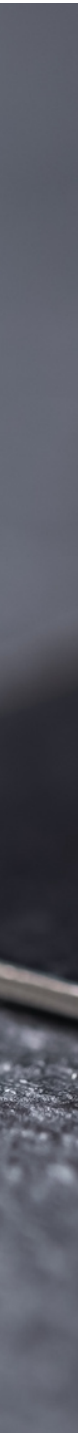
ÆLEX

ARTICLE SERIES

# PCI DSS – ITS RELEVANCE TO CARD SCHEMES AND FINTECHS

JANUARY 203

www.aelex.com



# INTRODUCTION

With the advancements made in payment systems space over the last few years, the purchase of goods and services is frequently done with the use of payment cards. Thus, whether you are swiping, inserting or placing your card on a scanner, payment cards have transformed the way we transact business. Vendors or merchants who accept payment cards usually enter into contracts with payment processors and banks for the processing of payments through their channels. One of the key conditions in these contracts is that the vendor/merchant must be compliant with the Payment Card Industry Data Security Standards ("PCI DSS").

The question that logically follows is what is the PCI DSS? In this article we explain what the PCI DSS is, the requirements that must be met to comply with the standards and the consequences of breaching the PCI DSS.

# WHAT IS THE PCI DSS?

The PCI DSS are the operational and technical requirements for organisations accepting or processing payment transactions, and for software developers and manufacturers of applications and devices used in those transactions[1]. It is a unified set of security requirements aimed at keeping cardholder data secure from data breaches and financial fraud[2].

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:

- understand and implement standards for security policies;
- understand technologies and ongoing processes that protect their payment systems from breaches and theft of cardholder data; and
- understand and implement standards for creating secure payment solutions[3].

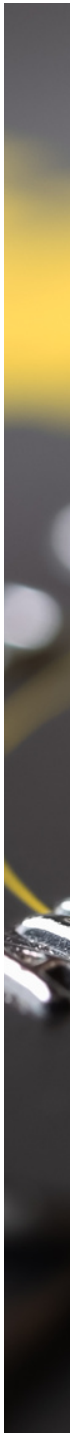
# WHO DOES IT APPLY TO?

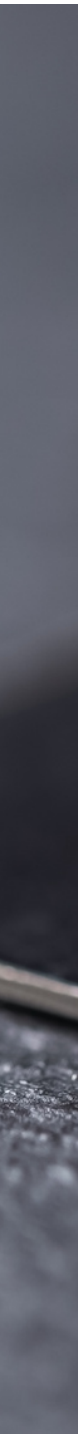
The PCI DSS is applicable to every entity that processes or accepts payment cards. It also applies to entities that store, transmit or process cardholder data or authentication data such as Know Your Customer Data for cardholders [4]. There is no exception to its application as even merchants who process small volumes of transactions are expected to comply with the standards.

There have been arguments made in some quarters that since the PCI DSS is not a legal obligation or legal requirement, compliance should be optional.

[1]https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security. Accessed 11 November 2020.
[2]https://www.lexology.com/library/detail.aspx?g=6c3deb36-5832-4e2c-80a0-c25f97d39a9a. Accessed 11 November 2020
[3] https://www.pcisecuritystandards.org/pci_security/. Accessed 11 November 2020.
[4]https://www.lexology.com/library/detail.aspx?g=94f604cc-acac-4d26-ac74-b9e329db1067. Accessed 11 November 2020.







However, as stated earlier in this article, vendors are required to comply with all their contractual obligations, including fulfilling any obligations related to PCI DSS. Furthermore, complying with the PCI DSS signals that the entity has exercised reasonable care in performing its functions and can be used as a strong defence should allegations of data breaches be levied against the organisation.

In Nigeria, the Central Bank of Nigeria ("CBN") makes compliance with the PCI DSS mandatory for card schemes, payment gateway, payment processors and other relevant stakeholders in the ecosystem.

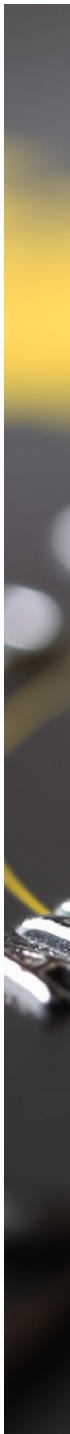
The Guidelines on Operations of Electronic Payment Channels in Nigeria, as well as the Guidelines for Card Issuance and Usage in Nigeria, stipulate that all industry stakeholders who process and/or store cardholder information shall ensure that their applications and processing systems comply with the minimum requirements and standards, the minimum standard being PCI DSS certification[5]. This therefore brings a lot of fintech companies within this umbrella as they process and store cardholder information in order to consummate transactions.

## PCI DSS REQUIREMENTS

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

[5] Paragraph 3.2





| S/N | GOALS | REQUIRMENTS |
|---|---|---|
| 1. | Implement Strong Access Control Measures | 1. Restrict access to cardholder data. Access to data should be on a business need-to-know basis.<br>2. Restrict physical access to cardholder data.<br>3. Assign a unique ID to each person who has computer access to cardholder data. |
| 2. | Maintain a Vulnerability Management Program | 1. Use anti-virus software and malware programs. Keep them up to date as possible.<br>2. Develop and maintain secure systems and applications. |
| 3. | Build and Maintain a Secure Network | 1. Install and maintain firewalls to protect cardholder data.<br>2. Do not use third party system passwords or vendor supplied defaults for system passwords and other security parameters. |
| 4. | Regularly Monitor and Test Networks | 1. Track and monitor all access to network resources and cardholder data.<br>2. Regularly test security systems and processes. |
| 5. | Protect Cardholder Data | 1. Protect stored cardholder data.<br>2. Encrypt transmission of cardholder data across open, public networks. |

| S/N | GOALS | REQUIRMENTS |
|---|---|---|
| 6. | Maintain an Information Security Policy | 1. Maintain a policy that addresses information security for employees and contractors[6]. |

The PCI SSC does not enforce compliance with the goals and requirements as compliance is usually done through contracts with payment processors and banks as earlier stated in this article. However, the PCI SSC recommends a three-step process for compliance[7], and even has accredited assessors who can assess if an entity is compliant with the standards. Where an entity cannot afford to hire an assessor, the PCI SSC has self-assessment forms and procedures for organisations and companies that want to implement the standards.

The PCI SSC recommends that entities should not treat compliance as an annual event; rather they should monitor compliance continuously to maximise the security of the cardholder data the entity possesses[8]. In Nigeria, non-compliance with the PCI DSS will attract appropriate sanctions from the CBN[3]. Therefore in order to avoid such penalties, merchants and entities should ensure they are compliant with the standards.

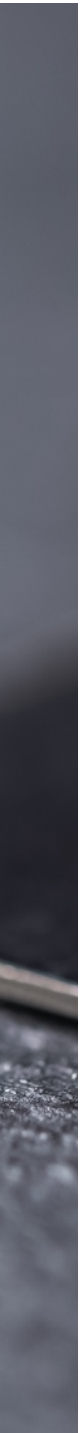
[6]https://www.pcisecuritystandards.org/merchants/process. Accessed 12 November 2020. For a more detailed version of the goals and the requirements of the PCI DSS see the current version of the Standards here.
[7] https://www.pcisecuritystandards.org/pci_security/how. Accessed 12 November 2020.
[2]https://www.pcisecuritystandards.org/pci_security/how. Accessed 12 November 2020.
[8]Paragraph 4.10 of the Guidelines on Operations of Electronic Payment Channels in Nigeria

## CONSEQUENCES OF BREACHING THE PCI DSS

Though some countries are considering legalising the standards, (Nigeria's CBN has already made compliance mandatory), there are also some consequences that push entities into obeying the requirements of the standards and they include the following:

**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. Some contracts that the Payment Card Brands have with entities that process card holder data even specify that a fine can be imposed where it seems that a breach is likely to occur. Also, non-compliance or a breach of the standards in Nigeria will attract fines from CBN.

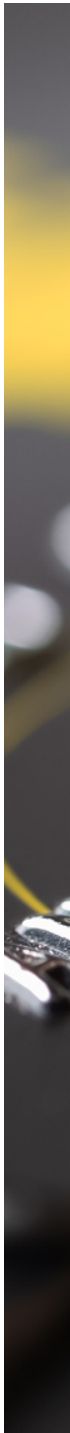
**Costs:** where a data breach occurs, the contract the entity entered into with a Payment Card Brand or Bank, may stipulate that the company or organisation must carry out an audit to investigate whether or not it is PCI DSS compliant. Investigative costs are quite expensive and small merchants may suffer a huge amount of loss due to the investigative costs.



Also, entities can incur hardening and demonstration costs after a data breach as the contracts or agreements will most likely impose an obligation on them to report, engage and show how they have rectified the data breach.

## CONCLUSION

All entities that handle cardholder data should be aware of the PCI DSS and strive to be compliant with the standards. Compliance with the standards outweighs the consequences of breaching them and entities should try to limit their liability for data breaches as much as possible by strongly considering being obedient to the PCI DSS and use acquiescence with the standards as a measure of how responsible they are with all card holder data they store or process.



ÆLEX

## AUTHOR

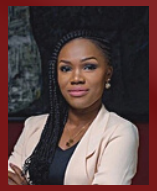

Davidson Oturu
doturu@aelex.com


## CONTACTS


Davidson Oturu
doturu@aelex.com

Ifeoluwa Ebiseni
iebiseni@aelex.com

Florence Bola Balogun
fbola-balogun@aelex.com



Peretimi Pere
ppere@aelex.com


ÆLEX is a full-service commercial and dispute resolution firm. It is one of the largest law firms in West Africa with offices in Lagos, Port Harcourt and Abuja in Nigeria and Accra, Ghana. A profile of our firm can be viewed here. You can also visit our website at www.aelex.com to learn more about our firm and its services.'

# CONTACT DETAILS


**LAGOS, NIGERIA**

4th Floor, Marble House
1, Kingsway Road, Falomo
Ikoyi, Lagos

Telephone: (+ 234 1) 2793367; 2793368
4736296, 4617321-3;
Facsimile: (+ 234 1) 2692072; 4617092
E-mail: lagos@aelex.com

**PORT HARCOURT, NIGERIA**

2nd Floor,
Right Wing UPDC Building
26, Aba Road
P.O. Box 12636, Port Harcourt
Rivers State, Nigeria

Telephone: (+234 84) 464514, 464515
574628, 574636
Facsimile: (+234 84) 464516, 574628
E-mail: portharcourt@aelex.com

**ABUJA, NIGERIA**
4th Floor,
Adamawa Plaza
1st Avenue, Off Shehu Shagari Way
Central Business Area
FCT Abuja, Nigeria

Telephone: (+234 9) 8704187, 6723568,
07098808416
Facsimile: (+234 9) 5230276
E-mail: abuja@aelex.com

**ACCRA, GHANA**

Suite CCasa Maria
28 Angola Road
Kuku Hill, Osu
Accra

Telephone: (+233-302) 224828, 224845-6
Facsimile: (+233-302) 224824
E-mail: accra@aelex.com