An Overview of Cybercrime (Prevention & Prohibition) Act, 2015

By

Abbah Sambo Usman CISSP, CFE

Head, Cybercrimes Section, Abuja Zone

Disclaimer

The views expressed herein are solely those of the authors and do not necessarily reflect the views of EFCC or any component or other officer thereof.

OUTLINE

- Introduction to cybercrime
- Legal Framework
- The "Guy men" & Yahoo Plus
- Trend
- Overview

Legal Framework

LAWS:

- Advance Fee Fraud and other Fraud Related Offences Act (2006)
- Evidence Act, 2011
- Cybercrime (Prohibition, Prevention etc) Act, 2015

The " Guy Men"

- Perpetrators of what is called "419"
- Syndicate controlled by a "Chairman"
- Male of age 15 to 35 years
- Members play various roles
  - "Catchers"
  - "Pickers" – Mule

The " Guy Men"

- Freedom to operate independently
- Victim is called "Mugu", "Maga" etc
- Each scam type is called a "format"
- Mass mailing – "bombing"
- Use Bureau De Change (BDC) operators – foreign bank account for "drop"
- Previously had little hacking skills – script kiddies

Yahoo Plus

- Involves use of "fetish means to hypnotize victims"
  - Sleeping at cemetery
  - Bathing in river
  - "Sleep with ladies in order to take their star and fortune"
  - Festac Town, Shomolu, Opebi, Allen Avenue, Ojodu, Oke-Ira, Akiode, Bariga and the Akoka areas of Lagos

Trends – Cybercrime

Identity Fraud & Advance Fee Fraud

- 24 Year Old Godwin Bello Onamisi
- Hacked the email address of CG of Customs and sent emails therefrom, requesting for "assistance"
- Convicted to 6 months imprisonment

Trends – Cybercrime
Romance Scam

Trends – Kingsley Ezenwa

Romance Scam

- This 28 year old created a Facebook account using the name Sgt. Smith Muldoon, a US army officer from New York, and an email smithmuldoon@yahoo.com to match.
- Used this fake profile on social media to dupe ladies from Australia
  - Stephane - $300
  - Elizabeth - $500
  - Tina - $10,000
- Case is still under investigation

Trends – Cybercrime

Credit Card Schemes

- Chris Okeke, Nicholas Egboh and Kelechi Aro are members of a syndicate that specializes in cloning ATM cards
- Send phising emails to unsuspecting victims to steal ATM card details
- Use Skimmer to clone ATM Card
- Arrested in Lagos
- Case is under prosecution

TREND: CARD SCHEMES

TREND: ATM CARD SKIMMER

TREND: MAGNETIC STRIPE READER-WRITER

Overview

- **CYBERCRIMES (PROHIBITION, PREVENTION, (ETC) ACT 2015**
- The purpose of the Act is to provide an effective unified legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria.
- Ensure the protection of Critical National Information Infrastructure.
- Promote cyber-security and the protection of computer systems and networks, electronic communications, data and computer programs, intellectual property and privacy rights.

INFORMATION AND CYBER SECURITY AND THE ACT

- Three Cardinal guiding principles govern information and cyber security and form the bedrock of the provisions of the Cybercrime Prohibition, Prevention, etc. Act. 2015 (the Act).
- **The CIA principles:**
- **Confidentiality**—(privacy– information to be read and accessed by the right people)
- **Integrity** -- (Information only to be changed by the authorised persons and processes)
- **Availability** -- (information to be available to read and use when we want it)

- **Management of CNII's**
- The Order may prescribe minimum standards, guidelines, rules or procedure relating to their protection, preservation, management, access to, procedural rules and requirement for securing the integrity and authenticity of data, storage and archiving of data, recovery plans in the event of disaster, breach or loss, transfer and control of data in any CNII.
- The order may also require the NSA to audit and inspect any CNII at any time to ensure compliance with provisions of the Act.

- **OFFENCES AGAINST CNII's**
- Attracts grave penalties such as:
- Any cybercrime against CNII is punishable with 10 years imprisonment without option of fine.
- 15 years if it results in grievous bodily harm and
- Life imprisonment if death is the result.
- **ESTABLISHMENT OF THE NIGERIAN EMERGENCY RESPONSE TEAM**
- The Cybercrime Act provides for the Nigerian Emergency Response Team (ngCERT). Its operations centre was officially commissioned and domiciled in the office of the NSA by the then NSA -- Mohammed Sambo Dasuki on 25th May 2015, upon the Act being signed into law in 15th May 2015.
- Cyber attacks can now be reported on its web address namely:
- https://www.cert.gov.ng/

- Anyone who operates a computer system or network are to inform ng-CERT of attacks, intrusions and other disruptions liable to hinder functioning of another computer system or network is duty bound to report such to ng-CERT within 7 days or face denial of internet services and fine of N2m .
- Ng-CERT has the power to isolate affected computer systems or networks– (botnets)
- They also network and provide intelligence to other jurisdictions.

- **<u>OFFENCES AND PENALTIES</u>**
- The Act created offences and prescribed penalties for cybercrimes.
- Prescribes maximum sentence in most case with few exceptions so supports judicial discretion.
- 3 major categories of cybercrimes are covered by the Act being Cybercrimes against: **Persons, properties including computer systems** and **governments**.

- **CYBERCRIMES AGAINST PERSONS**
- **IDENTITY THEFT AND IMPERSONATION- S: 22**
- Making use of false e-signature, password or other unique identification feature of any person.
- Impersonation.
- Making false statement relating to a person's identity for the purpose of procuring issuance of card or other instrument to himself or another–
- Can be helpful where bank accounts were opened with false IDs for fraudulent purposes.
- Attracts punishment upon conviction of 7 years imprisonment or N5, 000,000.00 fine or both.

- **<u>CYBER STALKING, BULLYING AND HARASSMENT- section 24</u>**
- Sending or causing to be sent false, offensive, pornographic or indecent, obscene or menacing, false, annoying, insolent, intimidating, or hateful, message to another.
- Online defamation of character, and threats to kidnap or demanding ransom on line, are also covered here as well as harassment and bullying.
- Liable on conviction to a fine ranging from N7,000,000.00 to N25,000,000 or imprisonment for a term of ranging from 3 years to 10 years or to both such fine and imprisonment.

- **VICTIMS PROTECTION UNDER THE ACT** Section 24 (3)-(6)
- A court in sentencing or otherwise dealing with a person convicted of cyber harassment or bullying may make a restraining order (for a specified period or upon further order) for the protection of the victim/s.
- Flouting such restraining order attracts a fine of not more than N10m and/or imprisonment not exceeding 3 years.
- Interim order for the protection of victims.

- **CHILD PORNOGRAPHY– SECTION 23**
- Pornography generally is prohibited by the Act but child pornography is specifically defined to include:
- Producing, offering or making available, transmitting, distributing, procuring, or possessing child pornography.
- Proposing, Grooming or soliciting a child for such.
- Engaging in sexual activities with a child including using coercion, inducement, force or threats, abuse of position of trust, authority or influence or abuse is made of vulnerable situation of a child.
- Exposing or causing a child to participate in pornographic performances.

- **Racist and Xenophobic Offences** - Section 26
- Distributing or otherwise making available such materials that:
- Threatens a person on account of his race, colour, ethnic origin, religion etc.
- Publicly Insulting persons on those account
- Approving acts of genocide, crimes against humanity etc.,

- **CRIMES AGAINST AND PROPERTIES AND COMPUTER SYSTEMS**
- Producing, supplying, adapting, manipulating, procuring for use, importing, exporting, distributing, offering for sale or otherwise making available devices to aid committing cybercrime.
- Dealing in passwords, access codes, devices designed to overcome security measures.
- Possession of such devices, disclosing passwords or access code or any means of gaining access to any program or data
- **PHISHING, SPAMMING AND SPREADING OF COMPUTER VIRUS**
- Section 32
- Phishing—attempt to obtain sensitive information such as passwords, credit/debit card details, user names for fraudulent means by appearing to be a trustworthy entity in electronic communications.
- Spamming- sending unsolicited mails especially advertising repeatedly. However the Act requires intent to disrupt the operations of a computer.
- Sending viruses and malwares/ need to have caused damage to critical information in systems.

- **ELECTRONIC CARD OFFENCES**
- Using access device like financial cards to obtain cash, credit, goods or services.
- Stealing an electronic card,
- Receiving and/or retaining stolen or mislaid E-Card.
- Obtaining E-Card as security for debt
- Signing E-Card of another with intent to commit fraud.
- Using E-card of another by misrepresentation
- Possessing counterfeit E-card, invoices, vouchers, sales cards or card account number of another etc.
- Dealing in E-card
- Institution making available, lending, donating or selling list or portion of list of card holders and their addresses and card numbers to any person without their prior written consent. Exemption– CBN or licensed credit bureau to determine financial rating of cardholder but must give notice of such disclosure within 7days.

- **CYBERSQUATTING – section 25**
- Domain name serves as an on-line trademark, source identifier, and indicates quality and repository of good will.
- Companies sometimes buy up all available names associated with a particular word or phrase to protect their trademark.
- Cyber squatters attacks websites by registering similar domain name to an existing one and thus **make profit** off another person's trademark, including interfering with the use of the legitimate owner e.g. for employment purposes, diverting legitimate revenue, online infringement of copyright, name of celebrity for pornographic site etc.
- Liable on conviction to imprisonment for a term of not more than 2 years or a fine of not more than N5,000,000.00 or to both fine and imprisonment.

- **ATTEMPT, CONSPIRACY, AIDING AND ABETTING- SECTION 27**
- Attracts on conviction the punishment provided for the principal offence under the Act.
- Any employée of a Financial institution found to have connive with another person, or group of persons to perpetrate fraud using computer system(s) or network, commits an offence and shall be 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.

- **OTHER OFFENCES**
- Hacking
- Manipulation of ATM or POS Terminals
- System interference
- Intercepting electronic message, money transfers and emails
- Computer related forgeries
- Computer related fraud
- Theft of electronic devices
- Unauthorised modification of computer systems

Cybercrime Acts. 2015

- **10.** Allows for the **interception of electronic communication**, by way of a court order by a Judge, 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 proceedings.

Jurisdiction Section 50 CCA

- Federal High Court, regardless of where offence was committed
- Nigeria: Citizen, resident, offender in Nigeria, Ship, aircraft registered in Nigeria,
- Outside: Victim is citizen or resident, offender in Nigeria