CYBERCRIMES

(PROHIBITION, PREVENTION, ETC) ACT, 2015

WITH AMENDMENT ACT 2024

NOT TO BE SOLD

TABLE OF CONTENTS

Cybercrimes (Prohibition, Prevention, etc) Act, 2015 ..... 3 - 48

Cybercrimes (Prohibition, Prevention, etc) (Amendment) Act, 2024 .... 49- 55

Federal Republic of Nigeria
Official Gazette

No. 82 **Lagos - 18th May, 2015** **Vol. 102**

Government Notice No. 162

The following is published as supplement to this *Gazette* :

Act No.	*Short Title*	*Page*
17	Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.	A617-660

Printed and Published by The Federal Government Printer. Lagos. Nigeria
FGP 66/82016/2.200

Annual Subscription from 1st January, 2016 is Local : ₦25,000.00 Overseas : ₦37,500.00 [Surface Mail] ₦49,500.00 [Second Class Air Mail]. Present issue ₦2,500 per copy. Subscribers who wish to obtain *Gazette* after 1st January should apply to the Federal Government Printer, Lagos for amended Subscriptions.

CYBERCRIMES (PROHIBITION, PREVENTION, ETC.) ACT, 2015

ARRANGEMENT OF SECTIONS

Section :

PART I—OBJECT AND APPLICATION

1. Objectives.
2. Application.

PART II—PROTECTION OF CRITICAL NATIONAL INFORMATION STRUCTURE

3. Designation of certain Computer Systems or Networks as Critical National Information Infrastructure.
4. Audit and Inspection of Critical National Information Infrastructure.

PART III—OFFENCES AND PENALTIES

5. Offences against Critical National Information Infrastructure.
6. Unlawful Access to a Computer.
7. Registration of Cybercafe.
8. System Interference.
9. Intercepting Electronic Messages. Emails, Electronic Money Transfers.
10. Tampering with Critical Infrastructure.
11. Willful Misdirection of Electronic Messages.
12. Unlawful Interceptions.
13. Computer Related Forgery.
14. Computer Related Fraud
15. Theft of Electronic Devices
16. Unauthorized Modification of Computer Systems. Network data and System Interference.
17. Electronic Signature.
18. Cyber Terrorism.
19. Exceptions to Financial Institutions posting and authorised options.
20. Fraudulent Issuance of e-instructions.
21. Reporting of Cyber threats.
22. Identity Theft and Impersonation.
23. Child Pornography and related offences.
24. Cyberstalking.

CYBERCRIMES (PROHIBITION, PREVENTION, ETC.) ACT, 2015

Act No. 17

AN ACT TO PROVIDE FOR THE PROHIBITION, PREVENTION, DETECTION, RESPONSE, INVESTIGATION AND PROSECUTION OF CYBERCRIMES : AND FOR OTHER RELATED MATTERS.

[15*th day of May*, 2015] Commencement.

ENACTED by the National Assembly of the Federal Republic of Nigeria :

PART I—OBJECT AND APPLICATION

Objectives.

1. The objectives of this Act are to—

(*a*) provide an effective and unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria ;

(*b*) ensure the protection of critical national information infrastructure ; and

(*c*) promote cyber security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

Application.

2. The provisions of this Act shall apply throughout the Federal Republic of Nigeria.

PART II—PROTECTION OF CRITICAL NATIONAL INFORMATION INFRASTRUCTURE

Designation of certain Computer Systems or Networks as Critical National Information Infrastructure.

3.—(1) The President may, on the recommendation of the National Security Adviser by Order published in the Federal *Gazette*, designate certain Computer Systems or Networks, whether Physical or Virtual. the Computer Programs, Computer Data or Traffic Data Vital to this Country that the incapacity or destruction of or interference with such Systems and Assets would have a debilitating impact on Security, National or Economic Security, National Public Health and Safety, or any Combination of those matters as constituting Critical National Information Infrastructure.

The Presidential Order made under sub-section (1) of this Section may prescribe Minimum Standards, Guidelines, Rules or Procedure in respect of—

(*a*) protection or preservation critical information infrastructure ;

(*b*) the general management of critical information infrastructure ;

(*c*) access to, transfer and control of data in any critical information infrastructure ;

(*d*) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any designated critical national information infrastructure ;

(*e*) the storage or archiving of data or information designated as critical national information infrastructure ;

(*f*) recovery plans in the event of disaster, breach or loss of the critical national information infrastructure or any part of it ; and

(*g*) any other matter required for the adequate protection, management and control of data and other resources in any critical national information infrastructure.

Audit and inspection of critical national information infrastructure.

4. The Presidential Order made under Section 3 of this Act may require the Office of the National Security Adviser to audit and inspect any critical national information infrastructure at any time to ensure compliance with the provisions of this Act.

PART III—OFFENCES AND PENALTIES

Offences against Critical National Information Infrastructure.

5.—(1) A person who, with intent, commits any offence punishable under this Act against any critical national information infrastructure, designated under section 3 of this Act, is liable on conviction to imprisonment for a term of not more than 10 years without option of fine.

(2) Where the offence committed under sub-section (1) of this section results in grievous bodily harm to any person, the offender is liable on conviction to imprisonment for a term of not more than 15 years without option of fine.

(3) Where the offence committed under sub-section (1) of this section results in the death of a person, the offender is liable on conviction to life imprisonment.

Unlawful Access to a Computer.

6.—(1) A Person, who, without authorisation, intentionally accesses, in whole or in part, a Computer System or Network for fraudulent purposes and obtains data that are vital to National Security, commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦5,000,000.00 or both.

(2) Where the offence provided in sub-section (1) of this Section is committed with the intent of obtaining Computer Data, securing access to any Program, Commercial or Industrial secrets or classified information, the punishment shall be imprisonment for a term of not more than 7 years or a fine of not more than ₦7, 000,000.00 or both.

(3) A Person who, with the intent to commit an offence under this section, uses any device to avoid detection or otherwise prevent identification or attribution with the act or omission, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or to a fine of not more than ₦7,000,000.00 or both such.

(4) A Person or Organisation who knowingly and intentionally trafficks in any password or similar information through which a Computer may be accessed without lawful authority, if such trafficking affects Public, Private or Individual interest within or outside the Federation of Nigeria, commits an offence and is liable on conviction to a fine of not more than ₦7, 000,000.00 or imprisonment for a term of not more than 3 years or both.

Registration of Cybercafé.

7.—(1) From the commencement of this Act, all Operators of a Cybercafe shall—

(*a*) register as a business concern with Computer Professionals' Registration Council in addition to a business name registration with the Corporate Affairs Commission ; and

(*b*) maintain a register of users through a sign-in register and the register shall be available to law enforcement personnel whenever needed.

(2) A Person who perpetrates Electronic or Online Fraud using a Cybercafé, commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1,000,000.00 or both.

(3) In the event of proven connivance by the owners of the Cybercafe, such owners are guilty of an offence and are liable to a fine of ₦2,000,000.00 or imprisonment for a term of 3 years or both.

(4) The burden of proving connivance in sub-section 3 of this Section shall be on the prosecutor.

System Interference.

8. A Person who, without Lawful Authority, Intentionally or for fraudulent purposes does an act which causes directly or indirectly the serious hindering of the functioning of a Computer System by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing Computer Data or any other form of interference with the Computer System, which prevents the Computer System or any part thereof, from functioning in accordance with its intended purpose, commits an offence and is liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than ₦5,000,000.00 or both.

Intercepting Electornic messages. e-mails and Electronic Money Transfer.

9. A person who unlawfully destroys or aborts any electronic mail or process through which money or valuable information is being conveyed, commits an offence and is liable on conviction to a term of imprisonment for 7 years in the first instance and, upon second conviction, is liable to 14 years imprisonment.

Tampering with Critical Infrastructure.

10. From the commencement of this Act, any Person being employed by or under a Local Government of Nigeria, Private Organization or Financial Institution with respect to working with any critical infrastructure or electronic mail, commits any act which he is not authorized to do by virtue of his contract of service or intentionally permits, tampering with such Computer, commits an offence and is liable on conviction to a fine of ₦2,000,000.00 or imprisonment for 3 years.

Willful Misdirection of Electronic Messages.

11. A person who misdirects electronic messages with either the intention to fraudulently obtain financial gain as a result of such act or with the intention of obstructing the process in order to cause delay or speeding the messages with a view to cause an omission or commission that may defeat the essence of such messages, commits an offence and is liable on conviction to a term of imprisonment for 3 years or a fine of ₦1,000,000.00 or both.

Unlawful Interceptions.

12.—(1) A person, who intentionally and without authorization, intercepts by technical means, non-public transmissions of Computer Data, content, or traffic data, including electromagnetic emissions or signals from a Computer, Computer System or Network carrying or emitting signals, to or from a Computer, Computer System or connected system or network, commits an offence and is liable on conviction to a term of imprisonment of not more than 2 years or to a fine of not more than ₦5,000,000.00 or both.

(2) A person or organization who, by means of false pretense, induces any person employed by or under the Federal, State or Local Government of Nigeria or any person in charge of Electronic Devices to deliver to him any electronic message which includes e-mail, credit and debit cards information, facsimile messages which is not specifically meant for him or his organization (in the latter case except he is authorised to receive such messages for and on behalf of his organization), commits an offence and is liable on conviction to a term of imprisonment for 2 years or a fine of not more than ₦1,000,000.00 or both.

(3) A person who, being employed by or under the authorities of the Local, State or Federal Government of Nigeria or Private Organization who intentionally hides or detains any Electronic Mail, Message, Electronic Payment, Credit and Debit Card which was found by him or delivered to him in error

and which, to his knowledge, ought to be delivered to another person, commits an offence and is liable on conviction to imprisonment for a term of 1 year or a fine of ₦250,000.00 or both.

Computer related Forgery.

13. A person who knowingly accesses any Computer or Network and inputs, alters, deletes or suppresses any data resulting in inauthentic data with the intention that such inauthentic data will be considered or acted upon as if it were authentic or genuine, regardless of whether or not such data is directly readable or intelligible, commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than ₦7,000,000.00 or both.

Computer related Fraud.

14.—(1) A person who, knowingly and without authority or in excess of authority, causes any loss of property to another by altering, erasing, inputting or suppressing any data held in any Computer, whether or not for the purpose of conferring any economic benefits on himself or another person, commits an offence and is liable on conviction to imprisonment for a term of not less than 3 years or to a fine of not less than ₦7,000,000.00 or both.

(2) A person who, with intent to defraud, sends electronic message materially misrepresents any fact or set of facts upon which reliance the recipient or another person is caused to suffer any damage or loss, commits an offence and is liable on conviction to imprisonment for a term of not less than 5 years and to a fine of not less than ₦10,000,000.00 or both.

(3) A person who with intent to defraud, franks electronic messages, instructions, superscribes any electronic message or instruction, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦5,000,000.00 or both.

(4) A person employed in the Public or Private Sector who, with intent to defraud, manipulates a Computer or other Electronic Payment Devices with the intent to short pay or over pay or actually short pays or over pays any employee of the Public or Private Sector, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years and shall forfeit the proprietary interest in the stolen Money or Property to the Bank Financial Institution or the Customer.

(5) A person employed by or under the Authority of any Bank or other Financial Institution who, with intent to defraud, directly or indirectly diverts Electronic Mails, commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or a fine of not more than ₦7,000,000.00 or both.

(6) A Person who commits an offence Under Subsection (4) of this Section, which results in Material or Financial loss to the Bank, Financial Institution or Customer, shall, in addition to 7 years imprisonment, be liable to refund the stolen money or forfeit any property to which it has been converted to the Bank, Financial Institution or the Customer.

(7) An Employee of a Financial Institution found to have connived with another Person or Group of Persons to perpetrate fraud using Computer Systems or Network, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years and shall in addition, refund the stolen Money or Forfeit any Property to which it has been converted to the Bank, Financial Institution or the Customer.

Theft of Electronic Devices.

15.—(1) A Person who steals a Financial Institution or Public Infrastructure Terminal commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1,000,000.00 or both.

(2) A person steals an Automated Teller Machine (ATM) commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦10,000,000.00 or both and all proceeds of such theft shall be forfeited to the lawful owners of the ATM.

(3) A person who attempts to steal an ATM, commits an offence and is liable on conviction to imprisonment for a term of not more than 1 year or a fine of not more ₦1,000,000.00 or both.

Unauthorised Modification of Computer Systems. Network Data and System Interference.

16.—(1) A Person who, with intent and without lawful authority, directly or indirectly modifies or causes modification of any data held in any Computer System or Network, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦7,000,000.00 or both.

(2) For the purpose of this section, a modification of any data held in any Computer System or Network includes modifications that take place whereby the operation of any function of the Computer System or Network concerned, or any—

(*a*) program or data held in it is altered or erased ;

(*b*) program or data is added to or removed from any program or data held in it ;

(*c*) program or data is suppressed to prevent or terminate the availability of the data or function to its authorised users ; or

(*d*) act occurs which impairs the normal operation of any computer, computer system or network concerned.

(3) A Person who, without lawful authority, intentionally does an act which causes directly or indirectly the serious hindering of the functioning of a Computer System by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or any other form of interference with the Computer System, which prevents the Computer System or any part thereof, from functioning in accordance with its intended purpose, commits an offence and is liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than ₦5,000,000.00 or both.

Electronic Signature.

17.—(1) Electronic Signature in respect of purchases of goods, and any other transactions shall be binding.

(2) Whenever the genuiness or otherwise of such signature is in question, the burden of proof, that the signature does not belong to the purported originator of such Electronic Signature shall be on the contender.

(3) A Person who, with the intent to defraud or misrepresent, forges through Electronic Devices another Person's Signature or Company's Mandate, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦10,000,000.00 or both.

(4) The following transactions shall be excluded from the categories of contractual transactions or declarations that are valid by virtue of Electronic Signature :

(*a*) creation and execution of wills, codicils and other testamentary documents ;

(*b*) death certificate ;

(*c*) birth certificate ;

(*d*) matters of family law such as marriage, divorce, adoption and other related issues ;

(*e*) issuance of court orders, notices, official court documents such as affidavits, pleadings, motions and other related judicial documents and instruments ;

(*f*) a cancellation or termination of utility services ;

(*g*) an instrument required to accompany any transportation or handling of dangerous materials either solid or liquid in nature ; and

(*h*) any document ordering withdrawal of drugs, chemicals and any other material either on the ground that such items are fake, dangerous to the people or the environment or expired by any authority empowered to issue orders for withdrawal of such items.

Cyber Terrorism.

18.—(1) A Person who accesses or causes to be accessed any Computer or Computer System or Network for purposes of terrorism, commits an offence and is liable on conviction to life imprisonment.

(2) For the purpose of this section, "*terrorism*" shall have the same meaning under the Terrorism (Prevention) Act, 2011, as amended.

Exceptions to Financial Institutions. posting and authorized options.

19.—(1) From the commencement of this Act, no Financial Institution shall give posting and authorising access to any single employee.

(2) A Person or Persons authorised to give access to Computer to employees and gives more than one access to any person or persons commits an offense and is liable on conviction to a fine of ₦1,000,000.00 or 7 years imprisonment or both.

(3) Financial Institutions shall, as a duty to their customers, put in place effective counter-fraud measures to safeguard their sensitive information, where a security breach occurs the proof of negligence lies on the customer to prove the Financial Institution in question could have done more to safeguard its information integrity.

Fraudulent Issuance of E-Instructions.

20. A Person being authorised by any Financial Institution and charged with the responsibility of using Computer or other Electronic Devices for Financial Transactions such as posting of debit and credit, issuance of Electronic Instructions as they relate to sending of Electronic Debit and Credit messages or charged with the duty of confirmation of Electronic Fund Transfer, unlawfully with the intent to defraud, issues false Electronic or Verbal Messages commits an offence and is liable on conviction to imprisonment for a term of 7 years.

Reporting of Cyber threats.

21.—(1) A Person or Institution who operates a Computer System or a Network, whether Public or Private, shall immediately inform the National Computer Emergency Response Team (CERT) Co-ordination Center of any attack, intrusion and other disruption liable to hinder the functioning of another Computer System or Network, so that the National Computer Emergency Response Team Co-ordination Center can take the necessary measures to tackle the issues.

(2) In such cases mentioned in sub-section (1) of this section, and in order to protect Computer Systems and Networks, the National CERT Co-ordination Center may propose the isolation of affected Computer Systems or Network pending the resolution of the issues.

(3) A Person or Institution who fails to report any such incident to the National CERT within 7 days of its occurrence, commits an offence and is liable to denial of Internet Services, and such Persons or Institution shall, in addition, pay a mandatory fine of ₦2,000,000.00 into the National Cyber Security Fund.

Indetity theft and Impersonation.

22.—(1) A Person who is engaged in the services of any Financial Institution and, as a result of his special knowledge, commits identity theft of its Employer, Staff, Service Providers and Consultants with the intent to defraud commits an offence and is liable on conviction to imprisonment for a term of 7 years or a fine of ₦5,000,000.00 or both.

(2) A person who—

(*a*) fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person ; or

(*b*) fraudulently impersonates another entity or person, living or dead, with intent to—

(*i*) gain advantage for himself or another person ;

(*ii*) obtain any property or an interest in any property ;

(*iii*) cause disadvantage to the entity or person being impersonated or another person ; or

(*iv*) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice, commits an offence and is liable on conviction to imprisonment for a term of 5 years or a fine of not more than N7,000,000.00 or both.

(3) A Person who makes or causes to be made, either directly or indirectly, any false statement as to a material fact in writing, knowing it to be false and with intent that it be relied upon respecting his identity or that of any other Person or his Financial condition or that of any other Person for the purpose of procuring the issuance of a card or other instrument to himself or another person, commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or a fine of not more than N7,000,000.00 or both.

Child Pornography and related Offences.

23.—(1) A Person who intentionally uses any Computer System or Network in or for—

(*a*) producing child pornography ;

(*b*) offering or making available child pornography ;

(*c*) distributing or transmitting child pornography ;

(*d*) procuring child pornography for oneself or for another person ;

(*e*) possessing child pornography in a computer system or on a computer-storage medium.

Commit offence under this Act and is liable on conviction—

(*i*) in the case of paragraphs (*a*), (*b*) and (*c*) of this sub-section, to imprisonment for a term of 10 years or fine of not more than ₦20,000,000.00 or both ; and

(*ii*) in the case of paragraphs (*d*) and (*e*) of this sub-section, to imprisonment for a term of not more than 5 years or a fine of not more than ₦10,000,000.00 or both.

(2) A Person who knowingly makes or sends other Pornographic images to another Computer by way of unsolicited distribution commits an offence and is liable on conviction to imprisomnent for a term of 1 year or a fine of ₦250,000.00 or both.

(3) A Person who Intentionally proposes Grooms or Solicits, through any Computer System or Network to meet a child for the purpose of :

(*a*) engaging in sexual activities with the child ;

(*b*) engaging in sexual activities with the child where—

(*i*) use is made of coercion, inducement, force or Threats ;

(*ii*) abuse is made of a recognized position of trust, authority or influence over the child, including within the family ; or

(*iii*) abuse is made of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence ;

(*c*) recruiting, inducing, coercing, exposing, or causing a child to participate in pornographic performances or profiting from or otherwise exploiting a child for such purposes ;

Commits an offence under this Act, and is liable on conviction—

(*i*) in the case of paragraph (*a*) of this subsection, to imprisonment for a term of not more than 10 years and a fine of not more than ₦15,000,000.00 ; and

(*ii*) in the case of paragraphs (*b*) and (*c*) of this subsection, to imprisonment for a term of not more than 15 years and a fine of not more than ₦25,000.000.00.

(4) For the purpose of sub-section (l) of this section, the term "*Child Pornography*" includes Pornographic Material that Visually depicts—

(*a*) a minor engaged in sexually explicit conduct ;

(*b*) a person appearing to be a minor engaged in sexually explicit conduct ; and

(*c*) realistic images representing a minor engaged in sexually explicit conduct.

(5) For the purpose of this Section, the term "*child*" or "*minor*" means a person below 18 years of age.

Cyberstalking.

24.—(1) A person who knowingly or intentionally sends a message or other matter by means of Computer Systems or Network that—

(*a*) is grossly offensive, pornographic or of an indecent obscene or menacing character or causes any such message or matter to be so sent ; or

(*b*) he knows to be false, for the purpose of causing annoyance, inconvenience danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or causes such a message to be sent.

Commits an offence under this Act and is liable on conviction to a fine of not more than ₦7,000,000.00 or imprisonment for a term of not more than 3 years or both.

(2) A Person who knowingly or Intentionally Transmits or causes the Transmission of any communication through a Computer System or Network—

(*a*) to bully, threaten or harass another person, where such communication places another person in fear of death, violence or bodily harm to another person ;

(*b*) containing any threat to kidnap any person or any threat to harm the person of another, any demand or request for a ransom for the release of any kidnapped person, to extort from any person, firm, association or corporation, any money or other thing of value, or

(*c*) containing any threat to harm the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, to extort from any person, firm, association. or corporation, any money or other thing of value, commits an offence under this Act and is liable on conviction—

(*i*) in the case of paragraphs (*a*) and (*b*) of this sub-section, to imprisonment for a term of 10 years or a minimum fine of N25.000,000.00 ; and

(*ii*) in the case of paragraph (*c*) of this subsection, to imprisonment for a term of 5 years or a minimum fine of N15,000,000.00.

(3) A Court sentencing or otherwise dealing with a Person Convicted of an offence under subsections (1) and (2) may also make an order, which may, for the purpose of protecting the Victim or Victims of the offence, or any other Person mentioned in the order, from further conduct which—

(*a*) amounts to harassment ; or

(*b*) will cause fear of violence, death or bodily harm, prohibit the defendant from doing anything described or specified in the order.

(4) A defendant who does anything which he is prohibited from doing by an order under this section, commits an offence and is liable on conviction to a fine of not more than ₦10,000,000.00 or imprisonment for a term of not more than 3 years or both.

(5) The order made under subsection (3) of this section may have effect for a specified period or until further order, and the Defendant or any other Person mentioned in the order, may apply to the Court which made the order for it to be varied or discharged a further order.

(6) Notwithstanding the powers of the Court under subsections (3) and (5), the Court may make an interim order, for the protection of Victims from further exposure to the alleged offences.

Cybersquatting.

25.—(1) A Person who, Intentionally takes or makes use of a Name, Business Name, Trademark, domain name or other word or Phrase Registered, owned or in use by any Individual, Body Corporate or belonging to either the Federal, State or Local Government in Nigeria, on the Internet or any other Computer Network, without authority or right, and for the purpose of interfering with their use by the owner, registrant or legitimate prior user, commits an offence under this Act and is liable on conviction to imprisonment for a term of not more than 2 years or a fine of not more than ₦5,000,000.00 or both.

(2) In awarding any penalty against an Offender under this section, a Court shall have regard to—

(*a*) a refusal by the offender to relinquish, upon formal request by the rightful owner of the name, business name, trademark, domain name. or other word or phrase registered, owned or in use by any individual, corporate or belonging to either the Federal, State or Local Government in Nigeria ; or

(*b*) an attempt by the offender to obtain compensation in any form for the release to the rightful owner for use the name, business name, trademark, domain name or other word or phrase registered, owned or in use by any individual, body corporate or belonging to either the Federal, State or Local Government of Nigeria.

(3) In addition to the Penalty specified under this section, the Court may make an order directing the offender to relinquish such Registered Name, Mark, Trademark ; Domain Name, or other word or phrase to the rightful owner.

Racist and Xenophobic Offences.

26.—(1) A Person who with intent—

(*a*) distributes or otherwise makes available, any racist or xenophobic material to the public through a computer system or network ;

(*b*) threatens through a computer system or network—

(*i*) persons for the reason that they belong to a group distinguished by race, colour, descent, national of ethnic origin, as well as, religion, if used as a pretext for any of these factors ; or

(*ii*) a group of persons which is distinguished by any of these characteristics ;

(*c*) insults publicly through a computer system or network—

(*i*) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors ; or

(*ii*) a group of persons which is distinguished by any of these characteristics ; or

(*d*) distributes or otherwise makes available, through a computer system or network, to the public, material which denies or approves or justifies acts constituting genocide or crimes against humanity, commits all offence and is liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦10,000,000.00 or both, fine and imprisonment.

(2) For the purpose of subsection (1) of this section, the term "*crime against humanity*" includes any of the following acts committed as part of a widespread or systematic attack directed against any Civilian Population, with knowledge of the attack : murders, extermination, enslavement, deportation or forcible transfer of population, imprisonment torture, rape, sexual slavery, enforced prostitution, forced pregnancy, enforced sterilization or any other form of sexual violence of comparable gravity, persecution against an identifiable group on political, racial, national, ethnic, cultural, religious or gender grounds, enforced disappearance of persons, the crime of apartheid, other inhumane acts of similar character intentionally causing great suffering or serious bodily or mental injury.

"*Genocide*" means any of the following acts committed with intent to destroy in whole or in part, a national, ethnic, racial or religious group as such : killing members of the group, deliberately inflicting on the group conditions of life calculated to bring about its physical destruction in whole or in part ; imposing measures intended to prevent births within the group ; forcibly transferring children of the group to another group.

"*Racist or Xenophobic Material*" means any written or printed material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual group of individuals, based on race, color descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

Attempt Conspiracy. Aiding and Abetting.

27.—(1) A person who—

(*a*) attempts to commit any offence under this Act ; or

(*b*) aids, abets, conspires, counsels or procures another person to commit any offence under this Act,

Commits an offence and is liable on conviction to the punishment provided for the principal offence under this Act.

(2) An employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using a computer system or network, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years and shall in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer.

Importation and Fabrication of E-tools.

28.—(1) A Person who unlawfully produces, supplies, adapts, manipulates or procures for use, imports, exports, distributes, offers for sale or otherwise makes available—

(*a*) any device, including a computer program or a component designed or adapted for the purpose of committing an offence under this Act,

(*b*) a computer password, access code or similar data by which the whole or any part of a computer system or network is capable of being accessed for the purpose of committing an offence under this Act ; or

(*c*) any device, including a computer program designed to overcome security measures in any computer system or network with the intent that the devices be utilized for the purpose of violating any provision of this Act, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦7,000,000.00 or both.

(2) A Person who, with intent to commit an offence under this Act, has in his possession any device or program referred to in subsection (1) of this section, commits an offence and is liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than ₦5,000,000.00 or both.

(3) A Person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any Computer or Network for any unlawful purpose or gain, commits an offence and is liable on conviction to imprisonment for a term of not more than 2 years or to a fine of not more than ₦5,000,000.00 or both.

(4) Where the offence under sub-section (1) of this section results in loss or damage, the offender is liable to imprisonment for a term of not more than 5 years or to a fine of not more than ₦10,000,000.00 or both.

(5) A Person who, with intent to commit any offence under this Act uses any automated means or device or any computer program or software to retrieve, collect and store password, access code or any means of gaining access to any program, data or database held in any computer, commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦10,000,000.00 or to both fine and imprisonment.

(6) A Person who, without lawful authority or appropriate licence where required, with fraudulent intent, imports, transports or installs within the Federation of Nigeria any tool, implement, item used or designed to be used in making, forging, altering, or counterfeiting any electronic device, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦5,000,000.00 or both.

Breach of Confidence by Service Providers.

29.—(1) A Person or Organization who, being a Computer Based Service Provider or Vendor, does any act with intent to defraud and by virtue of his position as a service provider, forges, illegally used security codes of the consumer with the intent to gain any financial or material advantage or with intent to provide less value for money in his or its services to the consumer, if Corporate Organization, commits an offence and is liable on conviction to a fine of ₦5,000,000.00 and forfeiture of further equivalent of the monetary value of the loss sustained by the consumer.

(2) Where an offence under this Act which has been committed by a body corporate is proved to have been committed on the instigation or with the connivance of, or attributable to, any neglect on the part of a director, manager, secretary or other similar officer of the body corporate, or any officer purporting to act in any such capacity, he, as well as the body corporate, where practicable, are deemed to be guilty of that offence and are liable to be proceeded against and punished accordingly.

(3) Where a Body Corporate is convicted of an offence under this Act, the court may order that the Body Corporate shall, thereupon and without any further assurances, but for such order, be wound up and all its assets and property be forfeited to the Federal Government.

(4) If the offender is a natural person, he commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years and to a fine of not more than ₦5,000,000.00 or both.

(5) Nothing contained in this section shall render any person liable to any punishment, where he proves that the offence was committed without his knowledge or that he exercised all due diligence to prevent the commission of the offence.

Manipulation of ATM/POS Terminals.

30.—(1) A Person who manipulates an ATM Machine or Point of Sales Terminals with the intention to defraud commits an offence and is liable on conviction to imprisonment for a term of 5 years or ₦5,000,000.00 fine or both.

(2) An Employee of a Financial Institution found to have connived with another person or group of persons to perpetrate fraud using an ATM or Point of Sales Device, commits an offence and is liable on conviction to imprisonment for a term of 7 years without an option of fine.

Employees responsibility:

31.—(1) Without prejudice to any contractual agreement between the employer and the employee, all employees in both the Public and Private Sectors shall relinquish or surrender all codes and access rights to their employers immediately upon disengagement from their employment, and if such code or access right constitutes a threat or risk to the employer, it shall, unless there is any lawful reason to the contrary, be presumed that the refusal to relinquish or surrender such code or access right is intended to be used to hold such employer to ransom.

(2) An employee who, without any lawful reason, continues to hold unto the code or access right of his employer after disengagement without any lawful reason commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of ₦3,000,000.00 or both.

Phishing. Spamming. Spreading of Computer Virus.

32.—(1) A Person who knowingly or intentionally engages in computer phishing shall be liable on conviction to imprisonment for a term of 3 years or a fine of ₦1, 000,000.00 or both.

(2) A Person who engages in spamming with intent to disrupt the operations of a Computer, be it public or private or financial institutions, commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1,000,000.00 or both.

(3) A Person who, engages in malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in Public, Private or Financial Institution's Computers commits an offence and is liable on conviction to imprisonment for a term of 3 years or a fine of ₦1, 000,000.00 or both.

Electronic Cards Related Fraud.

33.—(1) A Person who, with intent to defraud, uses any access device including credit, debit, charge, loyalty and other types of financial cards, to obtain cash, credit, goods or service commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦5,000,000.00 or to both fine and imprisonment and is further liable to pay, in monetary terms, the value of loss sustained by the owner of the credit card.

(2) A Person who uses—

(*a*) a counterfeit access device ;

(*b*) an unauthorised access device ;

(*c*) an access device issued to another person.

resulting in a loss or gain, commits an offence and is liable on conviction to imprisonment for a term of not more than 7 years or a fine of not more than ₦5,000,000.00 and forfeiture of the advantage or value derived from his act.

(3) A Person who steals an Electronic Card commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1,000,000.00 and is further liable to repay in monetary terms the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.

(4) A Person who receives a card that he knows or ought to know to have been lost, mislaid, or delivered under a mistake as to the identity or address of the cardholder and who retains possession with the intent to use, sell, or to traffic it to a person other than the issuer or the cardholder, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1,000,000.00 and is further liable to pay, in monetary terms, the value of loss sustained by the cardholder.

(5) A person who, with intent to defraud the issuer, a creditor, or any other person, obtains control over a card as security for a debt, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦3,000,000.00 or both and is further liable to pay, in monetary terms the value of loss sustained by the card holder or forfeit the assets or goods acquired with the funds from the account of the cardholder.

(6) A Person, other than the cardholder or a person authorized by him, who, with the intent to defraud the issuer or a creditor, signs a card commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦1,000,000.00.

(7) A Person who, with intent to defraud the issuer or a creditor, uses, for the purpose of obtaining money, goods, services, or anything else of value, a card obtained or retained fraudulently or a card which he knows is forged or expired, or who obtains money, goods, services, or anything else of value by representing, without the consent or authorisation of the cardholder, that he is the holder of a specified card, or by representing that he is the holder of a card and such card has been validly issued, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years and a fine of not more than ₦1,000,000.00.

(8) A Creditor who, with intent to defraud the issuer or the cardholder, furnishes goods, services, or anything else of value upon presentation of a card which he knows is obtained or retained fraudulently or illegally or a card which he knows is forged, expired, or revoked commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦1,000,000.00 or to both fine and imprisonment.

(9) A Creditor who, with intent to defraud the issuer or the cardholder, fails to furnish goods, services, or anything of value which he represents in writing to the issuer or the cardholder that he has furnished, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦1,000,000.00 or both.

(10) A Person who is authorised by a creditor to furnish goods, services, or anything else of value upon presentation of a Card or Card Account Number by a cardholder, or any agent or employee of such person, who, with intent to defraud the issuer or the cardholder, presents to the issuer or the cardholder, for payment, a card transaction record of sale, which sale was not made by such person or his agent or employee, commits an offence and is liable on summary conviction to a fine of not more than ₦500,000 and to imprisonment for a term of 3 years.

(11) A Person who, without the Creditor's Authorisation, employs, solicits or otherwise causes a person who is authorised by the creditor to furnish goods, services or anything else of value upon presentation of card account number by the cardholder, or employs, solicits or otherwise causes an agent or employee, of such authorised person, to remit to the creditor a card transaction record of a sale that was not made by such authorised person or his agent or employee commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦1,000,000.00 or both.

(12) A Person who, with intent to defraud, possesses counterfeit cards, invoices, vouchers, sales drafts, or other representations or manifestations of counterfeit cards, or card account numbers of another person, commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦3,000,000.00 or both.

(13) A Person who receives, possesses, transfers, buys, sells, controls, or has custody of any card-making equipment with intent that such equipment be used in the manufacture of counterfeit cards commits an offence and is liable on conviction to imprisonment for a term of not more than 5 years or to a fine of not more than ₦7,000,000.00 or both.

(14) A Person who, with intent to defraud another person, falsely alters any invoice for money, goods, services, or anything else of value obtained by use of a card after that invoice has been signed by the cardholder or a person authorised by him, commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or to a fine of not more than ₦5,000,000.00 or both.

(15) An Institution that makes available, lends, donates, or sells any list or portion of a list of cardholders and their addresses and account numbers to any person without the prior written permission of the cardholders, commits an offence and is liable on conviction to a fine of ₦10.000,000.00.

(16) An Institution may make available to the Central Bank of Nigeria or a licensed Credit Bureau, which seeks to determine only the cardholders' rating, any list or portion of a list of any cardholder and their addresses without the permission of the cardholder, but shall, within 7 working days, give notice in writing of the disclosure to the cardholder and the institution which fails to comply with the requirement to notify the cardholder, commits an offence and is liable on conviction to a fine of not more than ₦1.000,000.00.

Dealing in Card of Another.

34. A Person, other than the issuer, who receives and retains possession of two or more cards issued in the name or names of different cardholders, which cards he knows were taken or retained under circumstances which constitute a card theft, commits an offence and is liable on summary conviction to imprisonment for a term of 3 years or to a fine of ₦1,000,000.00 and is further liable to repay, in monetary terms, the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.

Purchase or Sale of Card of Another.

35. A Person, other than an issuer or his authorised agent, who sells a card, or a person who buys a card from a person other than an issuer or his authorised agent, commits an offence and is liable on summary conviction to a fine of ₦500,000.00 and is further liable to pay, in monetary terms, the value of loss sustained by the card holder or forfeit the assets or goods acquired with the funds from the account of the cardholder.

Use of Fraudulent Device or attached E-mails and Websites.

36.—(1) A Person who, with intent to defraud, uses any device or attachment, e-mail or fraudulent website to obtain information or details of a cardholder, commits an offence and is liable on conviction to imprisonment for a term of 3 years or to a fine of ₦1,000,000.00 or both.

(2) A Person who fraudulently re-directs funds transfer instructions during transmissions over any authorised communications path or device and re-directs Funds Transferred Electronically with an Authorized Account, commits an offence and, is liable on conviction to imprisonment for a term of 3 years or

to a fine of ₦1,000,000.00 and is further liable to pay, in monetary terms, the value of loss sustained by the cardholder or forfeit the assets or goods acquired with the funds from the account of the cardholder.

PART IV—DUTIES OF FINANCIAL INSTITUTIONS

Duties of Financial Institutions.

37.—(1) A Financial Institution shall—

(*a*) verify the identity of its customers carrying out electronic financial transactions by requiring the customers to present documents bearing their names, addresses and other relevant information before issuance of ATM cards, credit cards, debit cards and other related electronic devices ; and

(*b*) apply the principle of know your customer in documentation of customers preceding execution of customers electronic transfer, payment, debit and issuance orders.

(2) An Official or Organization who fails to obtain proper identity of customers before executing Customer Electronic Instructions in whatever way, commits an offence and is liable on conviction to a fine of ₦5,000,000.00.

(3) A Financial Institution that makes an unauthorised debit on a customers account shall, upon written notification by the customer, provide clear legal authorisation for such debit to the customer or reverse such debit within 72 hours and any Financial Institution that fails to reverse such debit within 72 hours, commits an offence and is liable on conviction to restitution of the debit and a fine of ₦5,000,000.00.

Records Retention and Protection of Data.

38.—(1) A Service Provider shall keep all Traffic Data and Subscriber Information as may be prescribed by the relevant authority, for the time being, responsible for the regulation of communication services in Nigeria, for a period of 2 years.

(2) A Service Provider shall, at the request of the relevant authority referred to in subsection (1) of this section or any Law Enforcement Agency—

(*a*) preserve, hold or retain any traffic data, subscriber information, non-content information, and content data ; or

(*b*) release any information required to be kept under subsection (1) of this section.

(3) A Law Enforcement Agency may, through its authorised officer, request for the release of any information in respect of subsection (2) (*b*) of this section and it shall be the duty of the service provider to comply.

(4) A data retained, processed or retrieved by the service provider at the request of any Law Enforcement Agency under this Act shall not be utilized except for legitimate purposes as may be provided for under this Act, any other legislation, regulation or by an order of a court of competent jurisdiction.

(5) A person exercising any function under this section shall have due regard to the individual's right to privacy under the Constitution of the Federal Republic of Nigeria, 1999 and shall take appropriate measures to safeguard the confidentiality of the data retained, processed or retrieved for the purpose of law enforcement.

(6) Subject to the provisions of this Act, any person who contravenes any of the provisions of this section commits an offence and is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦7,000,000.00 or both.

Interception of Electronic Communication.

39. Where there are reasonable grounds to suspect that the content of any Electronic Communication is reasonably required for the purposes of a criminal investigation or proceeding, a Judge may, on the basis of information on Oath ;

(*a*) order a service provider, through the application of technical means to intercept, collect, record, permit or assist competent authorities with the collection or recording of content data or traffic data associated with specified communications transmitted by means of a computer system ; or

(*b*) authorise a law enforcement officer to collect or record such data through application of technical means.

Failure of Service Provider to Perform Certain Duties.

40.—(1) Every Service Provider in Nigeria shall comply with all the provisions of this Act and disclose information requested by any Law Enforcement Agency or otherwise render assistance in any inquiry or proceeding under this Act.

(2) Without prejudice to the generality of the foregoing, a service provider shall, at the request of any law enforcement agency in Nigeria or at its own initiative, provide assistance towards—

(*a*) the identification, apprehension and prosecution of offenders ;

(*b*) the identification, tracking and tracing of proceeds of any offence or any property, equipment or device used in the commission of any offence ; or

(*c*) the freezing, removal, erasure or cancellation of the services of the offender which enables the offender to either commit the offence, hide or preserve the proceeds of any offence or any property, equipment or device used in the commission of the offence.

(3) A Service Provider who contravenes the provisions of subsections (1) and (2) of this section commits an offence and is liable on conviction to a fine of not more than ₦10,000,000.00.

(4) In addition to the punishment prescribed under subsection (3) of this section and subject to the provisions of section 20 of this Act, each director, manager or officer of the service provider is liable on conviction to imprisonment for a term of not more than 3 years or a fine of not more than ₦7,000,000.00 or both.

PART V—ADMINISTRATION AND ENFORCEMENT

Co-ordination and Enforcement.

41.—(1) The Office of the National Security Adviser shall be the co-ordinating body for all security and enforcement agencies under this Act and shall—

(*a*) provide support to all relevant security, intelligence, law enforcement agencies and military services to prevent and combat cybercrimes in Nigeria ;

(*b*) ensure formulation and effective implementation of a comprehensive cyber security strategy and a national cyber security policy for Nigeria ;

(*c*) establish and maintain a National Computer Emergency Response Team (CERT) Co-ordination Center responsible for managing cyber incidences in Nigeria ;

(*d*) establish and maintain a National Computer Forensic Laboratory and co-ordinate utilization of the facility by all law enforcement, security and intelligence agencies ;

(*e*) build capacity for the effective discharge of the functions of all relevant security, intelligence, law enforcement and military services under this Act or any other law on cybercrime in Nigeria ;

(*f*) establish appropriate platforms for Public Private Partnership (PPP) ;

(g) co-ordinate Nigeria's involvement in international cyber security co-operation to ensure the integration of Nigeria into the global frameworks on cyber security ; and

(*h*) do such other acts or things that are necessary for the effective performance of the functions of the relevant security and enforcement agencies under this Act.

(2) The Attorney-General of the Federation shall strengthen and enhance the existing legal framework to ensure—

(*a*) conformity of Nigeria's cybercrime and cyber security laws and policies with regional and international standards ;

(*b*) maintenance of international co-operation required for preventing and combating cybercrimes and promoting cyber security ; and

(*c*) effective prosecution of cybercrimes and cyber security matters.

(3) All Law Enforcement, Security and Intelligence Agencies shall develop requisite institutional capacity for the effective implementation of the provisions of this Act and shall, in collaboration with the Office of the National Security Adviser, initiate, develop or organize training programmers nationally or internationally for officers charged with the responsibility for the prohibition, prevention, detection, investigation and prosecution of cybercrimes.

Establishment of Cybercrime Advisory Council.

42.—(1) There is established, the Cybercrime Advisory Council (in this Act referred to as "*the Council*") which shall consist of a representative each, of the ministries and agencies listed under the First Schedule to this Act.

First Schedule.

(2) A representative appointed under sub-section (1) of this section shall be an officer not below the Directorate Cadre in the Public Service or its equivalent.

(3) A member of the Council shall cease to hold office if—

(*a*) he ceases to hold the office on the basis of which he became a member of the Council ; or

(*b*) the President is satisfied that it is not in the public interest for the person to continue in office as a member of the Council.

(4) The Meetings of the Council shall be presided over by the National Security Adviser.

(5) The Council shall meet at least four times in a year and whenever it is convened by the National Security Adviser.

Functions and Powers of the Council.

43.—(1) The Council shall—

(*a*) create an enabling environment for members to share knowledge, experience, intelligence and information on a regular basis and shall provide recommendations on issues relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria ;

(*b*) formulate and provide general policy guidelines for the implementation of the provisions of this Act ;

(*c*) advise on measures to prevent and combat computer related offences, cybercrimes, threats to national cyberspace and other cyber security related issues ;

(*d*) establish a program to award grants to institutions of higher education to establish Cyber Security Research Centers to support the development of new cyber security defences ; techniques and processes in the real-world environment ; and

(*e*) promote Graduate Traineeships in cyber security and computer and network security research and development.

(2) The Council shall have power to regulate its proceedings and make standing orders with respect to the holding of its meetings, notices to be given, the keeping of minutes of its proceedings and such other matters as the Council may, from time to time, determine.

Establishment of National Cyber Security Fund.

44.—(1) There is established the National Cyber Security Fund (in this Act referred to as "*the Fund*").

(2) There shall be paid and credited into the Fund established under subsection (1) of this section and domiciled in the Central Bank of Nigeria—

Second Schedule.

(*a*) a levy of 0.005 of all electronic transactions by the businesses specified in the Second Schedule to this Act ;

(*b*) grants-in-aid and assistance from donor, bilateral and multilateral agencies ;

(*c*) all other sums accruing to the Fund by way of gifts, endowments. bequest or other voluntary contributions by persons and organizations :

Provided that the terms and conditions attached to such gifts, endowments. bequest or contributions will not jeopardize the functions of the Council ;

(*d*) such monies as may be appropriated for the Fund by the National Assembly ; and

(*e*) all other monies or assets that may, from time to time, accrue to the Fund.

(3) All monies accruing to the Fund shall be exempted from income tax and all contributions to the Fund shall be tax deductible.

(4) The levy imposed under subsection 2(*a*) shall be remitted directly by the affected businesses or organizations into the Fund domiciled in the Central Bank within a period of 30 days.

(5) An amount not exceeding 40 percent of the Fund may be allocated for programs relating to countering violent extremism.

(6) The Office of the National Security Adviser shall keep proper records of the accounts.

(7) The Account of the Fund shall be audited in accordance with guidelines provided by the Auditor-General of the Federation.

PART VI—ARREST, SEARCH, SEIZURE AND PROSECUTION

Power of arrest, search and seizure.

45.—(1) A Law Enforcement Officer may apply *ex-parte* to a Judge in Chambers for the issuance of a warrant for the purpose of obtaining electronic evidence in related crime investigation.

(2) The Judge may issue a warrant authorizing a Law Enforcement Officer to—

(*a*) enter and search any premises or place if. within those premises, place or conveyance—

(*i*) an offence under this Act is being committed ; or

(*ii*) there is evidence of the commission of an offence under this Act, or

(*iii*) there is an urgent need to prevent the commission of an offence under this Act ;

(*b*) search any person or conveyance found on any premises or place which such authorized officers who are empowered to enter and search under paragraph (*a*) of this subsection ;

(*c*) stop, board and search any conveyance where there is evidence of the commission of an offence under this Act ;

(*d*) seize, remove and detain anything which is, or contains, evidence of the commission of an offence under this Act ;

(*e*) use or cause to use a computer or any device to search any data contained in or available to any computer system or computer network ;

(*f*) use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format ; or

(*g*) require any person having charge of or otherwise concerned with the operation of any computer or electronic device in connection with an offence under this Act to produce such computer or electronic device.

(3) The Court shall issue a warrant under subsection (2) of this section where it is satisfied that—

(*a*) the warrant is sought to prevent the commission of an offence under this Act or to prevent the interference with investigative process under this Act ;

(*b*) the warrant is for the purpose of investigating cybercrime, cyber security breach, computer related offences or obtaining electronic evidence ;

(*c*) there are reasonable grounds for believing that the person or material on the premises or conveyance may be relevant to the cybercrime or computer related offences under investigation ; or

(*d*) the person named in the warrant is preparing to commit an offence under this Act.

Obstruction and refusal to release information.

46. Subject to the provisions of the Constitution of the Federal Republic of Nigeria, a person who—

(*a*) willfully obstructs any Law Enforcement Officer in the exercise of any power conferred by this Act ; or

(*b*) fails to comply with any lawful inquiry or request made by any Law Enforcement Agency in accordance with the provisions of this Act.

commits an offence and is liable on conviction to imprisonment for a term of 2 years or to a fine of not more than ₦500,000.00 or both.

Prosecution of offences.

47.—(1) Subject to the powers of the Attorney-General, relevant Law Enforcement Agencies shall have power to prosecute offences under this Act.

(2) In the case of offences committed under sections 19 and 21 of this Act, the approval of the Attorney-General must be obtained before prosecution.

Order of forfeiture of assets.

48.—(1) The Court, in imposing sentence on any person convicted of an offence under this Act, may order that the convicted person forfeits to the Government of the Federal Republic of Nigeria—

(*a*) any asset, money or property, whether tangible or intangible, traceable to proceeds of such offence ; and

(*b*) any computer, equipment, software, electronic device or any other device used or intended to be used to commit or to facilitate the commission of such offence.

(2) If it is established that a convicted person has assets or properties in a foreign country, acquired as a result of such criminal activities listed in this Act, such assets or property, shall subject to any Treaty or arrangement with such foreign country, be forfeited to the Federal Government of Nigeria.

(3) The Office of the Attorney-General of the Federation shall ensure that the forfeited assets or property are effectively transferred and vested in the Federal Government of Nigeria.

(4) A Person convicted of an offence under this Act shall have his International Passport cancelled and in the case of a Foreigner, his Passport shall be withheld and only returned to him after he has served the sentence or paid the fines imposed on him.

Order for Payment of Compensation or restitution.

49.—(1) In addition to any other penalty prescribed under this Act, the Court shall order a person convicted of an offence under this Act to make restitution to the victim of the false pretense or fraud by directing the person, where the property involved is money, to pay to the victim an amount equivalent to the loss sustained by the victim and in any other case to-

(*a*) return the property to the victim or to a person designated by him; or

(*b*) pay an amount equal to the value of the property, where the return of the property is impossible or impracticable.

(2) An order of restitution may be enforced by the victim or by the prosecutor on behalf of the victim in the same manner as a judgment in a civil action.

PART VII—JURISDICTION AND INTERNATIONAL CO-OPERATION

Jurisdiction.

50.—(1) The Federal High Court located in any part of Nigeria, regardless of the location where the offence is committed, shall have jurisdiction to try offences under this Act, if committed—

(*a*) in Nigeria ;

(*b*) in a ship or aircraft registered in Nigeria ;

(*c*) by a citizen or resident in Nigeria if the person's conduct would also constitute an offence under a law of the country where the offence was committed ; or

(*d*) outside Nigeria, where—

(*i*) the victim of the offence is a citizen or resident of Nigeria ; or

(*ii*) the alleged offender is in Nigeria and not extradited to any other country for prosecution.

(2) In the trial of any offence under this Act, the fact that an accused person is in possession of—

(*a*) pecuniary resources or property for which he cannot satisfactorily account ;

(*b*) which is disproportional to his known sources of income ; or

(*c*) that he had at or about the time of the alleged offence obtained an accretion to his pecuniary resources or property for which he cannot satisfactorily account, may, if proved, be taken into consideration by the court as corroborating the testimony of witness in the trial.

(3) The court shall ensure that all matters brought before it by the Council against any person, body or authority shall be conducted with dispatch and given accelerated hearing.

(4) Subject to the provisions of the Constitution of the Federal Republic of Nigeria, an application for stay of proceedings in respect of any criminal matter brought under this Act shall not be entertained until judgment is delivered.

Extradition. CAP. E25. LFN. 2004.

51. Offences under this Act shall be extraditable under the Extradition Act.

Request for mutual assistance.

52.—(1) The Attorney-General of the Federation may—

(*a*) request or receive assistance from any agency or authority of a foreign State in the investigation or prosecution of offences under this Act ; and

(*b*) authorize or participate in any joint investigation or cooperation carried out for the purpose of detecting, preventing, responding and prosecuting any offence under this Act.

(2) The joint investigation or cooperation referred to in sub-section (1) may be carried out whether or not any bilateral or multilateral agreement exists between Nigeria and the requested or requesting country.

(3) The Attorney-General of the Federation may, without prior request, forward to a competent authority of a foreign State, information obtained in the course of investigation, if such information will assist in the investigation of an offence or in the apprehension of an offender under this Act.

Evidence pursuant to a request.

53.—(1) Any evidence gathered, pursuant to a request under this Act, in any investigation or proceeding in the Court of any Foreign State, if authenticated, shall be prima facie admissible in any proceeding to which this Act applies.

(2) For the purpose of sub-section (1) of this section, evidence is authenticated if it is—

(*a*) certified by a Judge or Magistrate or Notary Public of the foreign State ; or

(*b*) sworn to under oath or affirmation of a witness or sealed with an official or public seal—

(*i*) of a Ministry or Department of the Government of the foreign State ; or

(*ii*) in the case of a territory, protectorate or colony, of the person administering the Government of the foreign territory, protectorate or colony or a department of that territory, protectorate or colony.

Form of request from a Foreign State.

54.—(1) A request under this Act shall be in writing, dated and signed by or on behalf of the person making the request.

(2) A request may be transmitted by facsimile or by any other electronic device or means, and shall include—

(*a*) the name of the authority conducting the investigation, prosecution or proceedings to which the request relates ;

(*b*) a description of the subject matter and nature of the investigation, prosecution, or proceedings, including the specific crimes which relate to the matter, the stage reached in the proceedings and any date for further proceedings ;

(*c*) a description of the evidence, information or other assistance sought ; and

(*d*) a statement of the purpose for which the evidence, information or other assistance is sought.

(3) To the extent necessary and possible, a request shall also include—

(*a*) information on the identity and location of any person from whom evidence is sought ;

(*b*) information on the identity and location of a person to be served, that person's relationship to the investigation, prosecution or proceedings, and the manner in which service is to be effected ;

(*c*) information on the identity and whereabouts of the person to be located ;

(d) a precise description of the place or person to be searched and of the articles to be seized ;

(*e*) description of the manner in which any testimony or statement is to be taken and recorded, including any special requirements of the law of the requesting State as to the manner of taking evidence relevant to its admissibility in that State ;

(*f*) list of questions to be asked of a witness ;

(*g*) description of any particular procedure to be followed in executing the request ;

(*h*) information as to the allowances and expenses to which a person asked to in the requesting State in connection with the request will be entitled ;

(*i*) court order, if any, or a certified copy thereof, which is to be enforced and a statement that such order is final ; and

(*j*) any other information which may be brought to the attention of the requested State to facilitate its execution of the request.

(4) A request shall not be invalidated for the purposes of this Act or any legal proceeding by failure to comply with the provision of subsection (2) of this section where the Attorney-General of the Federation is satisfied that there is sufficient compliance to enable him execute the request.

(5) Where the Attorney-General of the Federation considers it appropriate because an international arrangement so requires or it is in the public interest, he shall order that the whole or any part of any property forfeited under this Act or the value thereof, be returned or remitted to the requesting State.

Expedited preservation of Computer Data.

55.—(1) Nigeria may be requested to expedite the preservation of Electronic Device or Data stored in a Computer System or Network, referring to crimes described under this Act or any other enactment, pursuant to the submission of a request for assistance for search, seizure and disclosure of those data.

(2) The request under sub-section (1) of this section shall specify—

(*a*) the authority requesting the preservation or disclosure ;

(*b*) the offence being investigated or prosecuted, as well as a brief statement of the facts relating thereto ;

(*c*) the electronic device or computer data to be retained and its relation to the offence ;

(*d*) all the available information to identify the person responsible for the electronic device or data or the location of the computer system ;

(*e*) the necessity of the measure of preservation ; and

(*f*) the intention to submit a request for assistance for search, seizure and disclosure of the data.

(3) In executing the demand of a Foreign Authority under the preceding sections, the Attorney-General of the Federation may order any person who has the control or availability of such data, including a service provider, to preserve them or turn them in for proper preservation by an appropriate authority or person.

(4) Without prejudice to the provisions of subsection (3) of this section, the preservation may also be requested by any Law Enforcement Agency, with responsibility for enforcing any of the provisions of this Act, pursuant to an order of Court, which order may be obtained *ex-parte* where there is urgency or danger in delay.

(5) Where a Court grants an order, pursuant to the provisions of subsection (4) of this section, such order shall indicate—

(*a*) the nature of the evidence ;

(*b*) their origin and destination, if known ; and

(*c*) the period of time which shall not exceed 90 days over which data shall be preserved.

(6) In compliance with the preservation order, any Person who has the control or availability of such data, including a service provider, shall immediately preserve the data for the specified period of time, protecting and maintaining its integrity.

(7) A request for expedited preservation of electronic evidence or data may be refused if there are reasonable grounds to believe that the execution of a request for legal assistance for subsequent search, seizure and release of such data would be denied.

Designation of contact point.

56.—(1) In order to provide immediate assistance for the purpose of International co-operation under this Act, the Office of the National Security Adviser shall designate and maintain a contact point that shall be available 24 hours a day and 7 days a week.

(2) This contact point can be reached by other contact points in accordance with agreements, treaties or conventions by which Nigeria is bound, or in pursuance of protocols of cooperation with international judicial or law enforcement agencies.

(3) The immediate assistance to be provided by the contact point shall include—

(*a*) technical advice to other points of contact ;

(*b*) expeditious preservation of evidence in cases of urgency or danger in delay ;

(*c*) collection of evidence for which it has the legal jurisdiction in cases of urgency or danger in delay ;

(*d*) detection of suspects and provision of legal information in cases of urgency or danger in delay ;

(*e*) the immediate transmission of requests concerning the measures referred to in paragraphs (*b*) and (*d*) of this subsection, with a view to its expedited implementation.

PART VIII—MISCELLANEOUS

Regulations.

57.—(1) The Attorney-General of the Federation may make orders, rules, guidelines or regulations as are necessary for the efficient implementation of the provisions of this Act.

(2) Orders, rules, guidelines or regulations made under sub-section (1) of this section may provide for the—

(*a*) method of custody of video and other electronic recordings of suspects apprehended under this Act ;

(*b*) method of compliance with regulations or conventions issued by relevant international institutions on cyber security and cybercrimes ;

(*c*) procedure for freezing, unfreezing and providing access to frozen funds or other assets ;

(*d*) procedure for attachments, forfeiture and disposal of assets ;

(*e*) mutual legal assistance ;

(*f*) procedure for the prosecution of all cybercrime cases in line with national and international human rights standards ;

(*g*) procedure for ensuring prompt payment of any levy prescribed under this Act, including penalties and prosecution ; and

(*h*) any other matter the Attorney-General may consider necessary or expedient for the purpose of implementation of this Act.

erpretation. **58.** In this Act—

"*Access*" means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer system or network ;

"*Access Device*" includes electronic cards such as—

(*a*) Debit Cards ;
(*b*) Credit Cards ;
(*c*) Charge Cards ;
(*d*) Loyalty Cards ;
(*e*) Magnetic Stripe Based Cards ;
(*f*) Smart Chip Based cards ;
(*g*) EMV Cards ;
(*h*) Passwords ;
(*i*) Personal Identification Number (PIN) ;
(*j*) Electronic Plate ;
(*k*) Electronic Serial Number ;
(*l*) Code Number ;
(*m*) Mobile Identification Number ;

(*n*) any account number or other telecommunications service, equipment, or instrument identifier, or other means of account access including telephones, PDAs, etc. ;

(*o*) Automatic Teller Machines ;

(*p*) Point of Sales Terminals ; and

(*q*) other vending machines ;

"*ATM*" means Automated Teller Machine.

"*Authorised Access*" means a person has authorised access to any program or data held in a computer if—

(*a*) the person is entitled to control access to the program or data in question ; or

(*b*) the person has consent to access such program or data from a person who is charged with granting such consent ;

"*Authorised Manufacturer*" means a financial institution which, or any other person who, is authorised under any written law to produce a card ;

"*Authorised Officer or Authorised Persons*" means a member of any law enforcement agency or a person mandated by it, involved in the prohibition, prevention, elimination or combating of computer crimes and cyber security threats ;

"*Bank Card*" means any instrument, token, device, or card whether known as a bank service card, banking card, cheque guarantee card, or debit card or by any other similar name, issued with or without a fee by an issuer for the use of the cardholder in obtaining goods, services, or anything else of value or for the use in automated banking device to obtain money or any of the services offered through the device ;

"*Card*" means a bank card, credit card, or payment card ;

"*Cardholder*" means the person named on the face of a bank card, credit card or payment card to whom or for whose benefit such a card is issued by an issuer ;

"*Card-Making Equipment*" means any equipment, machine, plate, mechanism, impression, or any other device designed, used, or capable of being used to produce a card, a counterfeit card, or any aspect or component of a card ;

"*Computer*" means an electronic, magnetic, optical, electrochemical or other high speed data processing device performing logical, arithmetic, or storage functions and includes any data storage facility and all communication devices that can directly interface with a computer through communication protocols but it excludes portable hand-held calculator, typewriters and typesetters or other similar devices ;

"*Computer Data*" includes every information required by the computer to be able to operate, run programs, store programs and store information that the computer user needs such as text files or other files that are associated with the program the computer user is running.

"*Computer Program*" or "*Program*" means a set of instructions written to perform or execute a specified task with a computer ;

"*Computer System*"—

(*a*) refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated or interactive processing of data ;

(*b*) covers any type of device with data processing capabilities including, computers and mobile phones ;

(*c*) consists of hardware and software which may include input, output and storage components that may stand alone or be connected in a network or other similar devices ; and

(*d*) includes computer data storage devices or media ;

"*Consumer*" means every person or organization who enters into computer based purchase, lease, transfer, maintenance and consultancy service agreements with a computer service provider and the customer and agent of the consumer and includes bank account holders who carry financial cards ;

"*Content Data*" means the actual information or message sent across during a communication session ;

"*Counterfeit Card*" means a bank card, credit card or a payment card which is fictitious, altered, or forged and includes any facsimile or false representation, deception, or component of such a card, or any such card which is stolen, obtained as part of a scheme to defraud, or otherwise unlawfully obtained, and which may or may not be embossed with account information or an issuer's information ;

"*Countering Violent Extremism (CVE) Program*" includes any—

(*a*) intervention designed to counter the persistence of violent radicalization to reduce the incidence of violent activities, change the behaviour of violent extremists, and counter the negative extreme groups while promoting core national values ; and

(*b*) also any program that seeks to identify the underlying causes of radicalization (social, cultural, religious and economic) and develop strategies that provide solutions and also introduce measures to change the attitudes and perceptions of potential recruits, including providing vocational training of prisoners and means of sustainable livelihood and reintegration of reformed extremists to their families and communities ;

"*Credit*" includes a cash loan, or any other financial information ;

"*Credit Card*" means any instrument, token, device, or card, whether known as a charge card or by any other similar name, issued with or without a fee by an issuer for the use of the cardholder in obtaining goods, services, or anything else of value on credit from a creditor or for use in an automated banking device to obtain money or any of the services offered through the device ;

"*Creditor*" means a person or company that agrees or is authorised by an issuer to supply goods, services, or anything else of value and to accept payment by use of a bank card, credit card, payment card for the supply of such goods, services or anything else of value to the cardholder ;

"*Critical infrastructure*" means, systems and assets which are so vital to the country that the destruction of such systems and assets would have an impact on the security, national economic security, national public health and safety of the country ;

"*Counterfeit Access Device*" means counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or a counterfeit access device ;

"*Cyberstalking*" a course of conduct directed at a specific person that would cause a reasonable person to feel fear ;

"*Cybersquatting*" means the acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is—

(*a*) similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration ;

(*b*) identical or in any way similar with the name of a person other than the registrant, in case of a personal name ; and

(*c*) acquired without right or with intellectual property interests in it.

"*Damage*" means any impairment to a computer or the integrity or availability of data, program, system or information that—

(*a*) causes financial loss ;

(*b*) modifies or impairs or potentially modifies or impairs the medical examination, diagnosis, treatment or care of one or more persons ;

(*c*) causes or threatens physical injury or death to any person ; or

(*d*) threatens public health or public safety ;

"*Data*" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a Computer ;

"*Database*" means digitally organized collection of data for one or more purposes which allows easy access, Management and update of data ;

"*Device*" means any object or Equipment that has been designed to do a particular job or whose Mechanical or Electrical workings are controlled or monitored by a Microprocessor ;

"*Electronic Communication*" includes communications in electronic format, instant messages, Short Message Service (SMS), e-mail, video, voice mails, Multimedia Message Service (MMS), Fax, and Pager ;

"*Electronic Device*" means a device which accomplishes its purpose Electronically and this includes, Computer Systems, Telecommunication Devices, Smart Phones, Access Cards, Credit Cards, Debit Cards, Loyalty Cards, etc ;

"*Electronic Record*" means a record generated, communicated, received or stored by Electronic, Magnetic, Optical or other means in an Information System or for transmission from one information system to another ;

"*Electronic Transfer of Fund*" means any Transfer of Funds which is initiated by a person by way of instruction, authorisation or order to a Bank to Debit or Credit an account maintained with that Bank through Electronic means and includes point of sales transfers, Automated Teller Machine transactions, direct deposits or withdrawal of funds, transfer initiated by Telephone, Internet and Card Payment ;

"*Expired Card*" means a card which is no longer valid because the term shown of it has expired ;

"*Financial Institution*" includes any individual, body, association or group of persons, whether corporate or unincorporated which carries on the business of investment and securities, a discount house, finance company and money brokerage whose principal object includes factoring project financing equipment leasing, debt administration, fund management, private ledger services, investment management, local purchase order financing, export finance, project consultancy, financial consultancy, pension fund management, insurance institutions, debt factorization and conversion firms, dealer, clearing and settlement companies, legal practitioners, hotels, casinos, bureau de change, supermarkets and such other businesses as the Central Bank or appropriate regulatory authorities may, from time to time, designate ;

"*Financial Transaction*" means—

(*a*) a transaction which in any way involves movement of funds by wire or other electronic means ;

(*b*) involves one or more monetary instruments ;

(*c*) involves the transfer of title to any real or personal property ;

"*Function*" includes logic, control, arithmetic, deletion, storage, retrieval and communication or telecommunication to, from or within a computer ;

"*Identity Theft*" means, the stealing of somebody else personal information to obtain goods and services through electronic based transactions ;

"*Infrastructure Terminal*" includes terminals which include GSM Phones that can be used to access bank or any other sensitive information, Point of sales terminals (POS) and all other Card Acceptor Devices that are in use now or may be introduced in the future ;

"*Interception*" in relation to a function of a computer system or communications network, includes listening to or recording of communication data of a computer or acquiring the substance, meaning or purport of such and any act capable of blocking or preventing any of these functions ;

"*Issuer*" includes a financial institution which or any other entity who is authorised by the Central Bank to issue a payment card ;

"*Law Enforcement Agencies*" includes any agency for the time being responsible for implementation and enforcement of the provisions of this Act ;

"*Minister*" means the Attorney-General of the Federation ;

"*Modification*" means deletion, deterioration, alteration, restriction or suppression of data within computer systems or networks, including data transfer from a Computer System by any means ;

"*Network*" means a collection of hardware components and computers interconnected by communications channels that allow sharing of resources and information ;

"*Payment Card*" means any instrument, token, device, or card, or known by any other similar name, and encoded with a stated money value and issued with or without a fee by an issuer for use of the cardholder in obtaining goods, services, or anything else of value, except money ;

"*Person*" includes an individual, body corporate, organisation or group of persons ;

"*President*" means the President, Commander-in-Chief of the Armed Forces of the Federal Republic of Nigeria ;

"*Phishing*" means the criminal and fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication through e-mails or instant messaging either in form of an email from what appears from your bank asking a user to change his or her password or reveal his or her identity so that such information can later be used to defraud the user ;

"*Purchasing Forged Electronic*" means a Credit or Debit Transfer Instruments such as Credit Card, Debit Card, Smart Card, ATM or other related electronic payment system devices ;

"*Receives*" or "*Receiving*" means acquiring possession, title or control or accepting a card as security for credit ;

"*Revoked Card*" means a card which is no longer valid because permission to use it has been suspended or terminated by the issuer, whether on its own or on the request of the cardholder ;

"*Service Provider*" means—

(*a*) any public or private entity that provides to users of its services the ability to communicate by means of a computer system, electronic communication devices, mobile networks ; and

(*b*) any other entity that processes or stores computer data on behalf of such communication service or users of such service ;

"*Sexually explicit conduct*" includes at least the following real or simulated acts—

(*a*) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between children, or between an adult and a child, of the same or opposite sex ;

(*b*) bestiality ;

(*c*) masturbation ;

(*d*) sadistic or masochistic abuse in a sexual context ; or

(*e*) lascivious exhibition of the genitals or the pubic area of a child. It is not relevant whether the conduct depicted is real or simulated ;

"*Spamming*" means an abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages to individuals and corporate organizations ;

"*Traffic*" means to sell, transfer, distribute, dispense, or otherwise dispose of property or to buy, receive, possess, obtain control of, or use property with the intent to sell, transfer, distribute, dispense, or otherwise dispose of such property ; and

"*Traffic Data*" means any computer data relating to a communication by means of a computer system or network, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Citation.

59. This Act may be cited as the Cybercrimes (Prohibition, Prevention, Etc.) Act, 2015.

FIRST SCHEDULE

Section 42 (1)

MEMBERS OF THE CYBERCRIME ADVISORY COUNCIL

(1) The Cybercrime Advisory Council shall consist of a representative each of the following Ministries, Departments and Agencies—

(*a*) Federal Ministry of Justice ;

(*b*) Federal Ministry of Finance ;

(*c*) Ministry of Foreign Affairs ;

(*d*) Federal Ministry of Trade and Investment ;

(*e*) Central Bank of Nigeria ;

(*f*) Office of the National Security Adviser ;

(*g*) Department of State Services ;

(*h*) Nigeria Police Force ;

(*i*) Economic and Financial Crimes Commission ;

(*j*) Independent Corrupt Practices Commission ;

(*k*) National Intelligence Agency ;

(*l*) Nigerian Security and Civil Defence Corps ;

(*m*) Defence Intelligence Agency ;

(*n*) Defence Headquarters ;

(*o*) National Agency for the Prohibition of Traffic in Persons ;

(*p*) Nigeria Customs Service ;

(*q*) Nigeria Immigration Service ;

(*r*) National Space Management Agency ;

(*s*) Nigerian Information Technology Development Agency ;

(*t*) Nigerian Communications Commission ;

(*u*) Galaxy Backbone ;

(*v*) National Identity Management Commission ;

(*w*) Nigeria Prisons Service ;

(*x*) One representative each from the following—

(*i*) Association of Telecommunications Companies of Nigeria ;

(*ii*) Internet Service Providers Association of Nigeria ;

(*iii*) Nigeria Bankers Committee ;

(*iv*) Nigeria Insurance Association ;

(*v*) Nigerian Stock Exchange ; and

(*vi*) Non-Governmental Organization with Focus on Cyber Security.

(2) The Cybercrime Advisory Council shall also consist of a representative of any other Ministry, Department, Agency or institution which the Minister may, by notice published in the Federal *Gazette*, add to the list under paragraph 1 of this Schedule.

SECOND SCHEDULE *Section* 44 (2) (*a*)

Businesses which Section 44 (2) (*a*) refers to are—

(*a*) GSM Service providers and all telecommunication companies ;

(*b*) Internet Service Providers ;

(*c*) Banks and other Financial Institutions ;

(*d*) Insurance Companies ; and

(*e*) Nigerian Stock Exchange.

I certify, in Accordance with Section 2 (1) of the Acts Authentication Act, Cap. A2, Laws of the Federation of Nigeria 2004, that this is a true copy of the Bill passed by both House of the National Assembly.

SALISU ABUBAKAR MAIKASUWA, OON, mni
Clerk to the National Assembly
14*th Day of May*, 2015.

EXPLANATORY MEMORANDUM

This Act provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of Cybercrime in Nigeria. This Act also ensures the protection of critical national information infrastructure, and promotes Cyber Security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

SCHEDULE TO CYBERCRIMES (PROHIBITION, PREVENTION, ETC.) BILL, 2015

(1) *Short Title of The Bill*	(2) *Long Title of The Bill*	(3) *Summary of the Contents of the Bill*	(4) *Date Passed by the Senate*	(5) *Date Passed by the House of Representatives*
Cybercrimes (Prohibition, Prevention, Etc.) Bill, 2015.	An Act to provide for the prohibition, prevention, detection, response, investigation and prosecution of Cybercrimes ; and for other related matters.	This Bill provides an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of Cybercrimes in Nigeria. This Act also ensures the protection of critical national information infrastructure, and promotes Cyber Secutity and the protection of Computer Systems and Networks, Electronic communications, data and computer programs, intellectual property and privacy rights.	5th May, 2015.	7th May, 2015.

I certify that this Bill has been carefully compared by me with the decision reached by the National Assembly and found by me to be true and correct decision of the Houses and is in accordance with the provisions of the Acts Authentication Act Cap. A2, Laws of the Federation of Nigeria, 2004.

SALISU MAIKASUWA, OON, mni
Clerk to the National Assembly
14*th Day of May*, 2015

I ASSENT

LS

DR. GOODLUCK EBELE JONATHAN, GCFR
President of the Federal Republic of Nigeria
15*th Day of May*, 2015

CYBERCRIMES

(PROHIBITION, PREVENTION, ETC) (AMENDMENT)

ACT, 2024

CYBERCRIMES (PROHIBITION, PREVENTION, ETC) (AMENDMENT) ACT, 2024

EXPLANATORY MEMORANDUM

This Act amends the Cybercrimes (Prohibition, Prevention, Etc.) Act, No. 17, 2015 to insert some consequential words that were inadvertently omitted in the Act.

CYBERCRIMES (PROHIBITION, PREVENTION, ETC) (AMENDMENT) ACT, 2024

Arrangement of Sections

Section:

1. Amendment of Act No. 17, 2015
2. Amendment of section 17
3. Amendment of section 21
4. Amendment of section 22
5. Amendment of section 24
6. Amendment of section 27
7. Amendment of section 30
8. Amendment of section 37
9. Amendment of section 38
10. Amendment of section 41
11. Amendment of section 44
12. Amendment of section 48
13. Citation

CYBERCRIMES (PROHIBITION, PREVENTION, ETC) (AMENDMENT) ACT, 2024

A Bill

For

An Act to amend Cybercrimes (Prohibition, Prevention, etc.) Act, No. 17, 2015 to insert some consequential words that were inadvertently omitted in the Act; and for related matters.

[ ] Commencement

ENACTED by the National Assembly of the Federal Republic of Nigeria —

1. The Cybercrimes (Prohibition, Prevention, etc.) Act, No. 17, 2015 (in this Act referred to as "the Principal Act" is amended as set out in this Act. Amendment of Act No. 17, 2015

2. Section 17 of the Principal Act is amended — Amendment of section 17

(a) in subsection (2) by substituting for the word "geniuses" the word "genuineness"; and

(b) in subsection (4) by inserting after the word "signature", the words, "except where they are legally verified in "Certified True Copies".

3. Section 21 (1) of the Principal Act is amended — Amendment of section 21

(a) in subsection (1) by inserting after the words "Coordination Center" in line 6, the words, "through their respective sectoral CERTs or sectoral Security Operations Centres (SOC)"; and

(b) in subsection (3) by substituting for the expression "7 days of its occurance", the expression, "72 hours of its detection".

4. Section 22 (1) of the Principal Act is amended by inserting after the words "any Financial Institution", the words "public or private organisation". Amendment of section 22

5. Section 24 (1) of the Principal Act is amended by substituting for paragraphs (a) and (b), new paragraphs "(a)" and "(b)" — Amendment of section 24

"(a) is pornographic; or

(b) he knows to be false, for the purpose of causing a breakdown of law and order, posing a threat to life, or causing such message to be sent,".

6. Section 27 (2) of the Principal Act is amended by substituting for the words "a financial institution" in lines 1 and 2, the words, "any public or private organisation". Amendment of section 27

7. Section 30 of the Principal Act is amended — Amendment of section 30

(a) in subsection (1) by inserting after the word "terminals", the words "or any other payment technology means"; and

(b) in subsection (2) by substituting for the words "or point of sales device", the words "or any other payment technology means".

8. Section 37 (1) (a) of the Principal Act is amended by inserting after the word "present", the words, "National Identification Number issued by the National Identity Management Commission and other valid". Amendment of section 37

9. Section 38 of the Principal Act is amended by substituting for subsection (1) a new subsection "(1)" — Amendment of section 38

"(1) A service provider shall keep and protect specific traffic data and subscriber information in accordance with the provision of the Nigeria Data Protection Act and as may be prescribed by the relevant authority for the time being, responsible for the regulation of communication services in Nigeria, for a period of two years."

10. Section 41 (1) of the Principal Act is amended by substituting for paragraphs (d) – (h) new paragraphs "(d)"–"(j)" — Amendment of section 41

"(d) ensure the establishment of sectoral Computer Emergency Response Teams (CERT) and sectoral Security Operation Centres (SOC) that shall feed into the national CERT;

(e) ensure that all public and private organisations integrate and route their internet and data traffic to the sectoral SOCs thereby protecting the national cyberspace;

(f) establish and maintain a National Computer Forensic Laboratory and coordinate utilisation of the facility by all law enforcement, security and intelligence agencies;

(g) build capacity for the effective discharge of the functions of all relevant security, intelligence, law enforcement and military services under this Act or any other law on cybercrime in Nigeria;

(h) establish appropriate platforms for public private partnership (PPP);

(i) coordinate Nigeria's involvement in international cyber security cooperation to ensure the integration of Nigeria into the global frameworks on cyber security; and

(j) do such other acts or things that are necessary for the effective performance of the functions of the relevant security and enforcement agencies under this Act."

11. Section of 44 of the Principal Act is amended — Amendment of section 44

(a) in subsection (1) by substituting for paragraph (a) a new paragraph "(a)"

"(a) a levy of 0.5% (0.005) equivalent to a half percent of all electronic transactions value by the business specified in the Second Schedule to this Act"; and

(b) by substituting for subsection (6), new subsections "(6)" — "(8)" —

(6) The Office of the National Security Adviser shall administer, keep proper records of the accounts and shall ensure compliance monitoring mechanism.

(7) The account of the Fund shall be audited in accordance with guidelines provided by the Auditor General for the Federation.

(8) A business specified in the Second Schedule to this Act that fails to remit the levy under section 44 (2)(a) of this Act commits an offence and is liable on conviction to a fine of not less than 2% of the annual turnover of the defaulting business and failure to comply shall lead to closure or withdrawal of the business operational licence.

12. Section 48 of the Principal Act is amended by deleting subsection "(4)" Amendment of section 48

13. This Act may be cited as the Cybercrimes (Prohibition, Prevention, etc.) (Amendment) Act, 2024 Citation

I, CERTIFY, IN ACCORDANCE WITH SECTION 2 (1) OF THE ACTS AUTHENTICATION ACT, CAP. A2, LAWS OF THE FEDERATION OF NIGERIA, 2004, THAT THIS IS A TRUE COPY OF THE BILL PASSED BY BOTH HOUSES OF THE NATIONAL ASSEMBLY.

SANI MAGAJI TAMBAWAL, fcna
CLERK TO THE NATIONAL ASSEMBLY

27th DAY OF Feb., 2024

'HEDULE TO THE CYBERCRIMES (PROHIBITION, PREVENTION, ETC) (AMENDMENT) BILL, 2024

HORT TITLE OF HE BILL	LONG TITLE OF THE BILL	SUMMARY OF THECONTENTS OF THE BILL	DATE PASSED BY THE SENATE	DATE PASSED BY THE HOUSE O REPRESENTATIVI
'ybercrimes Prohibition, revention, etc.) Amendment) Bill, 024	An Act to amend the Cybercrimes (Prohibition, Prevention, etc.) Act, No. 17, 2015 to insert some consequential words that were inadvertently omitted in the Act; and for related matters.	This Bill amends the Cybercrimes (Prohibition, Prevention, etc.) Act, No. 17, 2015 to insert some consequential words that were inadvertently omitted in the Act.	21st December, 2023	14th February, 2024

55

I certify that this Bill has been carefully compared by me with the decision reached by the National Assembly and found by me to be true and correct decision of the Houses and is in accordance with the provisions of the Acts Authentication Act Cap. A2, Laws of the Federation of Nigeria, 2004.

SANI MAGAJI TAMBAWAL, fcna
Clerk to the National Assembly
27th Day of February, 2024

ASSENT.

BOLA AHMED TINUBU, GCFR
President of the Federal Republic of Nigeria
28th Day of Feb., 2024