BANWO & IGHODALO

Milestone in Electronic Commerce: How the Cybercrimes Act 2015 impacts businesses

INTRODUCTION

Globalisation, a characterising feature of the 21st Century, is fast shrinking the world into a borderless global village. This trend is being facilitated by advancement in technology by which people and information residing miles apart are readily accessible through one or few clicks on a simple digital device, such as a smartphone or the iPad. A new digital revolution is said to be underway in which about 30% of global population is actively living in the cyberspace, in real terms.

Today, virtually all business transactions and other daily human endeavours (teaching, learning, sales and promotional activities, commercial transactions, shopping, procurement, supply, payments, banking, insurance and professional services) take place via online platforms. The world's growing cyberspace is driven by new innovations which are increasingly being aided by modern computer technologies, the Big Data phenomenon and the Internet of Things (**IoT**).

Since activities which, before the computer age, took place only in the physical spheres like land, air and the sea (but are now taking place over the cyberspace) are governed by laws made to handle the peculiar natures of those spaces; it is imperative that cyber laws are enacted in order to cater to the needs of, as well as the problems emanating from, doing business through the cyberspace.

Many advanced countries of the world had long enacted their respective cyber laws. However, online transactions continued in Nigeria for a long time without any specific governing law, thereby posing great risks to individuals, businessmen, organisations and even the government; some of whom in many instances in the past, had fallen victims to cybercrimes without any concrete legal regime for seeking redress. Succour, however, came in May 2015 when the **Cybercrimes (Prohibition, Prevention, etc.) Act 2015** (the **"Cybercrimes Act"**) – was signed into law.

Apart from criminalising certain acts, prescribing punishments for their commission and creating an institutional and enforcement framework, the Cybercrimes Act addresses most of the lacunae which had hitherto rendered the Nigerian cyberspace unsafe for transacting business. However, in addition to potentially improving investors' confidence in the Nigerian e-business environment, the Cybercrimes Act has also generated fresh risk management issues.

This article takes an analytical look at why the enactment of the Cybercrimes Act is considered a milestone in electronic commerce and the potential major impacts it may have on domestic and international commercial transactions undertaken in Nigeria.

PRIOR LEGAL REGIME

A review of the legal regime before the enactment of the Cybercrimes Act can best be done by understanding how electronic/online business transactions fared in the periods before 2011 and

98 Awolowo Road, South-West Ikoyi, Lagos, Nigeria
Afri-Investment House, Plot 2669, Aguiyi-Ironsi Street, Maitama, Abuja, Nigeria
T +234(0) 700LAWYERS F +234(1) 4615205 E banwigho@banwo-ighodalo.com W www.banwo-ighodalo.com

Attorney list at www.banwo-ighodalo.com

thereafter (but before the enactment of the Cybercrimes Act). In the first period (that is, before 2011), no recognition was given to electronic or computer generated documents in our evidential law. The main effect of this situation was that where disputes arose out of commercial deals concluded by e-mails or via online platforms, the computer-generated contract documents were not competent for proving their contents in the court of law (even where they were admitted for "relevancy" sake); as it was not clear whether they should be treated as primary or secondary evidence under the **Evidence Act, Cap. E14, Laws of the Federation of Nigeria, 2004** (the "**Old Evidence Act**").

Besides, there was the challenge of proving the authenticity and/or the identity of the owner of an electronic signature appearing on any computer or online print-out of contractual terms. Under the Old Evidence Act, procedure for proving the sealing of a document required actual "writing" on a tangible medium by the person alleged to have executed such document; so as to examine his signature or finger impression **– see sections 100, 102 and 108 of the Old Evidence Act.** This legislation did not envisage the now widespread use of electronic signature in e-mail transactions, cryptographic codes on internet platforms and biometric system in financial institutions (such as the current use of Bank Verification Number (BVN) in the banking system).

However, the enactment of the **Evidence Act 2011** (the **"New Evidence Act"**) which resulted in substantial improvements on the Old Evidence Act, ushered in the second period of the previous legal regime. **Sections 84 and 93 of the New Evidence Act** provide for the admissibility of computer-generated documents, the recognition of electronic signature and waiver of its proof by means of writing on a tangible medium. This was the first major boost to e-commerce in Nigeria prior to the coming into force of the Cybercrimes Act.

However, despite improvements on the evidential value of electronically-generated documents since 2011, many cybercrimes which undermine the confidence of parties to online transactions and deter, *ipso facto*, the growth of e-commerce still went unchecked. This was due to certain circumstances, including:

(i) the fact that common fraudulent and harmful electronic and internet activities such as scamming, cybersquatting, cyberattack, PIN theft, hacking, phishing etc. were not defined in any statute and therefore were somewhat "unknown" to the Nigerian legal system. It is trite that an action will only constitute a crime in Nigeria where it is stated, by a statute, to be a crime and the penalty thereof is prescribed in a written law **– see section 36(12), Constitution of the Federal Republic of Nigeria 1999, as amended.**

(ii) neither any court with designated jurisdiction to prosecute cybercrimes nor a body with the needed specialised skill and machinery for properly investigating alleged commission of same (other than the Economic and Financial Crimes Commission and the Police Force, which are trained to generally deal with conventional criminal matters) existed.

THE REFORM

The coming into force of the **Cybercrimes Act** changed the Nigerian legal landscape significantly, with the overall effects of better securing and further expanding the scope of e-business transactions. Some of the specific provisions of the Cybercrime Act which are expected to impact investments and general commercial activities in Nigeria include:

1. Creation of the concept of "Critical Infrastructure" (**see section 58 of the Cybercrimes Act**) and the empowerment of the President to designate any computer system as Critical National Information Infrastructure – **see section 3 of the Cybercrimes Act**

2. Presumption of regularity and binding effect of electronic signatures in respect of many common business transactions – **see section 17(1) of the Cybercrimes Act**

3. Creation of new offences by criminalising certain fraudulent activities done through electronic devices and the internet, which were not previously defined as crimes in the country's regular penal laws – **see Part III (sections 5-36), section 46 and generally section 58 of the Cybercrimes Act** – and the creation of both individual and corporate liabilities and penalties such as committal of the directors of affected companies to various terms of imprisonment, as well as imposition of heavy fines on affected organisations.

4. Protection of organisations' copyrights in trademarks and domain names

5. Obligation of business entities to report incidences amounting to cyber threats – **see section 21 of the Cybercrimes Act**

6. Duty of service providers to collaborate with law enforcement agents (including by providing access to data stored) in relation to electronic transactions – **see sections 38, 39 & 40 of the Cybercrimes Act**

7. Establishment of institutions for the enhancement of cybersecurity – **see sections 42 & 44 of the Cybercrimes Act**

8. Obligation of financial institutions to ascertain and secure identities of customers that are provided with "Access Devices" for computer transactions, and the prohibition of the vesting of posting and authorising access in a single employee – **see sections 37 & 19 of the Cybercrimes Act**

9. Provision for a well-coordinated system of administration and enforcement of the cybercrimes law – **see sections 41, 42, 44, 47 & 49 of the Cybercrimes Act**

10. Vesting of jurisdiction to try offences in the Federal High Court and provision for trans-border cooperation on investigation, prosecution and enforcement of court judgements in respect of cybercrimes – **see sections 50, 51 & 52 of the Cybercrimes Act**

WHAT TO EXPECT

Heightened risk management function

Business entities are going to tighten their belts in the area of risk management as it affects corporate information security. This will enhance the sanctity of electronic commercial transactions under the new legal regime because substantial breach of information security will not only affect customers/subscribers but will also be costly for business organisations.

Business organisations such as financial institutions, internet service providers ("**ISPs**") and communication companies, among others, hold critical data of private and corporate citizens in their computer systems/programs or networks which may now be considered as "Critical Infrastructure". Such data are vital to the country, and any incapacity or destruction of, or interference with, such system and assets could have a debilitating impact on national or economic security, national public health and safety, or any combination of those matters.

Where these entities are attacked (or are susceptible to attacks) by cybercriminals in a way that may pose serious threat to the resilience of the financial system as a whole; the President may, on the recommendation of the National Security Adviser, designate such computer systems/programs or networks as constituting Critical National Information Infrastructure ("**CNII**"). Given the level of technical know-how in the country, it is most likely that some business entities may be caught in the CNII web. Any affected company or business would no longer have private control of its computer system or network but would be compelled to take instructions from the government with respect to how the system or network could be accessed or data transferred therefrom.

Another risk issue for business entities is the new position that all electronic signatures on documents (with the exception of certain critical transactions listed under section 17(2) of the Cybercrimes Act) are legally presumed to be valid. The burden of proving that any electronic signature appearing on a document, evidencing a company's transaction or contract, is forged rests squarely on that company. Therefore, it will be imperative for corporate organizations and persons to invest in cybersecurity apparatus and techniques in order to fortify their computer systems/programs against hacking or other electronic identity-theft practices.

A new challenge is created, by the Cybercrimes Act, for business organisations as a result of the obligation imposed on them to report cyber threats on their computer systems. The new position is that all organisations operating a computer system or network must "immediately inform the National

Computer Emergency Response Team's ("National **CERT**") coordination center of attacks, intrusions and other disruptions likely to hinder the functioning of another computer system or network, so that the National CERT can take the necessary measures to tackle the issues; which measures may involve the isolation of such computer system or network till the issues are resolved. Failure to make the report within 7 days of the occurrence of the threats attracts the penalty of internet services denial with the compulsory payment of N2,000,000 into the National Cyber Security Fund ("**NCSF**"). As a result of these new requirements, businesses are going to be faced with the challenge of determining the optimal decision to make when confronted with cyber threats; for instance whether they should (i) immediately report such occurrences to the National CERT, a decision that may have adverse impacts on their operations (e.g. their systems/networks being declared as CNII); or (ii) first attempt to deal with the threat internally before reporting same (a situation that may make them liable to penalties if such internal actions eventually fail)?

Further, ISPs are required to report to relevant authorities or law enforcement agents, when requested, whatever traffic data and subscriber information which they are lawfully required as the case may be to intercept, record, retain and protect. This will be another important risk factor for other business organisations that are clients of the ISPs. It is likely that firms/companies will begin to demand the inclusion in their internet service agreements, clauses that will compel ISPs to notify them whenever any data that relate to their operations are requested by third parties such as law enforcement agents.

Improved confidence, more transactions

There is hope that the new legal regime will boost the confidence of individuals, firms and companies to transact more businesses and render services online, without the fear of falling victims to identity theft, plagiarism or copyright violation. For instance, the Cybercrimes Act criminalises cybersquatting, that is any act which amounts to "the acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name" is an existing and legally registered trademark or is confusingly similar or identical to it; or similar and identical to the name of a person; or acquired without right or with intellectual property in it.

The widespread confidence which the new regime is likely to engender, to the extent that one will most likely be dealing with the real person/entity as represented in any online business proposal, negotiation or actual transaction; should significantly raise the volume of e-business in the country.

The establishment of institutions which are going to work together to enhance cybersecurity in the country should further boost confidence and ultimately result in increase in the volumes of e-commerce. In this connection, the Cybercrimes Act established (i) the Cybercrimes Advisory Council, which is the policy think-tank for coordinating all research and policy issues "relating to the prevention and combating of cybercrimes and the promotion of cyber security in Nigeria"; and (ii) the NCSF which will provide substantial part of the needed capital for financing the country's cybersecurity policy.

The NCSF, by the provisions of **section 44(2)(a) of the Cybercrimes Act,** shall be entitled to receive sums equivalent to 0.005% of all electronic transactions done by certain entities, such as GSM service providers and all telecommunication companies; ISPs; banks and other financial institutions; insurance companies; and the Nigerian Stock Exchange. It is however not clear whether this levy is payable on deals done by these entities themselves or those transacted through their platforms. The accrued amount in the NCSF may be allocated, to the maximum limit of 40%, for executing programs relating to countering violent extremism.

Expansion of coverage and financial inclusion

Although the Central Bank of Nigeria's Know-Your-Customer (KYC) policy has been in force and is being implemented by deposit money banks and other financial institutions for several years, the Cybercrimes Act further mandates all financial institutions to verify the identities of their customers before providing them with any "Access Device" (a list of what constitutes an "Access Device" is contained in section 58 of the Cybercrimes Act) for electronic transactions. Similarly, no employee of a financial institution is to be vested with both posting and authorising access at the same time.

It is expected, that these statutory provisions shall limit the incidences of identity theft; fraud via ATM/POS terminals; and fraudulent issuance of electronic instructions. Invariably, as the cyberspace becomes more secure and also easy to link through simple electronic devices such as the mobile phone; the use of electronic money transfer, mobile banking and other electronic financial services will become almost ubiquitous. One hopes to see more people from the informal sector of the economy and those who are largely regarded as previously 'un-bankable', opening bank accounts and subscribing to financial services through e-platforms.

Increasing commercial litigation

Last (but not the least) of what to expect, is the rise in volume of commercial litigation arising out of contractual disputes. The lack of a specialised statutory regime governing cyber-related contractual agreements in the past, had limited not only the volume of commercial deals concluded electronically but also the number of cases instituted for seeking redress in cases of breaches.

The Federal High Court is now conferred with special powers to try cyber-related offences and the jurisdiction is nationwide. Disputes shall be given speedy trial without room for interlocutory applications for stay of proceedings. Again, the Cybercrimes Act provides for cross-jurisdictional cooperation. This will ensure that investigation of allegations of offences shall enjoy mutual assistance from foreign countries while accused persons, against whom *prima facie* cases are established, and convicted persons in respect of trans-border transactions; shall be liable to extradition. In effect, there will be better guarantee of the sanctity of commercial contracts.

CONCLUSIONS

As cyberattacks are a universal threat with implications that cut across the global financial and economic systems, Nigeria, with its Cybercrimes Act, has moved a step further towards joining the league of cyber-protected markets. The country is also now poised to take advantage of information sharing among nations of the world having cyber-related laws. Expectedly, information will be shared about sophisticated technologies deployed by cybercriminals whose activities include hacking, phishing, spamming, spreading of computer virus, cybersquatting and violent attacks; as well as the mechanisms for combating these crimes.

According to the latest *System Risk Barometer Survey* conducted by The Depository Trust & Clearing Corporation (DTCC) – a US global financial services firm – and reported in the January 2016 issue of The Banker (a publication of the Financial Times of London), "cyber risk remained the number one concern globally among financial service professionals, with 70% of all respondents citing it as a top five risk" in recent years.

With a population that is 170 million strong, and who are fast connecting to one another and to institutions on the internet and social media (about 4 million of this population are said to be very active players already on such electronic/online platforms like Jumia, Konga, Amazon etc. while many more are subscribing to the services of e-payment solution companies like Master Card, InterSwitch, VisaCard and e-transact); the country will become open to e-business much more in the new dispensation.

Though there are concerns that the cost of compliance with the Cybercrimes Act will significantly raise overhead costs for businesses in terms of training, research, and capacity development; the attached benefits of security, reliability, automation, integration, and increased profitability in the long-run make compliance worthwhile. At any rate, doing business in the Nigerian cyberspace is set to experience a paradigm shift, going forward.

The Grey Matter Concept is an initiative of the law firm, Banwo & Ighodalo