulting in a higher level of security than the early version (Bhargav, 2014). However, PCI DSS version 2 became the industry standard in active use until December 2, 2014.

### *2.4 Challenges of implementing PCI DSS Frameworks*

The CBN had directed all players in the banking and electronic payment sector to speedily attain Payment Card Industry Data Security Standard (PCI DSS) compliance which is the security standard adopted by the CBN for Nigeria cashless e-payment system. This is to ensure that card users in the country will continue to experience enhanced payment data security.

The challenges of implementing Payment Card Industry Data Security Standard (PCI DSS) in Nigeria as adopted by the CBN are as follows:

i. It provides data security but is very expensive to implement with an ordinary stakeholder such as a merchant.

ii. It is very complex and complicated to implement and not user-friendly. It therefore costs a lot of money and time to train IT staff to master it.

iii. Because of fines and penalties imposed by the originators on defaulting stakeholders, a lot of suspicions are created on the real intentions for the introduction of the security framework thereby casting aspersions on the objectives of the framework.

## III. Research Methodology

To carry out this research, secondary data was used from existing literature, academic journals, existing data on the subject and the Central Bank of Nigeria policy documents on electronic payments and cashless economy. The research identified challenges in the implementation of the Payment Card Industry Data Security Standard and proposed an enhanced framework for the implementation of the Payment Card Industry Data Security Standard in Nigeria.

### *3.1 Propose Enhancing PCI DSS implementation in Nigeria*

To enhance the implementation of PCI DSS in Nigeria, there is a need to transfers the bulk of the burden of cost of compliance (COC) and cost of ownership (TCO) to the major e-payment stakeholders such as commercial banks, switching companies, card processing firms and mobile money providers who will at the long run recoup their investments through electronic transactions. Security vulnerability software can be provided by the switching company for other stakeholders to enable them to carry out regular vulnerability system scans. The license for this software should be a one-time life license updateable for a minimal fee per annum.

In Nigeria, the merchants and the consumers form the majority of the electronic payment stakeholders and to ensure full security compliance, these stakeholders must be accommodated; the total cost of ownership (TCO) must be reduced for the merchant while user education on security compliance must be transferred to the consumers at little or no cost to them. At the same time, the complexity of implementation must be reduced, and the security system made simpler to attract full compliance by all the stakeholders.

We therefore propose that to ensure compliance by all stakeholders, there is a need for enhanced guidelines and standards for all the categories of electronic payment stakeholders:

i. Security compliance guidelines for the consumers (on how to use credit and debit cards on payment terminals).
ii. Security compliance guidelines for the merchant (using Point-Of-Sale (PoS) and Online Ecommerce Portal).
iii. Security compliance guidelines for Switching firms and card processing companies.
iv. Security compliance guidelines for the commercial banks.

v. Security compliance guidelines for the Mobile Payment providers.
vi. Security compliance guidelines for the government/ regulatory agency
vii. Security Compliance Guidelines for the Consumers.

*3.1.1 Security compliance guidelines for the consumers*

The consumer or customer is the least of the e-payment stakeholders in terms of responsibilities of security compliance. His duties are merely to protect his credit/debit card pins from being exposed and stolen; also, to report to his bank or card provider immediately or in the event of loss or misplacement of his credit/debit card so that the account will be blocked to protect the money in his account from being stolen. Equally, the consumer should reconcile with his bank for every transaction via debit/credit alert confirmation in his mobile phone through the Bank's mobile apps or USSD code.

*4.1.2 Security Compliance Guidelines for the Merchant stakeholder*

The merchant deals directly with the consumers/customers. He sells goods or services to the consumer and the consumer pays him electronically via the e-payment channels or terminals such as POS, Mobile device, online e-Commerce shop or portal as depicted in Figure 8. The primary concern of the merchant is for the consumer to pay him through any of the available e-payment channels and his bank account successfully credited and he obtains a credit confirmation alert in his mobile phone from his bank before he can allow the consumer or customer to go away with his goods or services.

The suggested security requirements for the merchant using the Point of Sale (POS) channel are as follows:

i. To provide physical security for the PoS equipment so that robbers will not cart it away.
ii. To install PoS equipment in such a way as to prevent tampering by would-be criminals either from outside or within his shop.
iii. To capture the biometric feature of each customer (facial) using camera or close circuit television (CCTV) in case of fraud to identify the culprit by law enforcement agents.
iv. To reconcile his account status and balance with his banker via credit alter confirmation to his mobile phone to ensure that his account is credited before allowing the consumer/customer to go away with the goods.

For the merchant-customer e-payment model depicted in Figure 4.5, security vulnerability lies on the interfaces between the e-payment terminals and the merchant's Bank Server. It is therefore the duties of the e-payment switching companies to provide cryptographic data security through encryption and decryption and other additional data security such as digital signatures and hashing for every e-payment transaction.

For the merchant-consumer model using online e-Commerce shops or portal the merchant owes full responsibility to secure his online portal or shop to provide data security. The suggested guidelines for merchants operating online e-Commerce portal or shops are listed as follows:

- He must obtain certificate authority (CA) to verify buyer/consumer's identities before selling,
- He must provide point-to-point encryption for every transaction through the provision of secure socket layer (SSL) on http interface (i.e. https), secure shell (SH), Internet Protocol Security (IPSec) etc to ensure data confidentiality and hashing function to ensure data integrity.

*4.1.3 Security Compliance Guidelines for the Switching companies*

The e-payment switching companies play the major role in the entire electronic payment system in Nigeria. The switching firms conduct all debit/credit transactions switching from consumer credit/debit cards on e-payment terminals such as ATM, PoS, mobile devices, online ecommerce portals to the authorized bank accounts of the merchants or electronic switching from a business account in a bank to another business account in another bank.

The channels or interfaces in the electronic switching, most of the time being wireless and wired Local (LAN) or Wide Area Networks (WAN) are vulnerable to all sorts of data and operational security attacks. So, the switching firms must provide full compliance and protection for the data and operational capacity of all the e-payment transactions and only charge other stakeholders minimal fees per annum.

The following security guidelines are suggested for the switching companies. They should:

i. Providing end-to-end data encryption using strong cryptographic cipher engines (AES 128 bit) is suggested to ensure data confidentiality.
ii. Provide strong user authentication to provide data confidentiality and integrity.
iii. Provide Message Authentication Codes (MAC) or hashing functions to provide data integrity for all the e-payment transactions.
iv. Perform vulnerability and compliance system scan on all interconnected stakeholders on their network on a regular basis (maybe quarterly) at a minimal fee to the stakeholders.

The channels or interfaces in the electronic switching, most of the time being wireless and wired Local (LAN) or Wide Area Networks (WAN) are vulnerable to all sorts of data and operational security attacks. So, the switching firms must provide full compliance and protection for the data and operational capacity of all the e-payment transactions and only charge other stakeholders minimal fees per annum.

*4.1.4 Security Compliance Guidelines for the Commercial Banks*

Commercial banks have a lot of customers that deposit their funds with them. They also deal directly with merchants who maintain business accounts with them. The e-payment switching firms switch payment electronically from various e-payment terminals such as ATM, PoS, Online Ecommerce portals, Mobile devices once the consumers authorize payment using their credit/card cards.

Also switching firms switch payment electronically from one business account in one bank to another business account in another bank. All these e-payment transactions end up in the banks' transaction servers which work 24 hours a day, 7 days a week. It is therefore the duties of both the commercial banks and switching firms to provide security to protect the Transaction server and the e-payment interfaces from being security breached.

The following security compliance guidelines are suggested for the commercial banks to ensure compliance:

i. Banks should provide physical security for ATM terminals to ensure availability of ATM terminals at any time and to protect the ATM terminal from being attacked by armed robbers.
ii. Banks should provide end-to-end encryption of all transaction data from the Transaction Server to all e-payment terminals via electronic payment switching gateways. Powerful encryption engines such as AES (128 bit) are hereby suggested. This will provide data confidentiality and privacy.
iii. Banks should provide full authentication of their customers at ATM payment terminals using simple username and pin logins as well as additional biometric authentication mechanisms to capture customers' biometric features such as photography.
iv. Banks' core Banking solutions should be fully protected with hash functions or Message Authentication Codes (MAC) to protect the payment data from being compromised by fraudsters either from the within or outside. This will provide data integrity.
v. Additionally, banks should ensure that all customers are sent instant SMS transaction alert or confirmation through their mobile phones to enable account reconciliation.

The following flowchart (Figure 8) depicts the proposed enhanced modified security framework for the protection of transaction data from a consumer (paying with his debit/credit card) to merchant account in the bank using electronic switching platforms.

### *4.1.5 Security Compliance Guidelines for the government/ regulatory agency*

The regulatory agency, the Central Bank of Nigeria (CBN) can spearhead the passing into law security compliance and liability bill that will force every e-payment stakeholder to become compliance and to accept responsibility in the event of any financial loss to a business or a consumer because of lack of security compliance. The legislative bill should equally spell out who should pay who in the event of security liability. Also, penalties should be clearly spelled out for would-be-criminals and fraudsters using long jail term sentences to discourage potential financial criminals.

CBN should also educate the users (consumers) and the other stakeholders on the need to be security compliance and how to develop framework for Nigeria cashless e-payment system from consumer to merchant accounts in the banks. Figure 4.6 shows the system flowchart depicting the proposed enhanced modified data security.

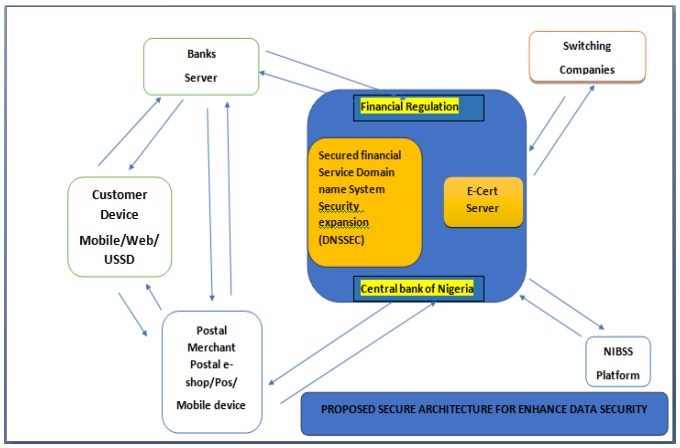


Figure 8

## IV. CONCLUSION

PCI DSS is the very first industry-wide standard that aims at achieving a strong protection of sensitive consumer and cardholder data and prevents major security issues. It is the result of a collaborative effort of the major payment card networks and issuers. The standard sets force requirements in many aspects, including secure networks, cardholder data protection, access control, vulnerability management, security assessments, and reporting.

The benefits of the standard are the definition of the standard set of security tools, practices, and measurements for stakeholder information protection, increased confidentiality and integrity, and a strong infrastructure to prevent security attacks. Through a continuous process of assessment, remediation, and reporting, a compliant merchant or service provider would significantly reduce the risk of security breaches. Major card networks such as Visa, MasterCard, Discover, American Express, and JCB mandate that merchants and service providers achieve certain levels of compliance.

However, its 12 requirements are non-trivial to implement due to its complexity in both technical and organizational terms. For example, it is widely acknowledged that security key management is difficult to maintain. In addition, the standard calls for continuous assessments of their security programs, which is often regarded as a burden to many merchants. Furthermore, some of the unclear requirements, especially those which do not have any recommended implementation, lead to ambiguity. It has been observed that many merchants, acquirers, and service providers have difficulties to adapt the standards.

Nevertheless, a high level of PCI-compliance has not been achieved. As reported by Visa, only 22% of its largest merchants were PCI-compliant, not to mention smaller merchants with tight budgets and resources. As implementing all these requirements requires a significant amount of effort and technical competence, there are several companies that provide compliance solutions for the PCI DSS. Those solutions share certain similarities. However, to evaluate and compare their efficiencies properly, there needs to be available, complete implementation details of the vendors and survey reviews from the corresponding client companies.

Due to the challenges of standard compliance, there are many development opportunities. For example, merchants and banks maintain direct customer relationships, and customer data is pervasive in their business to provide high-quality customer service. It is difficult to track and assess data exposures. The pervasiveness of data is clearly a challenge for security protection. Another example is the key management. This issue is complicated by frequent keying and re-keying. Nevertheless, technical advances in many of these aspects can eventually lead to a reassessment and revision of the current standard, which may essentially improve penetration of the security standard, and may reduce the risks of security breaches.

## V. RECOMMENDATION

To continue to grow and protect stakeholder's data, recommendations are given to ensure there is compliance in the PCI DSS in Nigeria. The following recommendations are thus.

i. Identifying the business challenges: To implement a robust security environment, the processes and controls should require internal changes and investments in the IT infrastructure. Prioritizing the PCI activities, having a common understanding of the rational and business drives, documenting the standard and security policy, and audit trail, and managing the resource and cost burden of maintaining compliance in line with identified business risks, and budget constraints will contribute to identifying the business challenges.

ii. The IT infrastructure: The components in the environment must encrypt the stored data and the transmitted data. Communications must be mediated by firewall and logged via secure network. Each asset must be monitored and assessed for vulnerability in a timely manner

iii. Compliance management, governance & demonstration: Monitoring compliance posture has become a challenge for the organizations implementing the PCI DSS. To maintain and support the compliance management architecture and to map its technology requirements, several key disciplines are followed for incident prevention and management.

iv. Incident prevention is done by risk analysis and assessment, with the completion of independent compliance audits, and with self, external, and database security assessments.

v. Data protection is achieved through firewalls, antivirus tools, secure application configuration, and access control with strong authentication contributes to security incident prevention.

vi. Incident management is done with proper detection, investigation, and response. To ensure that compliance can be tested properly, standards and audit requirements are categorized.

## VI. REFERENCES


[1] Afaha, J. S. (2019). Electronic payment systems (E-payments) and Nigeria economic growth. European Business & Management, 5(6), 77.

[2] Soetan, T. O., & Mogaji, E. (2024). Modernization of the Nigerian Financial System. In *Financial Services in Nigeria: The Path Towards Financial Inclusion, Economic Development and Sustainable Growth* (pp. 245-268). Cham: Springer Nature Switzerland.

[3] Bebeji, U. S. (2024). AN EXAMINATION OF THE REGULATORY STRUCTURE FOR ELECTRONIC BANKING IN NIGERIA. *Fountain University Law Journal*, *1*(1), 9-22.

[4] Bhutta, M. N. M., Bhattia, S., Alojail, M. A., Nisar, K., Cao, Y., Chaudhry, S. A., & Sun, Z. (2022). Towards Secure IoT-Based Payments by Extension of Payment Card Industry Data Security Standard (PCI DSS). *Wireless communications and mobile computing*, *2022*(1), 9942270.

[5] Lessa, L., & Gebrehawariat, D. (2023). Effectiveness of banking card security in the Ethiopian financial sector: PCI-DSS security standard as a lens. *International Journal of Industrial Engineering and Operations Management*, *5*(2), 135-147.

[6] Razikin, K., & Widodo, A. (2021). General cybersecurity maturity assessment model: Best practice to achieve payment card Industry-Data security standard (PCI-DSS) compliance. *CommIT (Communication and Information Technology) Journal*, *15*(2), 91-104.

[7] Paul, E., Callistus, O., Somtobe, O., Esther, T., Somto, K., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the United States financial sectors. *International Journal on Soft Computing*, *14*(3), 01-16.

[8] Lessa, L., & Gebrehawariat, D. (2023). Effectiveness of banking card security in the Ethiopian financial sector: PCI-DSS security standard as a lens. *International Journal of Industrial Engineering and Operations Management*, *5*(2), 135-147.