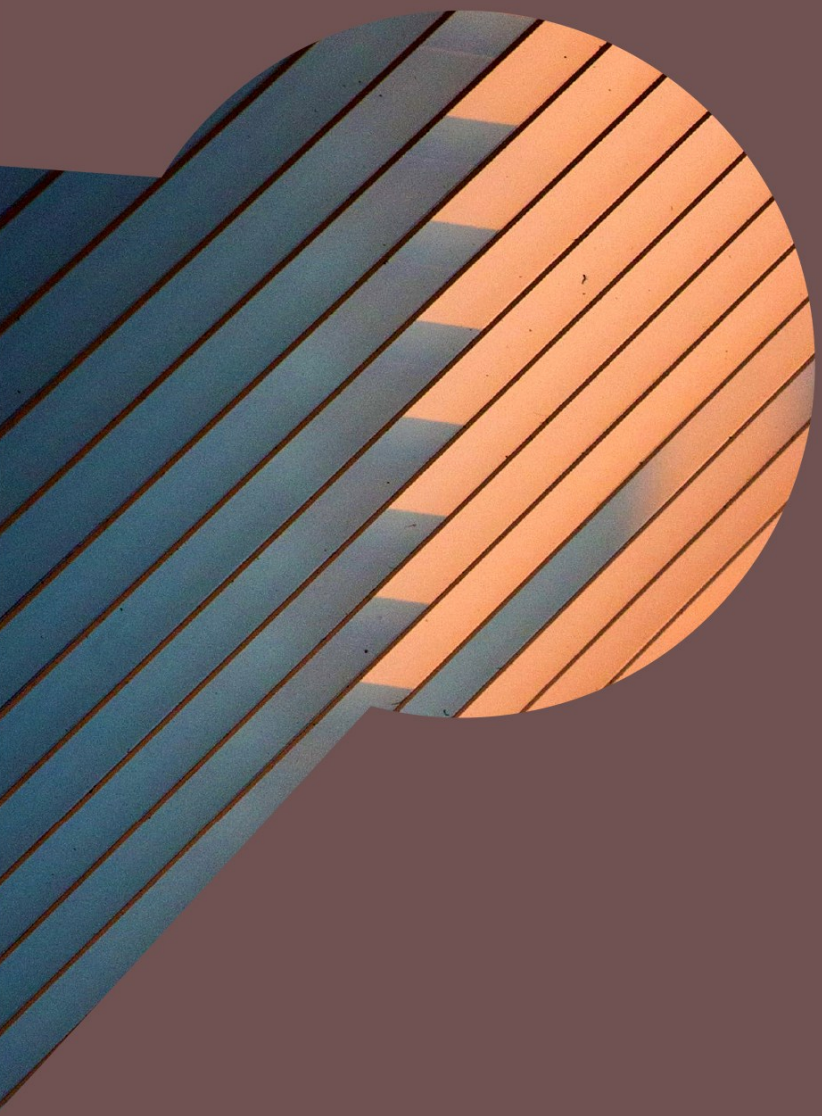
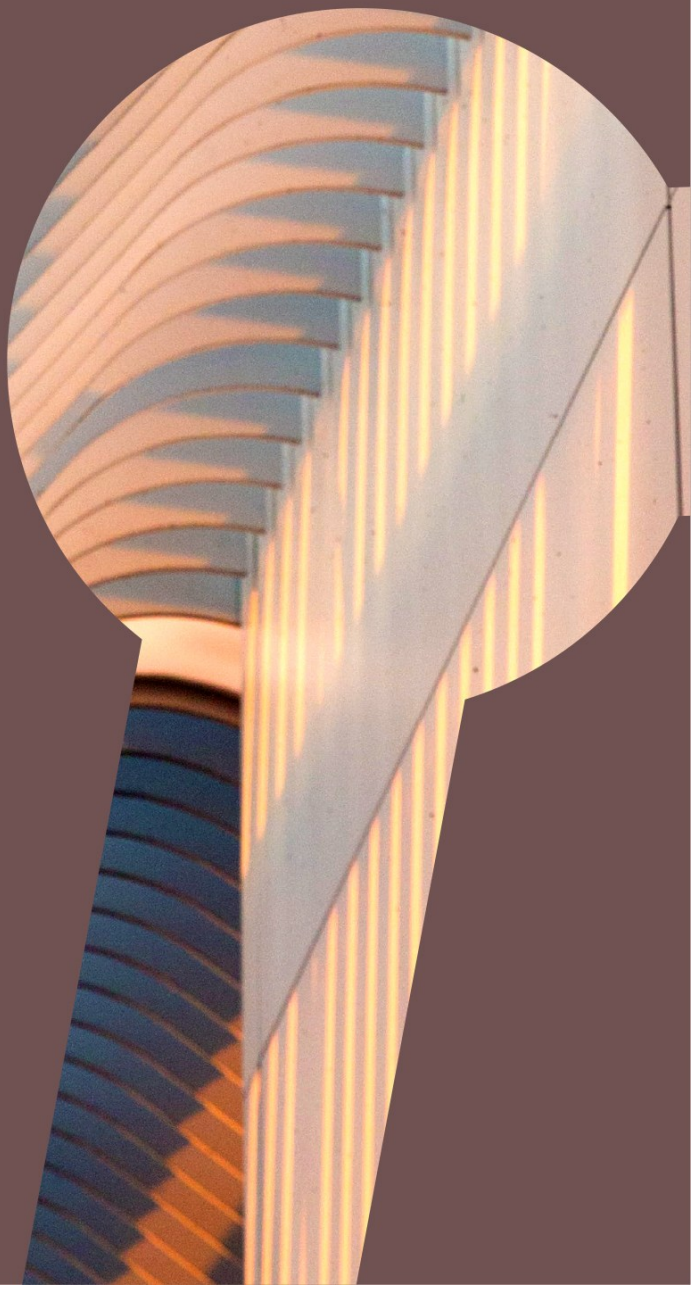
ALUKO & OYEBODE
ALN





Incident Response Beyond the Organisation: A Brief Overview on Cybersecurity Incident Reporting Obligations under Nigerian Law

Introduction

Generally, organisations may be categorised into those who have experienced cybersecurity incidents and those that would experience cyber incidents.[1] The reality is that most organisations, whether they have experienced a cyber threat/incident in the past or not, may be on their way to their first or the next cyber threat/incident. These incidents may manifest in different ways, most common occurrence include personal data breaches, loss of information, or other information technology related happenstances or incidents which impact information technology system/network. A cybersecurity incident may be an incident which has been defined as such, either by law or in the organisation's cyber-threat intelligence programs. Different laws have different requirements in respect of cyber incident responses and reporting. In preparing to respond to a cybersecurity incident, organisations are required to take into consideration applicable legal requirements for reporting cybersecurity incidents.

Against the recent spate of international cybersecurity incidents reported by Harrods, Marks & Spencer, Co-op, Addidas among others, this article examines some key requirements under Nigerian law in relation to escalating/reporting cybersecurity incidents.[2]

Cybercrimes Act (Prohibition, Prevention etc) Act 2015 and Cybercrimes Act (Prohibition, Prevention etc) (Amendment) Act 2024

A cyber threat under this law refers to any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network. Organisations are required to report ***all*** cyberthreats to the National Computer Emergency Response Team Coordination Center (**ngCERT**) through their respective sectorial Computer Emergency Response Team (**CERT**) or sectorial Security Operation Centers (**SOC**) (where available) ***immediately, and no later than 72 hours, after detection.***[3]

Therefore, organisations should identify the sectoral CERT or SOC relevant to their business operations and the relevant means of notifying such CERT or SOC in their incident response plans. Some sectoral CERTs and SOCs currently operating in Nigeria include (a) Nigeria Financial Computer Emergency Response Team (**NigFinCERT**); and (b) the Nigeria Communications Commission Computer Security Incidence Response Team (**NCC CSIRT**).

Nigeria Data Protection Act 2023

A personal data breach is a security incident that results or is likely to result in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data.[4] Personal data breach as a cybersecurity incident would typically involve where a breach of personal information through or contained in information technology system/network. In the event of a personal data breach, organisations acting as data controllers[5] are required to report such breaches to the Nigeria Data Protection Commission (**NPDC**) no later than ***72 hours*** after becoming aware of such breach, where the breach is likely to result in a risk to the ***rights*** and ***freedoms*** of a data subject.[6] A personal data breach may be deemed to result in such risk, where by the nature of the breach and personal data involved, is likely to impact any right and freedom of data subject, such as social or economic rights as contained in the

[1] Andrew T Garbarino, 'More Than Ever, Cybersecurity Is a Board-Level Concern' (2019) 262 New York Law Journal 1, 1.
[2] Cyber Monitoring Centre estimates cost of UK retail attacks at £440 million
[3] Section 21 Cybercrimes Act (Prohibition, Prevention etc.) 2015 and Section 3 Cybercrimes Act (Prohibition, Prevention etc.) (Amendment) Act 2024
[4] Section 65 Nigeria Data Protection Act 2023
[5] "Data controller" means an individual, private entity, public commission, agency or any other body who, alone or jointly with others, determines the purposes and means of processing of personal data.
[6] Section 40(2) Nigeria Data Protection Act 2023

constitution or other legal or similar instrument. Some examples of this includes personal data breaches involving account login information, residential address, criminal and health records, Bank Verification Numbers (BVN), National Identification Numbers (NIN) etc.

A notification to the NDPC should contain:

a) a description of the personal data breach including the date, time or period during which the personal data breach occurred, and the personal data involved;
b) an assessment of the risk of harm to individuals as a result of the personal data breach;
c) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the personal data breach;
d) a description of steps the organisation has taken to reduce the risk of harm to individuals;
e) a description of any steps the organisation has taken to notify individuals of the loss or unauthorised access or disclosure of their personal data; and
f) the contact details of the key personnel in the organisation for the purpose of corresponding with the NDPC.

Additionally, where an organisation acts as a data controller, the Nigeria Data Protection Act 2023 (**NDPA**) requires that such organisations should ***immediately*** notify concerned data subjects where a personal data breach is likely to result in a **high risk** to their rights and freedoms.[7] A notification to the data subject should include the following information:

a) a description of the nature of the personal data breach;
b) the name and contact details of a point of contact of the organisation where more information can be obtained;
c) a description of the likely consequences of the personal data breach; and
d) measures taken or proposed to be taken to address the breach or effectively mitigate the possible adverse effects of the data breach.

For organisations acting as data processors or a sub-processor[8], the NDPA requires that such organisations notify an engaging data controller/processor of personal data breaches ***upon becoming aware*** of such breach.[9] This notification should include the categories, and an approximate number of the data subjects whose personal data is compromised. Further, the processor must respond to all information requests from the engaging data controller or processor with respect to the personal data breach.

Based on the foregoing, it is essential that organisations identify and document their role (i.e. whether as controller, processor or sub-processor) with respect to their data processing operations; and attribute their incident response plans to take note of the differences in their reporting obligations in the different and relevant scenarios in Tables 1, 2 and 3 below.

[7] A personal data breach may be deemed to result in such risk, where by the nature of the breach and personal data involved, (a) is likely to lead to other personal data of the data subject being accessed; and (b) the data subject may become a victim of fraud, identity theft or exposure of sensitive personal data. *See Article 33(2) NDP Act 2023 General Application and Implementation Directive 2025*
[8] "Data processor" means an individual, private entity, public authority, or any other body, who processes personal data on behalf of or at the direction of a data controller. A sub-processor is a data processor that acts on behalf of another data processor.
[9] Section 40(1) Nigeria Data Protection Act 2023

Reporting Flow Table

Table 1: Data Controller Personal Data Breach Scenario

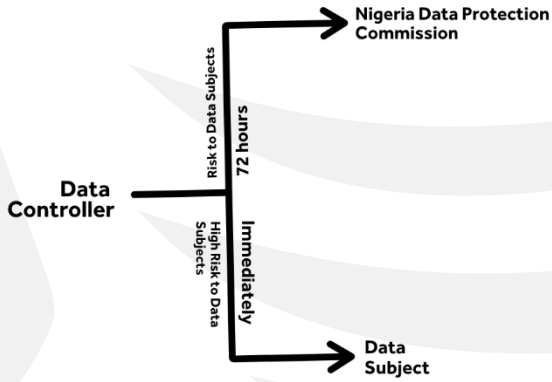


Table 2: Data Processor Personal Data Breach Scenario

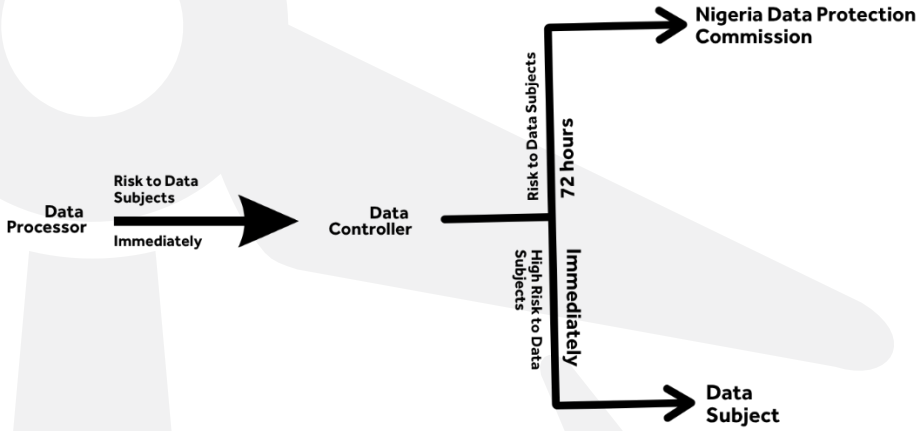
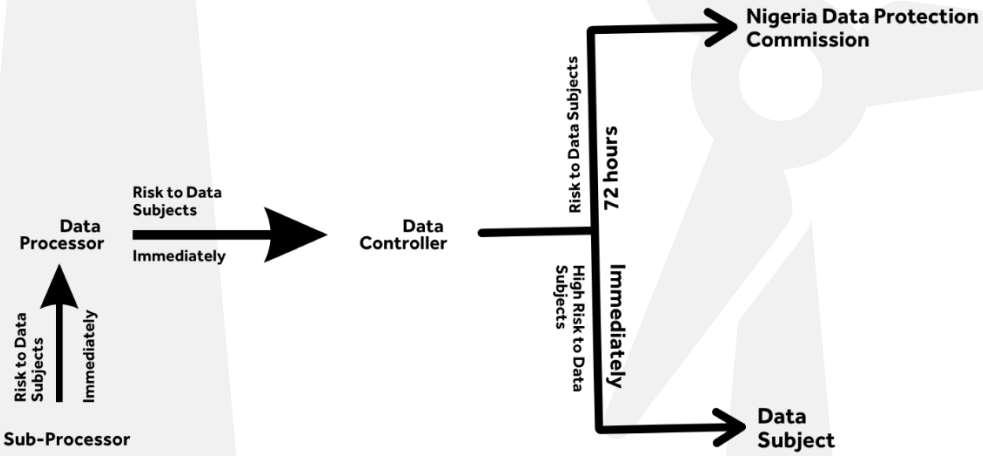


Table 3: Sub-Processor Personal Data Breach Scenario



Sectoral Regulations

Other cybersecurity incident reporting obligations may apply as a result of specific sectoral regulations. For example, in the case of financial services sector i.e. Central Bank of Nigeria's (**CBN**) licensees, the CBN's Cybersecurity Risk-Based Frameworks requires such organisations to ***promptly, and not later than 24 hours upon detection of such incident,*** report all cyber incidents to the Director of Banking Supervision of the CBN.[10] These reports are to be made using the template prescribed by the CBN. Therefore, organisations are to take note of the sectoral regulations applicable to their operations in designing a comprehensive incident response plan.

Conclusion

Technology, being part of the essential infrastructure for the delivery of products and services, means the prominence of cybersecurity threats/incident remains an inevitable reality that must be properly navigated to manage its attendant consequences. In light of these, organisations are encouraged to put in place incident response plans or reassess subsisting incident response plans to ensure that adequate measures are in place to trigger the required notifications as and when due.

Aluko & Oyebode is a full-service law firm with expertise in cybersecurity, technology, and privacy. For more information, kindly reach out to us at tmtpraticegroup@aluko-oyebode.com.

[10] Section 1.3 Paragraph (g) CBN Cybersecurity Risk-Based Framework for DMB and PSPs 2024, Section 7.6 CBN Cybersecurity Risk-Based Framework for Other Financial Institutions 2022

Key Contacts

Sumbo Akintola
Partner
Lagos, Nigeria
Sumbo.Akintola@aluko-oyebode.com

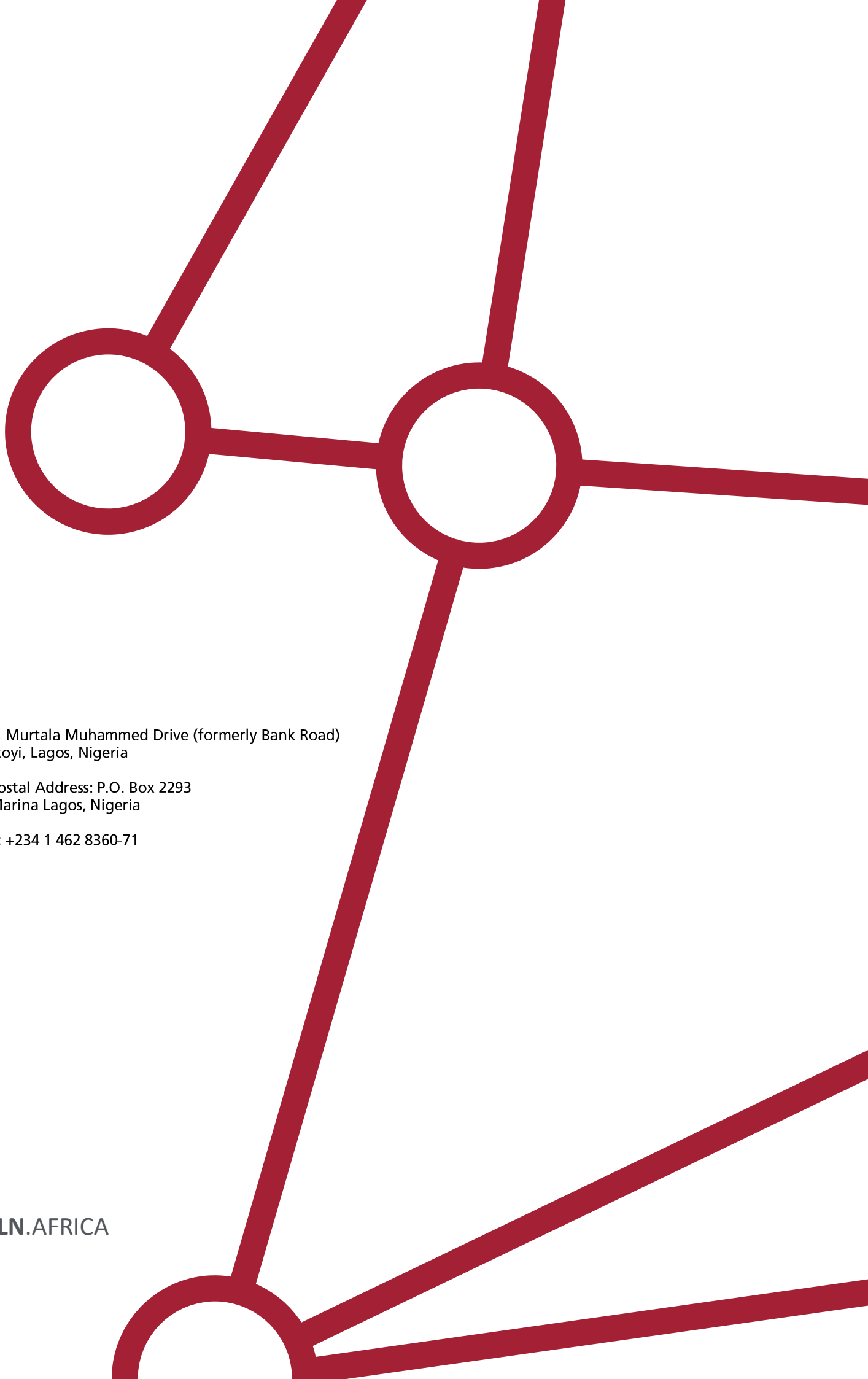
Timothy Ogele
Senior Associate
Lagos, Nigeria
Timothy.Ogele@aluko-oyebode.com
+234 913 937 0642

Yetunde Olashore
Associate
Lagos, Nigeria
Yetunde.Olashore@aluko-oyebode.com
+234 916 998 5150

1, Murtala Muhammed Drive (formerly Bank Road)
Ikoyi, Lagos, Nigeria

Postal Address: P.O. Box 2293
Marina Lagos, Nigeria

T: +234 1 462 8360-71



ALN.AFRICA