ICLG

The International Comparative Legal Guide to:

Cybersecurity 2018

1st Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Allen & Overy
Angara Abello Concepcion Regala & Cruz Law Offices
Baker McKenzie
Boga & Associates
BTG Legal
Christopher & Lee Ong
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
ENSafrica
Erkelens Law
Eversheds Sutherland
Holland & Hart LLP
JIPYONG
Josh and Mak International
King & Wood Mallesons
Lee, Tsai & Partners Attorneys-at-Law
Maples and Calder
MinterEllison
Mori Hamada & Matsumoto
Niederer Kraft & Frey Ltd.
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Shibolet & Co.
Simmons & Simmons LLP
Udo Udoma & Belo-Osagie

glg
global legal group

global legal group

Contributing Editors
Nigel Parker & Alex Shandro, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
October 2017

ISBN 978-1-911367-77-2
ISSN 2515-4206

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Nigeria

Olajumoke Lambo

Udo Udoma & Belo-Osagie

Godson Ogheneochuko

1 Criminal Activity

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

Yes, the activities listed below constitute offences under the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015 ("Cybercrimes Act").

Hacking (i.e. unauthorised access)

It is an offence, under Sections 6 and 8 of the Cybercrimes Act, for any person to intentionally and unlawfully access a computer system. The punishment depends on the fraudulent action that is committed by the offender after access is gained, but the maximum penalty is seven years' imprisonment or a fine of =N=7,000,000.00 or both.

In July 2017, it was reported that four persons had been charged by a court for the alleged hacking of the website of the West African Examinations Council.

Denial-of-service attacks

This is an offence under Section 8 of the Cybercrimes Act. The maximum punishment is imprisonment for a term of two years and a fine of =N=5,000,000.00. We are not aware of any prosecution for denial-of-service attacks.

Phishing

This is punishable under Sections 32(1) and 36(1) of the Cybercrimes Act. The punishment is three years' imprisonment or a fine of =N=1,000,000.00 or both.

In 2012, prior to enactment of the Cybercrimes Act, the Federal High Court sentenced a 25-year-old undergraduate to 20 years' imprisonment on four counts, including an attempt to obtain money by false pretence, which is an offence under the Criminal Code Act in Nigeria.

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

This is an offence under Section 32(3) of the Cybercrimes Act. The punishment is three years' imprisonment or a fine of =N=1,000,000.00 or both.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

This is a breach of Section 28 of the Cybercrimes Act. The punishment is imprisonment for a maximum term of three years or a fine of not more than =N=7,000,000.00 or both.

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

Section 22 of the Cybercrimes Act makes this an offence. Depending on the circumstances of the offence, the maximum punishment is seven years' imprisonment or a =N=5,000,000.00 fine or both.

In June 2017, the Economic and Financial Crimes Commission ("EFCC") arraigned a suspect for impersonating the former Chairman of the EFCC.

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

This is not expressly specified as an offence, but Section 31 of the Cybercrimes Act will be breached if an employee does not relinquish access rights and codes to the employer without lawful reason. The punishment is three years' imprisonment or a fine of =N=3,000,000.00 or both.

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

Yes. Some of which include:

Wilful misdirection of electronic messages: maximum punishment of three years' imprisonment or a fine of =N=1,000,000.00 or both (Section 11 of the Cybercrimes Act).

Computer-related forgery: maximum punishment is imprisonment of three years or a fine of not less than =N=7,000,000.00 or both (Section 13 of the Cybercrimes Act).

Computer-related fraud: the punishment varies depending on the specific crime, but the maximum punishment is a prison term of seven years and a fine of =N=10,000,000.00 (Section 14 of the Cybercrimes Act).

Fraudulent issuance of e-instructions by persons charged with the responsibility of using a computer or other electronic devices for financial transactions is an offence under Section 20 of the Cybercrimes Act. The maximum punishment is seven years' imprisonment.

Cyberstalking: depending on the circumstances, the maximum punishment is 10 years' imprisonment or a minimum fine of =N=25,000,000.00 (Section 24 of the Cybercrimes Act).

Cybersquatting: the maximum punishment is two years' imprisonment or a maximum fine of =N=5,000,000.00 or both a fine and imprisonment (Section 25 of the Cybercrimes Act).

Manipulation of ATM/POS terminals by persons with intent to defraud is an offence under Section 30 of the Cybercrimes Act. The punishment is five years' imprisonment or a =N=5,000,000.00 fine or both. In addition, any employee of a financial institution found

to have connived with another person to perpetrate fraud using an ATM/POS device shall be guilty of an offence and upon conviction sentenced to seven years' imprisonment without an option of a fine.

Electronic cards-related fraud is an offence under Section 33 of the Cybercrimes Act. The maximum punishment for a wide range of offences under this Section is seven years' imprisonment and/or a fine of not more than =N=10,000,000.00.

Failure by an organisation to implement cybersecurity measures

A service provider (defined as: "(i) 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 (ii) any other entity that processes or stores computer data on behalf of such communication service or users of such service") is required by Section 40 of the Cybercrimes Act to comply with a Judge's order 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" and to generally assist with the identification, apprehension and prosecution of offenders. Any service provider that contravenes this Section commits an offence and shall be liable on conviction to a fine of not more than =N= 10,000,000.00. Directors, officers and managers of the service providers may also be held liable and imprisoned for a maximum term of three years or a maximum fine of =N=7,000,000.00 or both.

Section 37 of the Cybercrimes Act will also be breached where a financial institution executes customers' electronic transactions without conducting KYC checks.

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

The provisions of the Cybercrimes Act apply only in Nigeria, but where an offence is committed outside Nigeria and the victim of the offence is a citizen or resident of Nigeria or the alleged offender is in Nigeria and not extradited to any other country for prosecution, the Federal High Court will have jurisdiction over the matter. (Section 50 (1) of the Cybercrimes Act.)

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

No, there are no actions that might mitigate any penalty or constitute an exception.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Under Section 5 of the Terrorism Prevention Act 2011 (as amended) (the "TPA"), any person who knowingly, in any manner, directly or indirectly solicits or renders support for the commission of an act of terrorism or to a terrorist group, commits an offence and is liable on conviction to imprisonment for a term of not less than 20 years. Support is defined to include incitement to commit a terrorist act through the internet, or any electronic means.

2 Applicable Laws

2.1 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, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import / export controls, among others.

- The Cybercrimes (Prohibition, Prevention, Etc.) Act 2015.
- The Terrorism Prevention Act 2011 (as amended).
- Guidelines for the Provision of Internet Service ("NCC Internet Service Guidelines") issued by the Nigerian Communication Commission ("NCC").

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, how (and according to what timetable) is your jurisdiction expected to implement the Network and Information Systems Directive? Please include details of any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Yes. An order by the President, designating certain computer systems, computer networks, computer programs, computer data or traffic data as critical infrastructure, may prescribe minimum standards, guidelines, rules or procedure regarding the protection, preservation, transfer and control of such data (Section 3 of the Cybercrimes Act).

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Service providers and financial institutions are required to keep appropriate records, conduct the relevant checks and safeguard the confidentiality of data. As mentioned previously, service providers must also provide lawful assistance to law enforcement authorities. Licensees of the NCC may also be required by the NCC to acquire interception capabilities for interception of certain information.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import / export controls of encryption software and hardware.

None that we are aware of.

2.5 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 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 (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Yes. Any person or institution that operates a computer system or a network must immediately (i.e. no later than seven days after the occurrence) report any attacks, intrusions and other disruptions that could hinder the functioning of another computer system or network to the National Computer Emergency Response Team Coordination Center ("CERT"). To the best of our knowledge, the information provided to the CERT is not published.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

There are no restrictions in the Cybercrimes Act, but it is advisable for financial institutions to notify the Central Bank of Nigeria ("CBN") of the intention to engage in such information sharing before doing so.

2.7 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.

There are no requirements for affected individuals to be informed of any Incidents, but, in our opinion, the individuals are owed a duty of care and should be informed if the potential impact of an Incident can be mitigated by actions that may be taken by the affected person, e.g. stolen passwords, compromised accounts, etc.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

No, the responses do not change.

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The law enforcement authorities in collaboration with the Office of the National Security Adviser ("NSA") are responsible for enforcing the provisions of the Cybercrimes Act, while the NCC is responsible for enforcing the provisions of the NCC Internet Service Guidelines. With respect to the Terrorism Prevention Act 2011, the Attorney-General of the Federation supervises the implementation and administration of the Act, while the law enforcement and security agencies are responsible for the enforcement of the Act.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

Please see our responses to questions 2.3 to 2.8 above.

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

We are not aware of any enforcement actions that have been taken for non-compliance with the above-mentioned requirements.

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Market practice with respect to information security does not significantly vary across different business sectors in Nigeria. The Cybercrimes Act prescribes the minimum standards that are applicable across all business sectors in Nigeria and incorporates, within its ambit, data protection/information security. It was passed into law in 2015 to provide the much-needed legislation to govern the growing menace of cybercrimes and it also sought to consolidate all other sector-specific regulations that have cybercrimes provisions into one cohesive legislation.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

(a) Obligations imposed on financial institutions:

(i) Sections 19 and 37 of the Cybercrimes Act require financial institutions to:

- not vest a single employee with both posting and access authorisation rights;
- implement effective counter-fraud measures to safeguard customers' sensitive information;
- verify the identity of customers carrying out electronic financial transactions before the issuance of cards and other related electronic devices;
- apply KYC principles on customers before executing customers' electronic transfer, payment, debit and issuance orders; and
- provide clear legal authorisation of any unauthorised debit on a customer's account or reverse such debit within 72 hours.

(ii) In addition, banks and other financial institutions are required by Section 44 of the Cybercrimes Act to contribute a levy of 0.005% of all electronic transactions

carried out by them into the National Cybersecurity Fund (the "Fund").

(iii) Section 14 of the TPA places an obligation on financial institutions to report suspicious transactions relating to terrorism to the Financial Intelligence Unit within 72 hours of such transactions. The TPA defines "acts of terrorism" to include an act which is deliberately done with malice aforethought and which involves or causes destruction to a government or public facility, a transport system, an infrastructure facility, including an information system. This obligation arises when the financial institution has sufficient reason to suspect that the funds involved in the transaction:

- are derived from legal or illegal sources, but are intended to be used for any act of terrorism;
- are proceeds of a crime related to terrorist financing; or
- belong to a person, entity or organisation considered as a terrorist or a terrorist organisation.

(iv) All banks and payment service providers are mandated by the CBN to maintain a dedicated fraud desk to provide support to customers on electronic fraud and block or place restrictions on customers' accounts upon receipt of fraud complaints, etc.

(b) Obligations of telecommunications companies:

(i) Based on the definition stated previously, companies in the telecommunications sector fall within the category of entities described as 'service providers'. They are thus required to:

- preserve, hold or retain any traffic data, subscriber information, non-content information, and content data, at the request of the relevant regulatory authority or any law enforcement agency; and
- comply with any request by a law enforcement agency for the release of any information kept by the service provider.

(ii) In addition, telecommunications companies are required by Section 44 of the Cybercrimes Act to contribute a levy of 0.005% of all electronic transactions carried out by them into the Fund.

(iii) Section 40 of the Cybercrimes Act also mandates all service providers (which include telecommunications companies) to disclose information requested by any law enforcement agency or otherwise render assistance howsoever in any inquiry or proceeding under the Act.

4 Corporate Governance

4.1 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' duties in your jurisdiction?

If a company that is a computer-based service provider or vendor does any act with intent to defraud and, by virtue of its position as a service provider, forges or illegally uses security codes of customers to gain a financial or material advantage, it would be a breach of a director's duty if commission of the offence resulted from his connivance, instigation or neglect.

The failure by a service provider to comply with the terms of Section 40 of the Cybersecurity Act (discussed in response to question 1.1 above) could also result in criminal liability for a director or other officers of the company.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (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?

Financial institutions are required to conduct regular checks to ensure the integrity of the networks and computer systems, in addition to maintaining a dedicated fraud desk to provide support to customers on electronic fraud and block or place restrictions on customers' accounts upon receipt of fraud complaints, etc.

Service providers must report any cyber attacks or similar actions to the CERT. There are no requirements in the cybersecurity regulations for designation of a Chief Information Security Officer.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

Please see our response to question 2.5 regarding mandatory reports to the CERT.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

No, companies are not subject to any other specific requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The laws governing cybersecurity in Nigeria do not contain provisions for civil actions that may be brought for Incidents, but a court may grant civil remedies to a victim and against a convict in a criminal action (such as compensation or an order of restitution). A victim of an Incident, could also, under general common law principles, file a civil action after the criminal action has been concluded. The type of civil action that may be brought will depend on the type of wrong that has been committed. For instance, a victim of an Incident that results from a contractual relationship could bring an action for breach of contract or confidentiality/duty of care and seek damages. The victim must, however, prove that a valid contract existed between the parties and the contract has been breached.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

Please see our response to question 1.1 above.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

There is potential liability in tort, depending on the nature of the Incident.

6 Insurance

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

There are no laws that prohibit or restrict organisations in Nigeria from taking out insurance against Incidents, neither are there any laws that make it mandatory for them to do so.

6.2 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?

No, there are no regulatory limitations to insurance coverage against specific types of loss.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

There are no specific requirements under the Cybercrimes Act in relation to the monitoring of employees for the purpose of preventing, detecting, mitigating and responding to Incidents. There are also no specific requirements regarding the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer.

Several sections of the Cybercrimes Act, however, set out specific actions of employees of government organisations and private organisations that constitute offences under the Act. These include:

(i) committing an act which the employee is not authorised to do by virtue of his contract of service or intentionally permitting or tampering with computers;

(ii) intentionally hiding or detaining any electronic mails, messages, electronic payment, credit and debit card found by the employee or delivered to him in error and which to his knowledge ought to be delivered to another person;

(iii) diverting electronic mails with intent to defraud; and

(iv) conniving with other persons to perpetrate fraud using computer systems or a network, automated teller machines or point-of-sales devices.

In addition, all employees in the public and private sectors are mandated to surrender all codes and access rights to their employers immediately upon disengagement from their employment.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

No, there are no such Applicable Laws.

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. antiterrorism laws) that may be relied upon to investigate an Incident.

Section 41 of the Cybercrimes Act provides that the office of the NSA shall be the coordinating body for all security and enforcement agencies under the Act.

Section 39 of the Cybercrimes Act empowers a Judge to order a service provider to intercept, collect or record content data or traffic data associated with specified communications transmitted by means of a computer where there are reasonable grounds to suspect that the content of such electronic communication is reasonably required for the purposes of a criminal investigation or proceedings. The Judge may also authorise a law enforcement officer to collect or record such data through application of technical means.

In addition, Section 45 of the Cybercrimes Act provides that 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.

Under the TPA, Section 24 provides that the NSA or the Inspector General of Police may apply to the court for the issuance of a warrant for the purposes of a terrorism investigation. Such warrant may authorise the NSA or the Inspector General of Police to enter any premises, search and seize any relevant materials found in the premises.

In order to issue this warrant, the court must be satisfied that the warrant is sought for the purpose of a terrorist investigation and there are reasonable grounds for believing that there is material on the premises which may be relevant to the terrorist investigation.

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?

Please see our response to questions 1.1 and 2.3 above regarding the obligations imposed by Section 40 of the Cybercrimes Act and the NCC's power to require its licensees to acquire interception capabilities.

Under the TPA, law enforcement agencies also have the power to apply for a court order to compel communication service providers to intercept specified communications, provided that they obtain the requisite approvals of the Attorney-General and the NSA. A Judge could also, by an order, require a telecommunications provider to intercept and retain specified communication received or transmitted by that service provider, or authorise the relevant law enforcement agency to enter any premises and install and subsequently remove any device with which a communication or communications of a specified description may be intercepted and/or retained, for purposes of intelligence gathering.

Olajumoke Lambo
Udo Udoma & Belo-Osagie
St. Nicholas House (10th & 13th floors)
Catholic Mission Street
Lagos
Nigeria

Tel: +234 1 4622 308-10
Email: jumoke.lambo@uubo.org
URL: www.uubo.org

Mrs. Jumoke Lambo, a Partner, heads the Business Advisory unit of the firm and is the co-head of the firm's Telecommunications team. She also oversees the firm's company secretarial practice. Commended in *Who's Who Legal* 2012 as one of Nigeria's foremost Corporate/M&A lawyers, she has over two decades of experience in telecommunications law, employment law, immigration law and general corporate practice with an emphasis on legislative drafting, mergers and acquisitions, foreign investment, corporate restructuring, regulatory compliance and due diligence. Her specialisations include foreign investment, communications, employment law, capital market transactions and regulatory compliance.

She has assisted various operators within and outside the telecommunications and broadcasting sectors with establishing and doing business in Nigeria. She also advises a variety of investors with acquisitions of interests in Nigerian companies and regulatory compliance.

Her work has also been noted in the *International Financial Law Review*'s Expert Guides. She is a fellow of the Centre for International Legal Studies ("CILS") and sits on the Board of Advisors for the Lazarski LL.M. Programme, a partnership between the Lazarski University of Warsaw, Poland and the CILS. She is a member of the Nigerian National Committee of the International Lawyers for Africa.

She has written and presented papers on a wide range of topics.

Godson Ogheneochuko
Udo Udoma & Belo-Osagie
St. Nicholas House (10th & 13th floors)
Catholic Mission Street
Lagos
Nigeria

Tel: +234 1 4622 308-10
Email: godson.ogheneochuko@uubo.org
URL: www.uubo.org

Mr. Godson Ogheneochuko is a Senior Associate in the firm with specialisations in a range of corporate matters including telecommunications, acquisitions, aviation and real estate transactions. He is a core member of the team that advises telecommunications operators in all areas of their operations including acquisition of licences and other telecommunications assets, real property acquisitions and leasing, data protection and interception of communication.

He is a core member of the team that advises multinational telecommunications operators in all areas of their operations including regulatory compliance and real property acquisitions. As part of his telecommunications practice, he advises and represents various clients in negotiations with regulatory authorities, and assists with procuring operational and regulatory permits relevant to their businesses and transactions in Nigeria. In addition to his work in the practice areas mentioned above, Godson regularly advises the firm's clients in connection with cybersecurity, the collection, processing, storage and transfer of personal information under the applicable laws in Nigeria.

Godson has been a contributor to the *World Bank Doing Business Reports* ("Registering Property in Nigeria") since 2009, the *International Law Office Newsletters* (Telecoms and Media) from 2012–2014, and the *International Comparative Legal Guide to: Telecoms, Media and Internet Laws and Regulations* since 2013.

UDO UDOMA & BELO-OSAGIE

Udo Udoma and Belo-Osagie ("UUBO") has been described in international rankings as one of Nigeria's "Magic Triangle" law firms – a description underscored by one of the highest ratios of internationally-recognised partners per firm in the Nigerian legal market. As a firm, we seek to provide timely, practical, sophisticated and responsive legal solutions based on a philosophy of consistently striving to structure accessible, commercially-oriented advice tailored to the needs of each client.

Although a full-service firm, we are especially well regarded in our niche specialisations which include: private equity; energy, electric power and natural resources; banking, finance and capital markets; corporate restructuring (including mergers and acquisitions); project finance; foreign direct investments; telecommunications; taxation; and labour and employment. Together with our litigation, alternative dispute resolution and company secretarial departments, we are able to provide proactive and cost-effective legal services throughout Nigeria and to clients outside Nigeria.

The firm was awarded the title of law firm of the year in 2014 by *Who's Who Legal* and has been ranked in Tier 1 by the *Chambers and Partners* ranking for its Banking and Finance and Corporate Commercial Practice. Over the years, the firm has been consistently ranked in Tier 1 by the *IFLR 1000* rankings in at least three practice areas including Capital Markets, Mergers and Acquisitions, and Banking and Project Finance practices. In the latest rankings, UUBO was ranked Tier 1 in the Banking, Capital Markets and Mergers and Acquisitions practices.

Current titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com