ICLG

The International Comparative Legal Guide to:

Cybersecurity 2019

2nd Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Angara Abello Concepcion Regala & Cruz Law Offices
Bagus Enrico & Partners
Boga & Associates
BTG Legal
Christopher & Lee Ong
Cliffe Dekker Hofmeyr Inc
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Ferchiou & Associés
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.
JIPYONG LLC
King & Wood Mallesons
Latham & Watkins LLP
Lee, Tsai & Partners Attorneys-at-Law
LT42 – The Legal Tech Company
Maples and Calder
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Simmons & Simmons LLP
Siqueira Castro Advogados
Stehlin & Associes
Synch
Templars
USCOV | Attorneys at Law

glg
global legal group

glg
global legal group

Contributing Editors
Nigel Parker & Alexandra Rendell, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Sam Friend

Senior Editors
Suzie Levy
Caroline Collingwood

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 2018

ISBN 978-1-912509-38-6
ISSN 2515-4206

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Nigeria

Ijeoma Uju

Templars

Ijeamaka Nzekwe

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:

Hacking (i.e. unauthorised access)

Yes. The Cybercrimes (Prohibition and Prevention etc. 2015) Act (the "Cybercrimes Act") makes it an offence for any person, without authorisation, to intentionally access in whole or in part a computer system or network with the intent of obtaining computer data, securing access to any program and commercial or industrial secrets or classified information.

Maximum penalty: imprisonment for a term of not more than seven years or a fine of not more than N7,000,000.00, or both such fine and imprisonment.

In June 2018, a suspected fraudster was arraigned before a Lagos Magistrate's Court for allegedly conniving with another suspect, to hack into the mobile app account of Eco Bank Plc and unlawfully withdrawing the sum of N207,000,000.00.

Denial-of-service attacks

Denial-of-service is covered by section 8 of the Cybercrimes Act, which makes it an offence for any person to intentionally commit an act without lawful authority which causes the serious hindering of the functioning of a computer system by inputting data which prevents the computer system from functioning in accordance with its intended purpose.

Maximum penalty: imprisonment for a term of not more than two years or a fine of not more than N5,000,000.00, or both such fine and imprisonment.

Phishing

Under the Cybercrimes Act, anyone who attempts to acquire sensitive information such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication through emails or instant messaging either in the form of an email from what appears to be your bank asking a user to change his or her password or by revealing his or her identity so that such information can later be used to defraud the use, is liable to three years' imprisonment or a fine of N1,000,000.00, or both.

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

Yes. The Cybercrimes Act makes it an offence for any person to engage in malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in public, private or financial institution's computers. Such a person is liable to three years' imprisonment or a fine of N1,000,000.00, or both.

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

Under the Cybercrimes Act, it is an offence for any person who, with intent to commit an offence under the Act, has in his possession any device, including a computer program, a computer password, access code or similar data by which a computer system or network is capable of being accessed for the purpose of committing an offence under the Act.

Maximum penalty: imprisonment for a term of not more than two years or a fine of not more than N5,000,000.00, or both such fine and imprisonment.

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

The Cybercrimes Act provides that any person who is engaged in the services of any financial institution, and as a result of his special knowledge commits identity theft of its employer, staff, service providers and consultants with the intent to defraud is guilty of an offence and upon conviction shall be sentenced to seven years' imprisonment or a fine of N5,000,000.00, or both.

On August 1, 2018 the EFCC (Kaduna Branch) secured the conviction of one accused on a charge bordering on impersonation, forgery and obtaining by false pretence.

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

The Cybercrimes Act makes it an offence for any person employed by or under the authority of any bank or other financial institutions to divert electronic mails with intent to defraud.

Maximum penalty: imprisonment for a term of not more than five years or a fine of not more than N7,000,000.00, or both such fine and imprisonment.

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. Child pornography: the maximum punishment is imprisonment for a term of 10 years or a fine of not more than N20,000,000.00, or both such fine and imprisonment.
2. Cyberstalking: the maximum punishment is a fine of not more than N7,000,000.00 or imprisonment for a term of not more than three years, or both such fine and imprisonment.
3. Cybersquatting: the maximum punishment is imprisonment for a term of not more than two years or a fine of not more than

N5,000,000.00, or both such fine and imprisonment. The court may also make an order directing the offender to relinquish such registered name, mark, trademark, domain name, or other word or phrase to the rightful owner.

4. Racist and xenophobic offences: the maximum penalty is imprisonment for a term of not more than five years or a fine of not more than N10,000,000.00, or both such fine and imprisonment.
5. Importation and fabrication of E-Tools: the maximum penalty is imprisonment for a term of not more than three years or a fine of not more than N7,000,000.00, or both.
6. Breach of confidence by service providers: the maximum punishment is a fine of N5,000,000.00 and forfeiture of further equivalent of the monetary value of the loss sustained by the consumer.
7. Manipulation of ATM/POS terminals: the maximum penalty is five years' imprisonment or a fine of N5,000,000.00, or both.

Failure by an organisation to implement cybersecurity measures

Yes. The Advance Fee Fraud Act ("the AFF Act") provides that a failure of providers of any internet services to register with the Economic and Financial Crimes Commission ("EFCC") is an offence and is liable on conviction to imprisonment for a term of not less than three years without an option of a fine, and in the case of a continuing offence, a fine of N50,000 for each day the offence persists.

The Cybercrimes Act provides that any person or institution who fails to report an Incident to the National Computer Emergency Response Team ("CERT") within seven days of its occurrence commits an offence and will be liable to denial of internet services, in addition to payment of a mandatory fine of N2,000,000.00.

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

Yes, the offences under the Act have extraterritorial application.

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 to the above offences.

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.

Yes, there are. The AFF Act provides that a person who is in possession of a document containing a false pretence commits an offence if he knows or ought to know, having regard to the circumstances of the case, that the document contains the false pretence. "Document" is defined under the Act to include a document transmitted through an electronic or electrical device.

Also, Section 5 of the Terrorism Prevention Act 2011 (as amended) (the "TPA") provides that 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.

1. The Cybercrimes (Prohibition and Prevention etc.) Act 2015.
2. The Advance Fee Fraud and other Related Offences Act 2006.
3. The Terrorism Prevention Act 2011, as amended.
4. The NCC Guidelines for Internet Service Providers.
5. Draft Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers 2018.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction is anticipated to exceed the requirements of the Directive.

Yes. The Cyber Crimes Act provides that any person who, being employed by or under a Local Government of Nigeria, private organisation or financial institution with respect to working with any critical infrastructure, electronic mails, commits any act which he is not authorised to do by virtue of his contract of service or intentionally permits tampering with such computer, is guilty of an offence and is liable to a fine of N2,000,000.00 or imprisonment for three years.

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.

Yes. Under the AFF Act, in order to prevent cyber fraud, any person or entity providing an electronic communication service or remote computing service either by e-mail or any other form is required 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.

The NCC Guidelines for Internet Service Providers Guidelines (the "NCC Guidelines") also provide that Internet Service Providers ("ISPs") must 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 NCC Guidelines also provide that ISPs must take reasonable steps to: inform users regarding proper email practices; ensure that users are updated regarding any changes to applicable laws or regulation; inform users of the consequences of acting contrary to proper email practices; and inform users of methods of reducing unsolicited email, including the availability of SPAM filters or similar services and the ISP's SPAM reporting and complaints procedures.

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.

We are not aware of any conflict of laws issues.

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. The Cybercrimes Act provides that any person or institution, who operates a computer system or a network, whether public or private, must immediately inform the (CERT) Coordination Center 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.

Also, if an ISP receives notification that any of its services have been used for the transmission of unsolicited communications contrary to these Guidelines, including the transmission of SPAM email, the ISP is required to take reasonable steps to notify the responsible user and describe the prohibited activity. If the prohibited activity is ongoing or serious, the ISP shall suspend or terminate the user's account (as provided for in paragraph 7 of the above), and shall report the activity to any responsible regulatory or law enforcement agency.

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?

The Applicable Laws do not restrict organisations from sharing information related to Incidents.

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 under Applicable Laws to report information related to Incidents or potential Incidents to affected individuals.

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 Nigerian Communications Commission (the "NCC") is responsible for enforcing the provisions of the Guidelines for the Provision of Internet Service.

The National Security Adviser ("NSA") is responsible for maintaining the (CERT) Coordination Center responsible for managing cyber Incidents in Nigeria.

The Attorney General of the Federation ("the AGF") supervises the implementation of the Cybercrimes Act, whilst law enforcement agencies are responsible for enforcing the provisions of the Cybercrimes Act and the TPA.

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

The AFF Act makes it an offence punishable with a fine of N100,000 and forfeiture of the equipment or facility used in providing the service for any person or entity providing electronic communication service or remote computing service to fail to obtain the stipulated details from its customer or subscriber.

The penalty under the Cybercrimes Act is stated in question 1.1 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 action taken in cases of 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.

No, market practice does not vary across different business sectors.

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) In the financial services sector: the Central Bank of Nigeria (the "CBN") recently issued a draft Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers (the "Draft DMB Guidelines").

The Draft DMB Guidelines provide for several specific legal requirements including: establishment of an information security steering committee by Deposit Money Banks ("DMBs") and Payment Service Providers ("PSPs") that shall be responsible for the governance of their cybersecurity programme; periodic review by the Compliance Department of DMBs and PSPs of their cybersecurity programmes and processes; and internal audit of DMBs/PSPs' cybersecurity programmes by an internal audit unit.

The Cybercrimes Act also requires financial institutions to verify the identity of its customers carrying out electronic financial transactions by requiring the customers to present documents bearing their names, addresses and other relevant information before the issuance of ATM cards, credit cards, debit cards and other related electronic devices.

(b) In respect of the telecommunications sector, the NCC Guidelines also require 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.

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?

There are no specific circumstances provided by the Applicable Laws whereby failure by a company to prevent, mitigate, manage or respond to an Incident amounts to a breach of directors' duties. However, every director owes a duty to exercise a degree of care, diligence and skill which a reasonable director would exercise. Hence, a failure to prevent or mitigate an Incident by a company may amount to a breach of duty by a director of the company if the director had not taken reasonable steps to prevent such Incident.

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?

The Draft DMB Guidelines provide that DMBs/PSPs must:

- appoint a CISO;
- ensure consistent conduct of risk assessments, vulnerability assessments and threat analysis to detect and evaluate risk to the DMB/PSP's information assets and determine the appropriateness of security controls in managing risk; and
- update cyber risk assessments regularly to address changes or introduction of new technologies, products, etc., before deployment to ensure accurate risk measurement.

The Guidelines also require DMBs and PSPs to develop an Incident response policy with stakeholders which will stipulate, among others, the creation of a cyber Incident response plan.

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)?

See the response in question 2.5.

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 other specific requirements under Applicable Laws except to the extent that the draft DMB Guidelines make specific provisions for DMBs and PSPs.

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 Applicable Laws do not make any specific provision for civil actions that may be brought in relation to an Incident. However, a victim could institute an action in court in respect of a civil wrong done to him simultaneously with or after a criminal action and the court may in its discretion grant civil remedies to the victim in respect of the Incident. The civil action to be instituted will be determined by the nature of the Incident that has been committed. For example, where a contractual relationship exists, the victim of the Incident could prove breach of contract or negligence to claim relief from the courts. For example, the draft DMB Guidelines provide for the minimum baseline security measures to be put in place by DMBs and PSPs. Where an Incident results from non-adherence to the provisions of the Guidelines by DMBs and PSPs (when the guidelines are eventually issued), the victim who has incurred damage or loss may bring a civil action on the ground of the implied duty of care owed by the DMBs/PSPs.

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

See our responses to question 1.1 above.

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

Depending on the nature of the Incident, there is potential liability in tort.

6 Insurance

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

There are no laws prohibiting organisations from taking out insurance against Incidents in Nigeria.

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?

Currently, there are no regulatory limitations to insurance coverage against specific types of loss under Nigerian law.

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?

The Cyber Crime Act has no direct provision or requirement in relation to the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents. In the same vein, there are no direct requirements for the reporting of cyber risk, security flaws, Incidents or potential Incidents by employees to their employer.

However, we note that the draft DMB Guidelines stipulate that the management of DMBs and PSPs is obligated to conduct background checks on employees who implement policies, and conduct procedures used to protect sensitive information of the DMBs and PSPs as part of the risk management steps.

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?

There are no such Applicable Laws in this regard.

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.

For the purposes of a criminal investigation or proceeding, the Cybercrimes Act makes provision for 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 system where there are reasonable grounds to suspect that the content of such electronic communication is reasonably required. Further, the Cybercrimes Act makes provision for the Judge to authorise a law enforcement officer to collect or record such data through the application of technical means.

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 crime investigation in relation to Incidents.

Section 24 provides that the NSA or the Inspector General of Police ("IGP") 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 IGP to enter any premises, and search and seize any relevant materials found in such premises.

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 such requirements under Applicable Laws.

Ijeoma Uju
Templars
5th Floor, Octagon Building
13A, A.J. Marinho Drive
Victoria Island, Lagos
Nigeria

Tel: +234 1 4611 294
Fax: +234 1 2712 810
Email: ijeoma.uju@templars-law.com
URL: www.templars-law.com

Ijeoma is a Partner in the Corporate and Commercial practice group. She has over a decade of experience advising clients on day-to-day compliance requirements applicable to the operation of their businesses in various issues, including oil and gas, power, telecommunications, intellectual property, manufacturing, consumer protection, acquisition, sale of property, and labour and employment.

She advises clients on Nigerian law and policy affecting the regulation and operation of businesses in Nigeria, including the establishment of foreign businesses, corporate restructuring, mergers and acquisitions and relations with relevant regulatory authorities.

Ijeoma advises clients on intellectual property exploitation rights, registration, management and assignment/transfer of brands and counterfeiting. She provides advice on trademark and patent infringement rectification processes and jurisdictional constraints and prospects.

Ijeoma also manages the government relations aspect of clients' regulatory compliance, and has led various negotiations and/or engagements undertaken by the firm in this regard.

Ijeamaka Nzekwe
Templars
5th Floor, Octagon Building
13A, A.J. Marinho Drive
Victoria Island, Lagos
Nigeria

Tel: +234 1 279 9396
Fax: +234 1 2712 810
Email: ijeamaka.nzekwe@templars-law.com
URL: www.templars-law.com

Ijeamaka is an Associate in the Corporate and Commercial Group. She graduated from the Obafemi Awolowo University with First Class Honours where she achieved distinctions in commercial law, international law and the law of taxation.

Ijeamaka has gathered myriad of experiences across the different practice areas at the Firm. Particularly she has advised on issues relating to Banking and different financing structures, capital markets, corporate insolvency, mergers and acquisitions, projects and infrastructure, real estate, divestments, foreign direct investments, legal due diligence, regulatory compliance, dispute resolution, business development and general corporate and commercial matters.

Ijeamaka also advises clients on issues relating to the setting up of businesses in Nigeria, labour and industrial relations, as well as Nigerian law and policy affecting the operation of businesses, the establishment of foreign businesses and foreign investments in Nigeria. She also provides corporate governance and compliance advice to clients in connection with local and international transactions.

TEMPLARS

Templars is one of Nigeria's foremost integrated full-service commercial law firms. With offices in key commercial centres, the firm is strategically placed to offer quality legal services to clients across the length and breadth of the country.

At Templars, our strengths lie in our coverage of diverse legal fields, as well as our familiarity with the major sectors of the Nigerian economy. Not only are we well acquainted with domestic and international business transactions, typically involving strategic alliances and complex business arrangements; our lawyers work daily with all kinds and sizes of businesses, to structure, negotiate and document their transactions. We have built a reputation for understanding each client's peculiar business needs, and applying legal principles to craft workable solutions to meet those business objectives. We analyse the risks involved in our clients' transactions, and devise appropriate risk management formulae to assist in the mitigation and hedging of those risks.

At Templars we are always consistent with our commercial approach in the service of our clients, and we constantly employ cost-effective procedures in the pursuit of each mandate.

Other 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
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State 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