iclg

Cybersecurity 2025

Eighth Edition



Contributing Editor:
Edward R. McNicholas
Ropes & Gray LLP

glg Global Legal Group

Expert Analysis Chapters

1 **Generative AI and Cyber Risk in China**
Susan Ning & Han Wu, King & Wood Mallesons

7 **Generative AI and Cyber Risk in Singapore**
Lim Chong Kin, David N. Alfred & Albert Pichlmaier, Drew & Napier LLC

Q&A Chapters

14 **Argentina**
Francisco Zappa & Agustina Pizarro Miguens, Bomchil

22 **Australia**
Dennis Miralis, Jasmina Ceic & Darren Pham, Nyman Gibson Miralis

30 **Canada**
Theo Ling, Conrad Flaczyk, Matthew Cook & Ahmed Shafey, Baker McKenzie

42 **China**
Susan Ning & Han Wu, King & Wood Mallesons

56 **Czech Republic**
Jana Pattynová, Dominik Vítek & Kryštof Lédl, Pierstone

66 **England & Wales**
Rohan Massey, Edward Machin & Robyn Bond, Ropes & Gray LLP

77 **Finland**
Erkko Korhonen, Louna Taskinen & Samuli Simojoki, Borenius Attorneys Ltd

84 **France**
Pierre Affagard & Mathilde Carvès, Clyde & Co

93 **Germany**
Dr. Alexander Niethammer, Stefan Saerbeck, Tobias Abersfelder & Isabella Norbu, Eversheds Sutherland

103 **Greece**
Dr. Nikos Th. Nikolinakos, Dina Th. Kouvelou & Alexis N. Spyropoulos, Nikolinakos & Partners Law Firm

116 **India**
Manisha Singh & Srinjoy Banerjee, LexOrbis

128 **Indonesia**
Oene J. Marseille, Kevin Sidharta, Giffy Pardede & Elsie Hakim, AGI Legal

137 **Italy**
Chiara Bianchi, Paradigma – Law & Strategy

150 **Japan**
Hiromi Hayashi, Masaki Yukawa & Daisuke Tsuta, Mori Hamada & Matsumoto

160 **Malaysia**
Timothy Siaw, Janet Toh, Hon Yee Neng & Yee Yong Xuan, Shearn Delamore & Co.

167 **Nigeria**
John C. Onyido, Franklin Okoro, Maryam Abdulsalam & Pelumi Adeyeye, S.P.A. Ajibade & Co.

178 **Singapore**
Lim Chong Kin, David N. Alfred & Albert Pichlmaier, Drew & Napier LLC

190 **Sweden**
Jonas Forzelius, Esa Kymäläinen & Jesper Jakobsson, TIME DANOWSKY Law Firm

199 **Switzerland**
Daniela Fábián & Aranya di Francesco, FABIAN PRIVACY LEGAL GmbH

208 **Taiwan**
Steven Hsu, Hsu & Associates

217 **USA**
Edward R. McNicholas & Frances E. Faircloth, Ropes & Gray LLP

Nigeria

S.P.A. Ajibade & Co.


John C. Onyido


Franklin Okoro


Maryam Abdulsalam


Pelumi Adeyeye

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)

Yes. Section 6 of the Cybercrimes (Prohibition and Prevention etc.) (Amendment) Act 2024 (the "Cybercrimes Act") makes it an offence for any person, without authorisation, to intentionally access a computer system in whole or in part, for fraudulent purpose in order to obtain data vital to national security. The maximum penalty for this offence in Nigeria is imprisonment for a term of not more than five years, a fine of not more than ₦5 million, or both such fine and imprisonment.

It is also an offence where, any person who, with the intent to commit an offence obtains computer data, secure access to any program, commercial or industrial secrets or classified information without authorisation. The maximum penalty for this offence in Nigeria is imprisonment for a term of not more than seven years, a fine of not more than ₦7 million, or both such fine and imprisonment.

However, any person who, with the intent to commit an offence, uses any device to avoid detection or otherwise prevent identification or attribution with the act or omission will be liable, on conviction, to imprisonment for a term of not more than seven years, a fine of not more than ₦7 million, or both.

Furthermore, where a person or organisation knowingly and intentionally traffics in any password or similar information through which a computer may be accessed without lawful authority, and such trafficking affects public, private and or individual interest within or outside the federation of Nigeria, such person or organisation would be held to have committed an offence and shall be liable, on conviction, to a fine of not more than ₦7 million, imprisonment for a term of not more than three years, or both such fine and imprisonment.

Examples of prosecution of this offence

In March 2023, the Lagos State police command of the Nigeria Police Force ("NPF") arraigned a fraud syndicate comprising eight men before the Federal High Court in Lagos for allegedly hacking into the server of an electronic platform, ITEX Integrated Services Limited, and stealing ₦435.3 million.[1]

In August 2024, the Police Special Fraud Unit arraigned two university students in Nigeria before the Federal High Court in Lagos for allegedly hacking MTN Nigeria Communication Plc's computers and stealing airtime and data valued at ₦1.9 billion. The case is still ongoing in court.[2]

Denial-of-service attacks

Yes. Section 8 of the Cybercrimes Act makes it an offence for any person without lawful authority, intentionally or for fraudulent purposes to carry out an act that 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.

The maximum penalty for such offence is imprisonment for a term of not more than two years, a fine of not more than ₦5 million, or both such fine and imprisonment.

Phishing

Yes. Under Section 32 of the Cybercrimes Act, it is an offence for anyone to attempt to obtain sensitive information such as usernames, passwords, or credit card details by masquerading as a trustworthy entity in electronic communications. This includes using emails or instant messaging to impersonate, and deceive users to change their password, or disclosing their identity with the intent of later using this information to commit fraud.

The maximum penalty for this offence is imprisonment for a term of three years, a fine of ₦1 million, or both.

Examples of prosecution of this offence

On 21 August 2024, the Economic and Financial Crimes Commission ("EFCC") convicted four suspected fraudsters, following their arrest by the EFCC, for impersonation, phishing and hacking of email accounts.[3]

On 30 August 2024, operatives of the Uyo Zonal Directorate of the EFCC arraigned over 40 suspected internet fraudsters for being involved in various forms of online fraud, such as romance scams, identity theft, phishing and money laundering.[4]

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. Section 32 (3) of the Cybercrimes Act makes it an offence for any person who engages in the malicious or deliberate spread of viruses or any malware that causes damage to critical information in public, private or financial institution's computers.

The maximum penalty for this offence is imprisonment for a term of three years, a fine of ₦1 million, or both.

Examples of prosecution of this offence

In June 2022, a suspected fraudster was convicted by a High Court Judge in Lagos following prosecution by the EFCC. The EFCC had received an intelligence report from the Interpol Global Complex for Innovation in Singapore regarding a group of internet fraudsters in Nigeria. These individuals were using

malware to steal personal information and credentials, which they then exploited to defraud unsuspecting victims.[5]

In November 2020, three suspects were arrested in Lagos following a joint INTERPOL, Group-IB, and NPF cybercrime investigation. The Nigerian nationals were believed to be members of a wider organised crime group responsible for distributing malware to damage IT systems, and carrying out extensive business email compromise scams.[6]

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Yes. It is an offence under Section 28 (1) of the Cybercrimes Act for any person to unlawfully produce, supply, adapt, manipulate, or procure for use, import, export, distribute, offer for sale, or otherwise make available: (a) any device, including a computer program or a component designed or adapted for the purpose of committing an offence under the 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 the Act; (c) the importation and fabrication of E-Tools; or (d) any device, including a computer program designed to overcome security measures in any computer system or network with the intent that the devices be utilised for the purpose of violating any provision of the Act.

The maximum penalty for this offence is imprisonment for a term of not more than three years, a fine of not more than ₦7 million, or both.

Possession or use of hardware, software or other tools used to commit cybercrime

Yes. It is an offence under Section 28 (2) of the Cybercrimes Act for any person who, with intent to commit an offence under the Act, has in his possession any device or program used in committing a cybercrime.

The maximum penalty for this offence is imprisonment for a term of not more than two years, a fine of not more than ₦5 million, or both such fine and imprisonment.

Identity theft or identity fraud (e.g. in connection with access devices)

Yes, Section 22 (1) of the Cybercrimes Act makes its an offence for any person who is engaged in the services of any financial institution and, as a result of acquired special knowledge, commits identity theft of an employer, staff, service providers and consultants with the intent to defraud. Upon conviction of such person, he/she shall be sentenced to seven years' imprisonment, a fine of ₦5 million, or both.

Furthermore, Section 22 (2) – (4) makes it an offence for any person who:

1. 22(2) fraudulently or dishonestly makes use of the electronic signature, password, or any other unique identification feature of any other person;
2. 22(3) fraudulently impersonates another entity or person, living or dead, with intent to: (a) gain advantage for himself or another person; (b) obtain any property or an interest in any property; (c) cause disadvantage to the entity or person being impersonated or another person; or (d) avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice; or
3. 22(4) make or cause to be made, either directly or indirectly, any identity theft or impersonation, or false statement as to a material fact in writing, knowing it to be false and with intent that it can 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.

The maximum penalty for these offences is imprisonment term of not more than five years, a fine of not more than ₦7 million, or both such fine and imprisonment.

Examples of the prosecution of this offence

On 2 September 2024, the Kaduna Zonal Command of the EFCC secured the conviction and sentence of Manasseh Hamza Bello before a judge of the Kaduna State High Court. He was prosecuted for falsely presenting himself as Domingos Pereira (a white man) on Facebook, which representation he knew to be false, in order to fraudulently extort money from his victims.[7]

On 28 August 2024, the EFCC arrested a four-man syndicate of alleged fraudsters impersonating and blackmailing the executive chairman of the Commission in a $1 million deal. The alleged fraudsters contacted the former Nigerian Ports Authority's ("NPA") Managing Director, Mr Mohammed Bello-Koko, falsely claiming that he was implicated in bogus EFCC investigations from his tenure. Upon receiving intelligence about the impersonators' actions, EFCC operatives were dispatched to engage with the alleged fraudsters. The suspects were successfully apprehended and are currently in EFCC custody. They will be charged in court once the investigation is completed.[8]

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes. It is an offence under Section 9 of the Cybercrimes Act for any person who unlawfully destroys or aborts any electronic mail or processes through which money and or valuable information is being conveyed. The maximum penalty for this offence is seven years in the first instance and upon second conviction, 14 years' imprisonment.

Furthermore, Section 11 of the Cybercrimes Act makes it an offence for any 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 up the messages with a view to cause an omission or commission that may defeat the essence of such messages. Such person, if found guilty, is liable to imprisonment for three years, a fine of ₦1 million, or both.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Although, Nigerian law does not specifically address unsolicited penetration testing, individuals or organisations can be prosecuted for such activities under Section 6 (3) of the Cybercrimes Act.

According to Section 6 (3) of the Act, anyone who unlawfully gains access to a computer with the intent to commit a crime using any device to evade detection or conceal their identity can face a penalty of imprisonment for a term of not more than seven years in prison, a fine of not more than ₦7 million, or both, upon conviction.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Other activities include:

1. Cyberstalking: it is an offence under Section 24 (1) of the Cybercrimes Act for any person to knowingly or intentionally send a message or other matter by means of

computer systems or networks 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. The maximum punishment for this offence is a fine of not more than ₦7 million or imprisonment for a term of not more than three years, or both such fine and imprisonment.

2. Cybersquatting: it is an offence under Section 25 (1) of the Cybercrimes Act for any person to, intentionally take or make 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 Governments 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. The maximum punishment for this offence is imprisonment for a term of not more than two years, a fine of not more than ₦5 million, or both such fine and imprisonment. The Court is also empowered to give an order directing the offender to relinquish such registered name, mark, trademark, domain name, or other word or phrase to the rightful owner.
3. Cyber terrorism: it is an offence under Section 18 of the Cybercrimes Act for any person to access or cause to be accessed, any computer or computer system or network for purposes of terrorism. Such person is liable on conviction to life imprisonment.
4. Manipulation of ATM/POS Terminals: it is an offence under Section 30 of the Cybercrimes Act for any person to manipulate an ATM or Point of Sales ("POS") terminals with the intention to defraud. Such person shall be liable upon conviction to five years' imprisonment, a ₦5 million fine, or both.
5. Breach of confidence by service providers: it is an offence under Section 29 of the Cybercrimes Act for any person or organisation that is a computer-based service provider and or vendor to carry out any act with the intent to defraud and, by virtue of his position as a service provider, forge illegally used security codes of the consumer with the intent of gaining any financial and or material advantage or with intent to provide less value for money in his or its services to the consumer. If the corporate organisation is found guilty, it shall be liable to a fine of ₦5 million and forfeiture of further equivalent of the monetary value of the loss sustained by the consumer.

1.2 Do any of the above-mentioned offences have extraterritorial application?

Yes, the Cybercrimes Act has extraterritorial application. Section 50 of the Act grants the Federal High Court of Nigeria the authority to adjudicate offences committed both within and beyond the country's borders.

2 Cybersecurity Laws

2.1 *Applicable Laws*: Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents.

This may include, for example, data protection and e-privacy laws, trade secret protection laws, data breach notification laws, confidentiality laws, and information security laws, among others.

a. The 1999 Constitution of the Federal Republic of Nigeria (as amended) ("CFRN").
b. The Cybercrimes (Prohibition and Prevention, Etc.) Amendment Act, 2024.
c. Nigeria Data Protection Act, 2023 ("NDPA").
d. Nigeria Data Protection Regulation, 2019 ("NDPR").
e. Nigeria Data Protection Regulation Implementation Framework, 2020.
f. The Advance Fee Fraud and other Related Offences Act, 2006 ("AFF").
g. Terrorism (Prevention and Prohibition) Act, 2022.
h. The Economic and Financial Crimes Commission (Establishment, etc.) Act, 2004.
i. The Money Laundering (Prevention and Prohibition) Act, 2022.
j. Nigerian Communications Communication Act, 2003.
k. The NCC Guidelines for the Provision of Internet Service.
l. Nigeria Bar Association Cybersecurity Guideline, 2024.
m. Designation and Protection of Critical National Information Infrastructure Order, 2024.
n. Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions, 2022.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Yes. Section 10 of the Cybercrimes Act makes it unlawful for any person being employed by or under a Local Government of Nigeria, private organisation or financial institution with respect to working with any critical infrastructure or emails, to commit any act that he is not authorised to do by virtue of his contract of service or intentionally permit tampering with such computer. A person found guilty of this offence is liable to pay a fine of ₦2 million or imprisonment for three years.

Also, paragraph 7 of the Designation and Protection of Critical National Information Infrastructure Order, 2024, which is an extension of the Cybercrimes Act, provides that any person, who: (a) without authorisation, and for fraudulent purposes, accesses in whole or in part, or tampers with any Critical National Information Infrastructure ("CNII"); (b) intentionally, or for fraudulent purposes, commits an act, which, directly or indirectly, hinders or interferes with the performance or functioning of a CNII; or (c) commits an unlawful act against any CNII, therefore commits an offence, and is liable to such penalties as may be prescribed in Part 3 of the Cybercrimes Act.

In the same vein, Article 2 (a) of the Nigeria Bar Association Cybersecurity Guideline, 2024 requires members of the Nigeria Bar Association ("NBA") (lawyers) to implement and maintain appropriate cybersecurity measures to protect client information against unauthorised access, disclosure, alteration, or destruction.

Additionally, Article 5 of the Guidelines for Internet Service Providers ("ISPs") require them to ensure that users are informed of any statements of cybercrime prevention or acceptable Internet use published by the Commission or any other authority.

Section 137 (2) of the Nigeria Communications Act, 2003 also grants a Communications Licensee power to deny any other Licensee access to its network facilities or right-of-way on a non-discriminatory basis where there is insufficient capacity, or for reasons of safety, security, reliability, or difficulty of a technical or engineering nature.

2.3 *Security measures*: Are organisations required under Applicable Laws to take specific security measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Yes. Article 5 of the Nigeria Bar Association Cybersecurity Guideline, 2024 requires lawyers and legal organisations to implement secure network configurations to protect against unauthorised access and cyber threats. This includes setting up firewalls and intrusion detection systems and utilising secure network protocols like VPNs for remote access. It also requires lawyers and legal organisations to conduct regular assessments and audits of network configurations to identify and remediate any vulnerabilities. This includes checking for unauthorised devices or access points on the network. Where appropriate, it is required that network should be segmented to ensure sensitive data is isolated from general office networks, as it limits potential exposure in case of a network breach.

Also, paragraph 4 of the Designation and Protection of Critical National Information Infrastructure Order, 2024 provides that the Office of the National Security Adviser ("ONSA") shall, in collaboration with relevant CNII stakeholders, establish a Trusted Information Sharing Network ("TISN") as a multidisciplinary framework, comprising: (a) owners and operators of CNII; (b) representatives from relevant Ministries, Departments, and Agencies of government ("MDAs"); and (c) identified private sector organisations, to (i) build and execute awareness campaigns on risks to CNII, (ii) share information and techniques required to assess and mitigate risks in a decentralised manner across sectors of the economy, and (iii) implement capacity building initiatives to strengthen and mainstream resilience and protection of the infrastructure and networks. Members and entities within the TISN shall also collaborate and share information on threats and vulnerabilities and develop strategies and solutions to mitigate known and evolving risks.

Data controllers and processors are required under Section 39 of the NDPA to implement appropriate technical and organisational measures to ensure the security, integrity and confidentiality of personal data in their possession or under their control, including protections against accidental or unlawful destruction, loss, misuse, alteration, unauthorised disclosure, or access. Such measures include: (a) pseudonymisation or other methods of de-identification of personal data; (b) encryption of personal data; (c) processes to ensure security, integrity, confidentiality, availability and resilience of processing systems and services; (d) processes to restore availability of and access to personal data in a timely manner, in the event of a physical or technical incident; (e) periodic assessments of risks to processing systems and services, including where the processing involves the transmission of data over an electronic communications network; (f) regular testing, assessing, and evaluation of the effectiveness of the measures implemented against current and evolving risks identified; and (g) regular updating of the measures and introduction of new measures to address shortcomings in effectiveness, and accommodate evolving risks.

Organisations are also required under Section 28 of the NDPA, to conduct Data Privacy Impact Assessments ("DPIA") to identify the risks and impact of their envisaged processing of personal data. This assessment involves: (a) a systematic description of the envisaged processing and its purpose, including the legitimate interest pursued by the data controller, data processor, or third party; (b) an assessment of the necessity and proportionality of the processing in relation to the purposes for which the personal data would be processed; (c) an assessment of the risks to the rights and freedoms of a data subject; and (d) the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data, taking into account the rights and legitimate interests of a data subject and other persons concerned.

Additionally, Appendix IV of the Central Bank of Nigeria's ("CBN") Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks ("DMBs") and Payment Service Providers ("PSPs"), provides the minimum controls required for a DMB/PSP to continue to support and provide business services even in the event of cyberattacks. It provides controls on access right management, secure system configuration, cybersecurity awareness, data loss prevention, system life cycle management, vulnerability management, continuous security monitoring, and enhancing incident response capabilities.

Furthermore, Section 12 (1) of the AFF requires any person or entity providing an electronic communications service or remote computing service either by email or any other form to obtain from the customer or subscriber: his full names; residential address, in the case of an individual; and corporate address, in the case of corporate bodies, as a security measure to prevent, detect and combat cyber-related crimes.

2.4 *Reporting to authorities*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes. By virtue of Section 21 (1) of the Cybercrimes Amendment Act, any person or institution, who operates a computer system or a network, whether public or private, must immediately inform the National Computer Emergency Response Team ("CERT") Coordination Centre through their respective sectoral CERTs or sectoral Security Operations Centres ("SOC") of any attacks, intrusions and other disruptions liable to hinder the functioning of another computer system or network, so that the National CERT can take the necessary measures to tackle the issues. In such cases, and in order to protect computer systems and networks, the National CERT Coordination Centre may propose the isolation of affected computer systems or network pending the resolution of the issues. See Section 21 (2) Cybercrimes Act.

Section 40 (2) of the NDPA requires data controllers or process, within 72 hours of becoming aware of a data breach

incident, to notify the Nigeria Data Protection Commission ("NDPC") of such breach.

Also, on an annual basis, data controllers/processors that process the personal data of more than 2,000 data subjects in the preceding 12-month period are required to file an audit report of their data protection practices not later than 15 March of the following year to the NDPC. See Reg. 4.1 (7) of the NDPR.

In the same vein, Article 4.3 of the Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions 2022 requires a report of the cybersecurity self-assessment signed by the Chief Information Security Officer ("CISO") to be submitted every year on or before 31 March to the director and Other Financial Institutions Supervision Department of the CBN. Other Financial Institutions ("OFIs") are also required to promptly report all potential cyber-threats to their information assets, to the director.

2.5 *Reporting to affected individuals or third parties*: Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

Yes. Under Section 40 (3) of the NDPA, when a personal data breach is likely to pose a high risk to the rights and freedoms of a data subject, the data controller must promptly notify the affected subjects in clear and straightforward language. This notice should include advice on steps the data subject can take to mitigate any potential adverse effects. If direct communication would involve disproportionate effort or cost, or is not feasible, the data controller may instead issue a public notice through widely used media channels that is likely to reach the data subject.

2.6 *Responsible authority(ies)*: Please provide contact details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

a. The NDPC is responsible for enforcing the provisions of the NDPA and NDPR.
b. The Nigerian Communications Commission ("NCC") is responsible for enforcing the provisions of the Guidelines for the Provision of Internet Service.
c. The National Security Adviser ("NSA") is responsible for maintaining the National CERT Coordination Centre responsible for managing cyber-incidents in Nigeria.
d. The Attorney General of the Federation ("AGF") supervises the implementation of the Cybercrimes Act, whilst law enforcement agencies are responsible for enforcing the provisions of the Cybercrimes Act.
e. The CBN is responsible for regulating the activities of financial institutions in Nigeria.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

Under Section 21 (3) of the Cybercrimes Amendment Act, any person or institution who fails to report any such incident to the National CERT within 72 hours of its detection, commits an offence and shall be liable to denial of internet services. Such persons or institution shall, in addition, pay a mandatory fine of ₦2 million into the National Cyber Security Fund.

Under the NDPA, where a data controller/processor is in breach after conclusive investigations, the NDPC may issue a Compliance and/or Enforcement Order in line with the Act and Regulations to curtail any further breach. Such Orders may include but are not limited to the following: payment of monetary damages; revocation of regulator-issued operational licences; closure of business operations; ordering the data controller or data processor to account for the profits realised from the violation; and issue public notice to warn the public to desist from patronising or doing business with the affected party.

Also, Section 48 (2) (d), (3), (4) and (5) of the NDPA provides that an enforcement order made, or sanction imposed shall include, amongst others, the ordering of the data controller or data processor to pay a penalty or remedial fee that may be an amount up to the higher maximum amount, in the case of a data controller or data processor of major importance; or standard maximum amount, in the case of a data controller or data processor not of major importance. The "higher maximum amount" shall be the greater of (a) ₦10 million, and (b) 2% of its annual gross revenue in the preceding financial year, whichever is greater. The "standard maximum amount" shall be the greater of (a) ₦2 million, and (b) 2% of its annual gross revenue in the preceding financial year, whichever is greater.

Furthermore, under Reg. 2.10 of the NDPR, any person who is found to be in breach of the data privacy rights of any data subject shall be liable, in addition to any other criminal liability, to the following: (a) in the case of a data controller dealing with more than 10,000 data subjects, payment of the fine of 2% of annual gross revenue of the preceding year or payment of the sum of ₦10 million, whichever is greater; and (b) in the case of a data controller dealing with less than 10,000 data subjects, payment of a fine of 1% of the annual gross revenue of the preceding year or payment of the sum of ₦2 million, whichever is greater.

2.8 *Enforcement*: Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In July 2024, following a joint investigation conducted by the Federal Competition and Consumer Protection Commission ("FCCPC") and NDPC, a penalty of $220 million and a reimbursement fee of $35,000 was imposed on WhatsApp LLC and Meta Platforms, Inc., for violations of the Federal Competition and Consumer Protection Act ("FCCPA") and the NDPR. The investigation was initiated based on evidence of abuse of consumer rights under the FCCPA and the NDPR and consumer feedback that WhatsApp's updated privacy policy, which became effective on 15 May 2021, was imposed on Nigerian users in a manner that did not comply with applicable standards of fairness.[9]

In August 2024, the NDPC imposed a hefty fine of ₦555.8 million on Fidelity Bank PLC for violating its customers' data privacy rights. Fidelity Bank PLC was found to have breached the NDPR and the NDPA. The fine, which amounts to 0.1% of the bank's annual gross revenue for 2023, is the largest ever issued by the NDPC.[10]

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
There is no universal legislation mandating specific software that organisations must use to protect their IT systems. Instead, organisations are free to implement any effective measures they deem appropriate. However, regulatory bodies like the NCC have established cybersecurity units, such as the NCC Computer Security Incident Response Team ("CSIRT"), which regularly issue updates and publications to warn the public about malicious software used by cybercriminals for fraud.[11]

Also, the NPF established a cybersecurity unit, which is the National Police Force – National Cybercrime Centre ("NPF–NCCC"). This unit was established with a direct response to the escalating global threat of cybercrime in Nigeria, to prevent, detect, and investigate cybercrimes.[12]

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
See our response above.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
See our response above.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber attacks?

Yes. Section 39 of the Cybercrimes Act provides that 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, 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 and/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.

Also, Section 4 of NCC's Lawful Interception of Communications Regulations, 2019 makes it lawful for any Authorised Agency (such as the ONSA and the State Security Services) to intercept any communication, pursuant to any legislation in force, where: (a) the interception relates to the use of a Communications Service provided by a Licensee to persons in Nigeria; or (b) the interception relates to the use of a Communications Service provided by a Communications Licensee to a person outside Nigeria, provided that the Licensee shall not be liable in any civil or criminal proceedings for damages, including punitive damages, loss, cost or expenditure suffered or to be suffered, either directly or indirectly, for any act or omission done in good faith in the performance of a duty imposed under paragraphs (a) or (b) of this regulation.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber attacks?

We are not aware of any restrictions in this regard.

However, Section 28 (1) of the Cybercrimes Act makes it illegal for any 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 the 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 the 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 utilised for the purpose of violating any provision of the Act.

4 Specific Sectors

4.1 Do legal requirements and/or market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Yes, in Nigeria, legal requirements and/or market practices related to information security do vary across different business sectors. While there are overarching laws such as the **NDPA** and the **Cybercrimes Act**, certain sectors have specific regulatory frameworks or practices that address information security in more detail as indicated in the responses in questions 2.2 and 4.2. Many organisations, especially in highly regulated sectors like **banking/finance** and **telecommunications**, tend to exceed the minimum cybersecurity requirements by adopting international standards such as **ISO/IEC 27001** and **Payment Card Industry Data Security Standard** ("PCI DSS"). Also, **multi-factor authentication** ("MFA"), while not mandated by law across all sectors, has become a standard practice in industries dealing with sensitive customer data. Some businesses in Nigeria, particularly those with multinational operations, implement **cross-border data protection measures** that comply not only with Nigerian law but also with international laws such as the **EU's General Data Protection Regulation** ("GDPR"). Overall, the legal landscape in Nigeria provides a baseline for information security, but market practices, particularly in more advanced sectors, often exceed these legal requirements to mitigate risks more effectively.

4.2 Excluding the requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services, health care, or telecommunications)?

Yes, there are specific laws, regulations and guidelines applicable to specific sectors in relation to cybersecurity. Financial

Institutions are bound by the Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions 2022 recently issued by the CBN. The Framework contains cybersecurity programmes and mechanisms designed to combat modern cyberattacks faced by those financial institutions. The Framework also provides the minimum level of cybersecurity for all OFIs in Nigeria.

Also, the Terrorism (Prevention and Prohibition) Act, 2022 makes salient provisions for curbing cybercrimes in financial institutions. Section 84 (1) of the Act mandates financial institutions or designated non-financial institutions to forward reports of suspicious transactions relating to terrorism, terrorism financing, or proliferation financing to the to the Nigeria Financial Intelligence Unit ("NFIU") within 24 hours.

The National Health Act 2014 is the principal legislation regulating the Nigerian healthcare sector. Section 26 (1) of the NHA provides that "*all information concerning a user, including information relating to his or her health status, treatment or stay in a health establishment is confidential*". The Act creates a secrecy obligation binding the officials and other employees of the scheme.

The NCC Guidelines for Internet Services Providers contains provisions governing cybercrime in the telecommunication sector. It requires ISPs to ensure that users are informed of any statements of cybercrime prevention or acceptable internet use published by the Commission or any other authority, and that failure to comply with these acceptable use requirements may lead to criminal prosecution.

The AFF Act imposes an obligation on telecommunication providers or ISPs to register with the EFCC and failure to comply might result in criminal prosecution.

5 Corporate Governance

5.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' or officers' duties in your jurisdiction?

Section 282 of the Companies and Allied Matters Act 2020 imposes a fiduciary relationship on a director of a company toward the company's actions. These duties include duty of care, skills and diligence. In fulfilling such duties, directors and officers must ensure appropriate governance is exercised by the company over cybersecurity risks and adequate and appropriate measures must be put in place.

Principle 11 of the Financial Reporting Council of Nigeria's Nigerian Code of Corporate Governance 2018 imposes a duty on directors to provide oversight and supervision of Information Technology ("IT") governance within the organisation. This means that directors have a responsibility to ensure that the company's IT-related practices, policies, and compliance with IT governance standards are in order. It is part of their fiduciary duty to act in the best interests of the company and its stakeholders, which includes overseeing various aspects of corporate governance, including IT governance. The Code recommends the creation of a Risk Management Committee ("RMC" or the "Committee") by the Board of Directors to manage all aspects of the company's risks. The duties of the RMC are detailed in Part A, Principle 11.5.6 of the Code.

Sections 29 and 39 of the NDPA stipulate the obligations of a data controller and data processer (company) to include ensuring effective data security by implementing appropriate technical and organisational measures to prevent, mitigate, manage and respond to data breaches and security incidents. Section 53 of the NDPA provides that principal officers are deemed culpable of their company's actions that are determined as offences or breach of provisions of the Act unless the officers can prove that the offence was committed without their consent or connivance and the officers exercised diligence to prevent the commission of the offence.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Yes, Article 2.4.18 of the Risk-Based Cybersecurity Framework and Guidelines for Other Financial Institutions 2022 provides that: (a) every OFI is required to appoint a CISO who shall be primarily responsible for the day-to-day cybersecurity activities; (b) OFIs are mandated to develop a written Incident Response Policy with stakeholders that regulates cyber incidents in the institution; (c) OFIs are required to conduct regular Cybersecurity Resilience assessments and internal audits to mitigate the risk exposure and ascertain the adequacy of the cybersecurity measures in place; and (d) OFIs must perform penetration tests and/or vulnerability assessments before taking informed decisions on cyber-threat intelligence.

Reg. 22 of NITDA's Public Key Infrastructure Regulations requires accredited certification authorities to implement an incident management plan that must at least provide for the management of the following incidents: compromise of key; penetration of certification authority system and network; unavailability of infrastructure; and fraudulent registration and generation of certificates, certificate suspension and revocation information.

Furthermore, Section 32 of the NDPA and Article 3.4 of the NDPR Implementation Framework require all data controllers/processors to appoint a Data Protection Officer ("DPO") with expert knowledge of data protection laws and practices to assist the organisation in adopting relevant technical and organisational measures/practices to prevent data breach incidents and ensure regulatory compliance, provide regular advisories to top management, members of staff and relevant third parties on their obligations under the NDPA and NDPR and on all matters related to privacy and data protection, serve as the contact person for data subjects and the regulatory body, etc.

Additionally, Article 11 of the Nigeria Bar Association Cybersecurity Guideline, 2024 requires lawyers and legal organisations to form an incident response team responsible for managing cybersecurity incidents. This team should have clear roles, responsibilities, and procedures for responding to incidents. Also, Article 13 of the Guideline requires lawyers and legal organisations to conduct thorough assessments of the cybersecurity measures of third-party vendors before engaging them. This includes evaluating their data protection practices, incident response capabilities, overall security posture, verifying the credentials, certifications, and reputation of third-party vendors by checking for compliance with industry-standard cybersecurity practices and any past security breaches or incidents.

6 Litigation

6.1 Please provide details of any civil or other private actions that may be brought in relation to any Incident and the elements of that action that would need to be met. Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Civil or other private actions that may be instituted in relation to cybercrime incidents include: negligence (proof of duty of care, breach of duty, causation, and damages); breach of contract; and data breach/violation incident.

Upon the occurrence and publicity of a cyber incident, affected persons could also bring a class action either against such organisation (victim of the cyber incident) and/or regulatory agencies/tier of government having supervisory oversight with respect to cybersecurity compliance. Class actions may be based on a multiplicity of legal possibilities including breach of fiduciary duty (where top executives are found to be dishonest) and other express or implied contractual terms (where the victim organisation specifically undertakes to take reasonable steps to forestall a data breach, or where the service supplier-client relationship involves an express or implied duty of privilege, confidentiality, and careful handling of personal information), negligence on the part of either/both the organisation and the government, violations of relevant laws including the NDPA, the Companies and Allied Matters Act, the FCCPA, etc.

Under Section 51 of the NDPA, a data subject who suffers injury, loss, or harm because of a violation of the data protection law by a data controller or data processor, may recover damages from such data controller or data processor in civil proceedings. Notwithstanding anything to the contrary, Section 52 of the NDPA and the Cybercrime Act provides that the Court may also make an order of forfeiture against a convicted data controller, data processor, or individual in accordance with the Proceeds of Crime (Recovery and Management) Act.

Also, an affected person whose right has been violated can institute an action for the enforcement of his/her fundamental human rights under Sections 37 and 39 of the 1999 Constitution.

Yes. The potential for tort liability may arise depending on the particulars of the incident. They may include negligence, invasion of privacy, conversion, personal injury, defamation, etc. Liability in negligence could occur where a data controller fails to take proper care to ensure the security of personal data, and that failure results in damages to a data subject.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

The case of *Julius v FRN* (2021) LPELR -54201 (CA), was an appeal against the judgment of the Federal High Court in Nigeria, wherein the trial court convicted and sentenced the defendant pursuant to the provisions of the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015. The defendant was charged with seven counts of offences related to computer forgery, fraud, cyberstalking, cybersquatting, racism, and xenophobia, and was found guilty of disseminating unverified information on his Facebook page with the intent to deceive the public and cause mayhem in the state. The appellate court upheld the decision of the trial court and confirmed the defendant's sentence of three years' imprisonment or a fine of ₦7 million by adopting the lone issue of the respondent, on whether the trial court rightly convicted and sentenced the appellant under the Cybercrimes (Prohibition, Prevention, etc.) Act, 2015.

In an ongoing action and enforcement order issued by the NDPC to Fidelity Bank PLC, a Financial Institution in Nigeria, the NDPC announced in August 2024 that, following an investigation into violations of the NDPA and NDPR, Fidelity Bank had been found guilty of data breach and violation of the provisions of the law. The Commission reviewed the data-processing activities following a complaint received from a data subject whose personal data was collected and processed without lawful basis for the purposes of opening an account for the data subject. At the conclusion of the investigation, the Commission found that, in certain critical cases, the bank processed personal data without the informed consent of the data subjects and the data-processing tools such as cookies and banking apps were deployed in violation of the NDPA. The bank also relies on some non-compliant third-party data processors and did not provide a requisite, satisfactory remedial plan. The Commission ordered Fidelity Bank PLC to pay a sum of ₦555.8 million, being only 0.1% of the bank's annual gross revenue in 2023.

In July 2024, following a joint investigation conducted by the FCCPC and the NDPC, a penalty of $220 million and a reimbursement fee of $35,000 was imposed on WhatsApp LLC and Meta Platforms, Inc. for violations of the FCCPA and the NDPR. The investigation was initiated based on evidence of consumer abuse under the FCCPA and NDPR and consumer feedback that WhatsApp's updated privacy policy, which became effective on 15 May 2021, was imposed on Nigerian users in a manner that did not comply with applicable standards of fairness.

7 Insurance

7.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

In Nigeria, there are very few operational insurance companies that offer insurance policies to protect organisations from IT-related risks. However, from a close reading of the provisions of the Insurance Act, 2003, the Act does not expressly prohibit the creation of such policy. Section 2 (5) of the Act provides that an insurer may be authorised to transact any new category of miscellaneous insurance business if he shows evidence of adequate reinsurance arrangement in respect of that category of insurance business and requisite capital where necessary and other conditions as may be required from time to time. Section 16 of the Act similarly provides a framework for approval of a new product introduced into any class or category of insurance business. Although there are no specific laws or regulations that prohibit or prevent organisations from obtaining cyber insurance, it is within an organisation's prerogative to take out insurance for risks that could affect the continuity of their business, which may include cybercrime incidents.

7.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

We are not aware of such limitations under Nigerian law.

7.3 Are organisations allowed to use insurance to pay ransoms?

There are no laws governing this kind of insurable risk in Nigeria. In practice, some insurance companies have policies that cover these types of incidents. Unlike what is obtainable in other jurisdictions, ransomware attacks that require organisations to use insurance to pay ransoms have not yet been exploited in Nigeria.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. anti-terrorism laws) that may be relied upon to investigate an Incident.

Under Section 45 (1) of the Cybercrimes Act, 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 a related crime investigation into matters like cyber terrorism. Such warrant confers on the law enforcement officer the investigatory powers to: (i) search any person or conveyance found on any premises or place that such authorised officers are empowered to enter and search; (ii) seize, remove and detain anything which is, or contains evidence of the commission of an offence; (iii) 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; (iv) use any technology to decode or decrypt any coded or encrypted data contained in a computer into readable text or comprehensible format; and (v) require any person having charge of or otherwise concerned with the operation of any computer or electronic device in connection with an offence to produce such computer or electronic device.

Section 58 of the NDPA empowers the NDPC to apply *ex-parte* to a Judge in Chambers for the issuance of a warrant for the purpose of obtaining evidence in relation to an investigation. The warrant may be issued by the Judge upon satisfaction that: (a) a person engaged or intends to engage in a conduct that contravenes the provisions of the NDPA; (b) the warrant is sought to prevent the commission of an offence under the NDPA; (c) the warrant is sought to prevent interference with investigative process under the NPDA; (d) the warrant is for the purpose of investigating data security breaches and data privacy breaches, or obtaining electronic evidence; or (e) the person named in the warrant is preparing to commit an offence under the NDPA. Such issued warrant shall therefore authorise the NDPC, in the company of a law enforcement officer, to enter and search any premises where a suspected, alleged, reported or investigated offence has been committed.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

There are no specific requirements for this under applicable laws in Nigeria; however, law enforcement authorities may have access to such backdoors or encryption keys if the need arises to secure, amongst others, the prevention, investigation, detection, prosecution, or adjudication of a criminal offence or the execution of a criminal penalty, prevention or control of a national public health emergency or for the purposes of national security.

9 International Compliance

9.1 How do international compliance regimes impact country-specific cybersecurity rules?

International compliance regimes profoundly influence Nigeria's cybersecurity laws, rules and regulations by driving the adoption of global best practices and standards. For instance, international frameworks like ISO/IEC 27001 (for information security management) and PCI DSS have become standards that Nigerian organisations aim to align with, particularly in sectors like banking, financial technology and telecommunications. These standards ensure that Nigerian businesses can operate within the global digital economy and meet the security expectations of international partners and customers. While Nigerian laws such as the Cybercrimes Act and the NDPA provide foundational requirements, compliance with these global frameworks often prompts companies to go beyond local laws to achieve higher levels of cybersecurity.

For example, international compliance regimes like the GDPR have had a ripple effect on Nigerian cybersecurity and data protection laws. Although the GDPR is not directly applicable in Nigeria, Nigerian companies that interact with European entities or process the personal data of EU citizens must ensure that their cybersecurity practices meet the requirements of the GDPR. This has influenced the NDPA, which adopts many similar principles, such as data subject rights, breach notification requirements, and cross-border data transfer rules. As a result, Nigerian organisations are aligning their cybersecurity measures not only with local laws but also with international regulations to ensure smooth cross-border operations.

10 Future Developments

10.1 How do you see cybersecurity restrictions evolving in your jurisdiction?

Cybersecurity restrictions in Nigeria are likely to evolve toward stricter regulations and enhanced enforcement as cyber threats become more sophisticated. The Nigerian government in collaboration with its MDAs will likely introduce sector-specific cybersecurity frameworks, particularly in critical sectors like finance, telecommunications, energy and technology. Global collaboration with foreign partners to combat cross-border cybercrime will increase, especially with the deployment of new technologies. Additionally, Nigeria may adopt stricter penalties for non-compliance, expand its focus on data security, and promote public-private partnerships to strengthen national cyber resilience.

10.2 What do you think *should* be the next step for cybersecurity in your jurisdiction?

The Nigerian government is urged to adopt a multifaceted approach to strengthening legal, organisational, and technical frameworks across all sectors. One of these is enhancing **data protection and privacy enforcement**. Stricter and broader enforcement of administrative and compliance orders is needed to comply with the NDPA, as individuals and companies should be held responsible for their actions or omissions in complying with it.

Another crucial step is introducing **sector-specific cybersecurity regulations** for industries such as healthcare and

e-commerce. These sectors face unique challenges and risks, so developing tailored cybersecurity standards that address their specific needs is essential. Nigeria can improve cybersecurity resilience in its most vulnerable sectors by implementing industry-specific frameworks.

Investments in **cybersecurity education and training programs** will help create a skilled workforce capable of addressing emerging threats. It will also promote the development of cybersecurity research and innovation, ensuring that Nigeria remains proactive in tackling cyber threats and keeping pace with global technological advancements.

Endnotes

1 https://punchng.com/fraudsters-hack-companys-server-steal-n435-3m/

2 https://punchng.com/two-students-arraigned-for-hacking-mtn-computers/

3 https://www.efcc.gov.ng/efcc/news-and-information/news-release/10327-abuja-court-jails-four-internet-fraudsters-in-abuja

4 https://www.efcc.gov.ng/efcc/news-and-information/news-release/10345-efcc-arrests-48-suspected-internet-fraudsters-in-umudike

5 https://bit.ly/3RsKVIM

6 https://www.interpol.int/en/News-and-Events/News/2020/Three-arrested-as-INTERPOL-Group-IB-and-the-Nigeria-Police-Force-disrupt-prolific-cybercrime-group

7 https://www.efcc.gov.ng/efcc/news-and-information/news-release/10347-kaduna-court-jails-internet-fraudster

8 https://www.efcc.gov.ng/efcc/news-and-information/news-release/10344-1million-fraud-efcc-arrests-syndicate-impersonating-olukoyede

9 https://www.dataguidance.com/news/nigeria-fccpc-fines-meta-and-whatsapp-220m-fccpa-and

10 https://www.channelstv.com/2024/08/21/fidelity-bank-fined-n555-8m-by-ndpc-for-data-breach/

11 https://ncc.gov.ng/technical-regulation/cybersecurity#projects-activities-3

12 https://nccc.npf.gov.ng/page/about-us



John C. Onyido is a highly experienced legal practitioner with a specialisation in Intellectual Property ("IP") Law. He has a proven track record of representing renowned multinational companies in securing and enforcing their intellectual property rights ("IPRs") in Nigeria and is well versed in all aspects of IP maintenance and enforcement mechanisms in the country. He heads the IP & Technology Department of S.P.A. Ajibade & Co. and is currently overseeing the Telecommunications Regulatory and Data Protection & Privacy Units. John is an IP law specialist and has also garnered considerable experience and expertise in the field of Data Privacy & Protection Law as well as Telecommunications Regulatory Advisory.

S.P.A. Ajibade & Co.
Suite 201, SPAACO House
27A Macarthy Street, Onikan, Lagos
Nigeria

Tel: +234 803 220 4371
Email: jonyido@spaajibade.com
LinkedIn: www.linkedin.com/in/johnchikeonyido



Franklin Okoro is a legal practitioner and an Associate with the IP & Technology, Data Privacy & Protection and Telecommunications Departments of S.P.A. Ajibade & Co., where he routinely advises clients on a wide range of IPRs, Privacy, Data Protection, and Telecommunications regulatory issues. Franklin generally advises high-net-worth companies on: Privacy & Data Protection and Telecommunications' regulatory requirements, registration, enforcement, rights transfers, and portfolio management of trademarks; copyright-related issues; and commercialisation, registration, renewal, assignment and licensing of patents and designs in Nigeria, OAPI, ARIPO and other jurisdictions.

S.P.A. Ajibade & Co.
Suite 201, SPAACO House
27A Macarthy Street, Onikan, Lagos
Nigeria

Tel: +234 706 054 1804
Email: fokoro@spaajibade.com
LinkedIn: www.linkedin.com/in/franklin-mark-okoro-a4ab77a2



Maryam Abdulsalam is an enthusiastic legal practitioner with zeal for Corporate & Commercial Law. Her professional and core interests include local and international legal and regulatory frameworks that cuts across Intellectual Property & Technology Law, Data Privacy & Protection. As an Associate in S.P.A. Ajibade & Co.'s IP & Technology Law Department, Maryam routinely advises local and international clients on IPRs and IP law, Data Privacy & Protection issues and compliance requirements under the relevant data protection legislations in Nigeria and telecommunications services.

S.P.A. Ajibade & Co.
Suite 201, SPAACO House
27A Macarthy Street, Onikan, Lagos
Nigeria

Tel: +234 903 967 5389
Email: mabdulsam@spaajibade.com
LinkedIn: www.linkedin.com/in/maryamabdulsalam



Pelumi Adeyeye is an Associate Trainee in the IP & Technology and Telecommunications Departments at S.P.A. Ajibade & Co. Pelumi's practice involves conducting thorough legal research on IP, Data Privacy and Telecommunications matters, and handling advisory services to support client needs. Pelumi had previously served as an intern at F.O. Fagbohungbe & Co, and Falana and Falana Chambers, where he developed practical experience in the legal field before becoming joining S.P.A. Ajibade & Co. Pelumi earned his Bachelor of Laws degree (LL.B.) from Afe Babalola University, Nigeria, in 2022, and his professional licence from the Nigerian Law School, Lagos in 2024.

S.P.A. Ajibade & Co.
Suite 201, SPAACO House
27A Macarthy Street, Onikan, Lagos
Nigeria

Tel: +234 703 215 0506
Email: padeyeye@spaajibade.com
LinkedIn: www.linkedin.com/in/pelumi-adeyeye-216668127

S.P.A. Ajibade & Co. is a leading Corporate & Commercial law firm based in Nigeria. Established in 1967, it has been at the forefront of developments in commercial practice in Nigeria and has continuously rendered sound technical advice and tailored customer solutions to its local and international partners. To our clients, S.P.A. Ajibade & Co. is a reliable partner and trusted counsel in various transactions and dispute resolution processes. We see our duty to our client as that of not just providing excellent technical advice, but also providing solutions that address and enhance a client's purpose and business objective. Over the last five decades, S.P.A. Ajibade & Co. has garnered an impressive track record of providing first-class specialised services in the areas of Commercial Dispute Resolution, Capital Market Law & Practice, Corporate Finance, Corporate Structuring & Restructuring, IP & Technology, Data Privacy & Protection, Telecommunications, Energy, Real Estate and Probate.

www.spaajibade.com

SPA Ajibade & Co.
Legal Practitioners, Arbitrators and Notaries Public

iclg International Comparative Legal Guides

The **International Comparative Legal Guides** (ICLG) series brings key cross-border insights to legal practitioners worldwide, covering 58 practice areas.

Cybersecurity 2025 features two expert analysis chapters and 21 Q&A jurisdiction chapters covering key issues, including:

- Cybercrime
- Cybersecurity Laws
- Preventing Attacks
- Specific Sectors
- Corporate Governance
- Litigation
- Insurance
- Investigatory and Police Powers
- International Compliance
- Future Developments



The International Comparative Legal Guides are published by: glg Global Legal Group