

**NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY (NITDA)**



**DRAFT ELECTRONIC COMMERCE REGULATION**

**2019**

**CONTENTS**

**FORWARD** ..... 3

**1.0 PART ONE** ..... 4

**1.1 Preamble** ..... 4

**1.2 Authority** ..... 4

**1.3 Application**..... 4

**1.4 Definition Of Terms**..... 4

**2.0 PART TWO: REGULATIONS** ..... 6

**2.2 Security** ..... 6

**2.3 Cybercrime Policy**..... 7

**2.4 Platform Information Requirement**..... 8

**3.0 PART THREE: ADVERTISEMENT AND FAIR USE POLICY REQUIREMENT** 10

**3.1 Requirements for Fair Business Practises**..... 10

**4.0 PART FOUR: ENFORCMENT AND VIOLATIONS**..... 10

**4.1 Violations** ..... 10

**4.2 Enforcements and Penalties** ..... 10

**4.3 Compliance Requirements** ..... 11

## **FORWARD**

E-commerce in Nigeria has recorded immense growth and acceptability as a viable method of trade and exchange of goods and services. Leading players in the space have made significant turnover in their operations in Nigeria. Other platforms have emerged offering products and services spanning retail of consumer electronics, fashion, home appliances, books, hoteling and leisure, children's items and personal care products, phones, electronics (including computers) and food.

With 146 million mobile phone users and 103 million internet subscribers, Nigeria is no doubt a significant market for e-commerce and digital trade. In spite of the slow pace of broadband penetration and other challenges which include; low cost intra-state courier infrastructure, insecurity, challenging electricity supply etc., e-commerce has continued to thrive and take root. Deepening smartphone usage and data consumption has catalysed demand for digital services and products in Nigeria. Currently, Nigeria's e-commerce market is estimated to be valued at about USD \$13 billion driven largely by a thriving Financial Technology (Fintech) eco-system.

These positives as highlighted which include the growth of fintech and ubiquity of mobile technology in Nigeria are unfortunately counterbalanced with other negative factors that have dogged further growth in the last few years. The Phillips Consulting Online Survey indicate that 52% of respondent who have used e-commerce channels have experienced challenges shopping online, these portends a disturbing trend that needs to be addressed. We are also witnessing a significant slowdown of e-commerce growth in other cities outside the central commercial hubs in Nigeria. Some reasons include infrastructural factors, but also critical are unmemorable experiences of customers who have used e-commerce channels in Nigeria. Furthermore, reports released by the Nigeria Electronic Fraud Forum indicate that e-payments fraud totalling losses of N5.571 billion have been committed in Nigeria in the last three years. These numbers point to an increasing sophistication of fraudsters and the need for continuous improvement of security of payment infrastructure across all sectors.

These alarming developments create the need to set benchmarks for quality customer service support, standardization of e-commerce platforms, delivery channels and to ensure the right infrastructure is utilized by vendors to protect the identity and financial information of customers. The Guidelines and standards in this regulatory document provide minimum stipulations and requirements for e-commerce platform operators in Nigeria. The regulation also provides compliance mechanisms to ensure Nigerians continue to have confidence in e-commerce as a veritable means of trade and as an economic enabler in Nigeria.

**Dr Isa Ali Ibrahim (Pantami), FNCS, FBCS, FIIM, MCPN**  
Director General/CEO

## 1.0 PART ONE

### 1.1 PREAMBLE

#### Whereas;

- a. The National Information Technology Development Agency (NITDA) is established by the NITDA Act of 2007 and mandated to create a frame work for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of Information Technology practices, activities and systems in Nigeria and all matters related thereto.
- b. NITDA's role in developing electronic commerce is to ensure that the digital platforms for the delivery of electronic commerce services meet minimum specifications that can assure customer satisfaction, economic growth, data protection and growth of medium and small-scale enterprises in Nigeria.

### 1.2 Authority

NITDA is empowered under Section 6(c) to develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields; where the use of electronic communication may improve the exchange of data and information.

### 1.3 Application

1. This regulation shall apply to enterprises which are engaged in the dissemination and exchange of digital data, electronic funds transfers, electronic stock exchange activities, commercial auctions, co-operative design and engineering, electronic bidding, direct consumer sales and after-sale services.
2. This regulation also applies to organizations who use digital platforms to wholly or partly sell goods (consumer goods or industrial products), deliver services (informational, financial, legal and other services) or create digital products and services such as books, periodicals, compact discs, software, banking services, television or radio programs, etc.

### 1.4 Definition of Terms

In this Regulation, unless the context otherwise requires:

**“Customer Terminal Equipment”** means a device that constitutes a point of termination of a communications circuit or channel domiciled or operated by a customer of the Vendor or Merchant. Terminal equipment includes all customer premises equipment (CPE), including voice terminal equipment and data terminal equipment (DTE).

**“Data Security Procedures”** means protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites.

**“Merchant”** means a registered business name or company engaged in the business of selling goods through a VENDOR

**“Nigerian Data Protection Guidelines”** means the Guidelines on data protection issued by the National Information Technology Development Agency (NITDA) currently in force in Nigeria

**“Payment Card Industry Data Security Standards (PCI DSS)”** means information security standard for organizations that handle branded credit cards from the major card schemes. The PCI Standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council.

**“Personally Identifiable Information (PII)”** means any data that could potentially be used to identify a particular person. Examples include a full name, National Identification number, driver’s license number, bank account number, passport number, and email address.

**“Privacy Policy”** means a statement or a legal document that discloses some or all of the ways a party gathers, uses, discloses, and manages a customer or client's data. It fulfils a legal requirement to protect a customer or client's privacy.

**“Secure Sockets Layer (SSL)”** means the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.

**“Vendor”** means organisations or business engaged in the sale of goods and services through electronic platforms generally referred to as e-commerce channels

## **2.0 PART TWO: REGULATIONS**

### **2.1 Processing of Personal Data**

- 1) E-Commerce businesses or platforms (hereinafter referred to as Vendors) that control, collect, store and process personal data or Personally Identifiable Information (OII) of Nigerian Residents and Citizens within and outside Nigeria shall be subject to Nigerian Data Protection Guidelines, 2019; all laws and international instruments binding on Nigeria with regards to electronic commerce.
- 2) Vendors shall publish a Privacy Policy which shall state the following
  - a. types of data collected;
  - b. purpose of collection;
  - c. what constitutes consent by the customer;
  - d. how data is used, how data is shared, confidentiality rights, any limitation of liability and any other information as may be directed from time to time by NITDA or by Acts of the National Assembly.
- 3) Vendors shall avail customers the opportunities to easily opt-in or opt-out of recurring promotions, adverts or service types.
- 4) Vendors shall comply with cyber security measures that protects the system from hacking, securely stores data, compliant with relevant encryption methodologies etc.
- 5) Vendors shall not collect personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life except
  - a. Explicit consent has been given
  - b. Any other grounds allowable by the provision of an Act of the National Assembly or a regulation issued pursuant to an Act.
- 6) Vendors shall implement technical and organizational measures to secure Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network.

### **2.2 Platform Security**

- 1) Vendors must in addition to compliance with the Central Bank of Nigeria's (CBN) directives comply with the following-
  - a. comply with Payment Card Industry Data Security Standards (PCIDSS) or any equivalent or higher standards approved for adoption in Nigeria.
  - b. must in addition to a Privacy Policy, publish a link about their information security processes and controls. The Vendor shall inform the consumer how their Personally Identifiable Information (PII) is secured during data transmission, on the website's server and at physical locations.

- c. publish a link to their Data Security procedures on the home page of their website and shall also provide detailed information on consumer data management principles and processes.
  - d. ensure its websites and linked third-party websites are Secure Sockets Layer (SSL) compliant.
  - e. ensure its website incorporates information encryption capabilities that offer reliable protection from unauthorized access and provide cardholders with the safest way to shop online.
- 2) The Vendor is responsible for seamless and efficient integration with third party websites and applications in the provision of service to customers. The Vendors shall make its integration specifications open or available on request to third party service providers.
- 3) When integrating with third party applications, the Vendors shall conduct its own acceptance testing in order to verify that the integration of its website or mobile application complies with minimum security and business process requirements necessary for the secure and efficient delivery of the service to customers.
- 4) Vendor shall be responsible for the security of cardholder data that it or its sub-contractors or agents possess, store, process or transmit and to the extent that the Vendor, its sub-contractors or agents could impact the security of the Vendor's cardholder data environment and the Vendor shall indemnify Customers against all losses, damages, penalties, fines and costs which the Customer may incur which is as a result of a failure by the Vendor, its sub-contractors or agents to comply with any of the requirements contained in the PCI DSS requirements such as, a breach of security of the cardholder data which the Vendor, its sub-contractors or agents possess, store, process or transmit on behalf of the Vendor which breach arises from any act or omission of the Vendor or that of its sub-contractors or agents.
- 5) The Vendor shall comply with any additional security, authentication, risk control or other requirements imposed by the industry, regulators or global best practices.
- 6) Vendor shall take measures to safeguard the security of their services, where applicable, in conjunction with other service providers in the value chain and inform customers of any potential or actual breach of the platform or network. The Vendor shall specify risks that are outside its scope of remediation and inform the Customer as quickly as possible.
- 7) Without prejudice to 3) the Vendor shall remain responsible to take measures to remedy any new, unforeseen security risk that could have impact on the Customer, whether or not, the Customer has been informed.

### **2.3 Cybercrime Policy**

- 1) The Vendor shall state in its terms and conditions, its compliance with the Nigerian Cybercrimes Act 2015 or its successor legislation.

- 2) Upon notification of an alleged breach of the Act or any criminal statute, the Vendor shall delete the said infringing information within 2 hours of notification from NITDA or Consumer Protection Council (CPC) and or immediately block the infringer from further use of the platform and write a report to the relevant security Agencies stating the technical and non-technical details including domain, email, internet exchange points etc.
- 3) Payment approval shall have multiple authentication process to reduce the incidence of fraud. The Vendor shall specify a transaction threshold upon which another authentication procedure shall be deployed.

#### **2.4 Platform Information Requirement**

- 1) Where the Vendor's efficient delivery of service is dependent on the availability of certain specifications in the Customer's Terminal Equipment, the Vendor shall state this explicitly using technical and non-technical language with visual illustration where possible.
- 2) Vendor Platforms must offer relevant but detailed information to the consumer about the products or services offered, provided such information is;
  - a. accurate, easily accessible and prominently displayed on all online platforms of the business;
  - b. describes the goods or services offered, in a manner which sufficiently enables consumers to make informed decision about purchase;
  - c. sufficient about the terms, conditions and costs associated with a transaction
- 3) Information displayed must include where applicable;
  - a. Value Added Tax and any other applicable taxes;
  - b. The terms and condition of product or service offered;
  - c. Warranties and/or guarantees on products and services offered;
  - d. Availability or otherwise of stock or specification on offer, this may include and not limited to size, colour, texture and so on.
  - e. Estimated timeframe for the delivery or conclusion of the transaction.
  - f. Terms of delivery or performance;
  - g. Terms, conditions and methods of payment;
  - h. Security or otherwise of available payment systems;
  - i. Restrictions, limitations or conditions of purchase, such as parental/guardian approval requirements, geographic or time restrictions;
  - j. Instructions for proper use including safety and health-care warnings;
  - k. Information relating to available after-sale service;
  - l. Details of and conditions related to withdrawal, termination, return, exchange, cancellation and/or refund policy information;
  - m. Available warranties and guarantees;
  - n. Applicable currency;
  - o. Applicable laws.
- 4) e-commerce Vendor platforms are further required to display the following prominently on their platforms:

- a. registered trademark and name of the platform;
- b. physical location of the administrative headquarters of the Vendor
- c. functional telephone number registered either in the trademark name of the platform on display or entity that owns the trademark;
- d. functional email address with “host specific URLs- preferably hosted with the platform”
- e. legal terms and conditions, buy or sell policy, legal limitations, privacy policy, return policy and other legal disclosures required.

## **2.5 Vendor and Merchants Customer Service Responsibility**

- 1) Vendor may not be responsible for quality and compliance with minimum Regulatory Standards of the products on display on their platform where product on display are to be supplied by a Merchant; however, Vendors shall:
  - a. verify the credibility of any merchant whose goods are displayed on platform to ascertain if merchant is a business concern;
  - b. demonstrate that steps have been taken to verify that products on display on their platforms meet Minimum Regulatory Standards to be sold in Nigeria;
  - c. ensure merchants put in place policy and systems for processing, reversal of payment and delivery of products in good condition.
- 2) Where Vendors are the Merchants, they shall be entirely liable for products and services displayed and offered to the public on their platforms. Vendors shall ensure products conform to all Minimum Regulatory Standards for sale of such products to the public.
- 3) Merchants shall be held solely responsible for any products or service offered to the public that is injurious to health, of poor quality and products that do not meet Minimum Regulatory Standards to be sold in Nigeria.
- 4) Notwithstanding article 2.5.1), Vendors shall;
  - a. ensure that products offered to public through their Platforms conform appropriately with the product information offered to the public and shall be entirely responsible to bear cost of fulfilment to replace such products.
  - b. replace products which do not conform to the description or information displayed on the channel at no cost to customer, and within reasonable time which shall not to exceed the length of the initial delivery time from the date of notice of rejection.
  - c. refund of the entire cost of the product is made to the customer through an electronic banking channel within 24 hours from when notice of non-conformity to product information as displayed on the platform is received from customer;
  - d. offer easy and simple payment channels to customer for reversal payment or refund of product;
  - e. not receive payment for products or services that are unavailable to consumers at the time of the purchase.
- l. bear responsibility for products in transit and shall replace product or refund consumer if product damaged in transit.

### **3.0 PART THREE: ADVERTISEMENT AND FAIR USE POLICY REQUIREMENT**

#### **3.1 Requirements for Fair Business Practice**

1) Vendors shall;

- a. have due regard to the interests of consumers and act in accordance with fair business, advertising, marketing and regulatory practices;
- b. ensure that platforms dealing with products or services that have legal age limitations, shall restrict unlawful access to their marketing and advertisement platforms;
- c. where applicable, ensure they obtain the necessary consent from parent/guardian in the case of underage/ dependents before sale of products where consent of a parent or guardian is specified or a requirement of any law;
- d. not make any representation, or omission, or engage in any practice that is likely to be deceptive, misleading, fraudulent or unfair;
- e. ensure that in promoting or marketing goods or services to consumers, they shall not engage in practices that are likely to cause unreasonable risk or harm to consumers;
- f. provide information about themselves or the goods or services they provide, in a clear, conspicuous, accurate and easily accessible manner;
- g. ensure that key terms and conditions associated with any offer must be in conspicuous areas of the website/platforms, and in clear legible and bold prints;
- h. stand by any representations made regarding policies or practices relating to their transactions with consumers;

### **4.0 PART FOUR: COMPLIANCE, ENFORCMENT AND VIOLATIONS**

#### **4.1 Violations**

- a. Non-compliance with requirements of this Guideline shall be construed as a violation of the NITDA Act 2007;
- b. Breach of the Provisions of Article 2.5 shall constitute breach of contract between Vendor/Merchant and customer. This violation shall also be construed as a breach of the NITDA Act 2007.

#### **4.2 Enforcements and Penalties**

- a. This Guidelines shall be enforced by NITDA, Standards Organisation of Nigeria (SON), Federal Competition and Consumer Protection Commission (FCCPC) or any Agency of Government empowered by law to compel compliance with the subject matter of this Regulation.
- b. Where Vendor's Planform do not confirm to any of the requirements of the following; Platform Security Requirement, Cybercrime Policy Requirement, Platform Information Requirement and Advertising and Fair Use Policy Requirement, a "TAKE DOWN" notice shall be issued by NITDA requiring

Vendor to take down the platform save for compliance within 24 hours from receipt of notice.

- c. Violation of this Guideline shall attract a fine of N500,000 in the first instance, N1, 500,000 in the second instance and all subsequent violations shall attract criminal prosecution as provided in Section 18.1 of the NITDA Act 2007.

#### **4.3 Compliance Requirements**

- a. All vendor platforms operating in Nigeria must complete and return a “Compliance with Vendor Platform Requirement Form” to NITDA within 45 days of every new year.
- b. Failure to submit form within the specified days will attract a Take Down Notice from NITDA.

**This Instrument was signed This 25th Day of January 2019**

.....  
**Dr Isa Ali Ibrahim (Pantami) FNCS, FBCS, FIIM**

Director General

National Information Technology Development Agency (NITDA)