**Comment on Good Practices, New Information on National Efforts and Recommendation with regards to the Meeting of the Open-Ended Intergovernmental Expert Group on Cybercrime (Submission from the Nigerian Financial Intelligence Unit (NFIU)).**

## LAW ENFORCEMENT, INVESTIGATIONS, ELECTRONIC EVIDENCE GATHERING AND CRIMINAL JUSTICE IN CYBRCRIMES

1. The emergence of cyber crime has become a major concern for financial institutions, regulatory agencies, financial intelligence units and law enforcement agencies in countries worldwide. Digitisation of payment for services and cross-border transfer of funds, communication, social activities, e-commerce and the emergence of cryptocurrencies or virtual assets were intended to make life easier, however, they have created an environment for money laundering and terrorist financing to thrive as criminals are constantly devising new ways to evade detection. On the internet, there are various channels exploited by criminals to convert 'dirty' money into 'clean' money. Prevalent channels include online banking, online gambling, e-gaming, online auctioning and digital payment methods amongst others. Money laundering now wears the cloak of cyber-laundering, because criminals today are able to access easier non face-to-face channels to launder funds using the internet. Some cybercrimes are both predicate offences to money laundering and also constitute one or more stages of money laundering, hence the shift to cyber-laundering.

2. The cyber domain has transformed businesses, security, collaboration and exchange of information. This has increasingly redefined concern over sensitivity of data, networks and trust issues bordering on monitoring, defence and awareness across a wide variety of users.

As at June 2017, the Nigerian Communications Commission (NCC) recorded a total of 142,654,738 active mobile (GSM) lines with 91,598,757 using internet services in Nigeria. With the spontaneous increase in the number of internet users so does the increase in spate of financial activities thus the increase in over dependence on the cyber space giving rise to more threats and the need to address vulnerabilities.

"As mondaq.com reported on December 3rd, 2018, cyber-attacks across Nigeria resulted in total losses of $649 million in 2017, significantly up from the $550 million it cost in 2016." Also according to Serianu; The Africa Cyber Immersion Centre 2017 report on Nigeria stated that "…cyber attacks cost Nigeria businesses around $649 million a year which includes direct damage plus post attack disruption to the normal course of business".

3. Nigeria is committed to tackling cybercrimes and related threats, safeguard critical information infrastructure, provide adequate legislative framework and encourage collaboration amongst stakeholders. To this end, Nigeria has taken steps to curd cybercrimes through:

a) The creation of the cyber security strategy document which assigns roles to stakeholders. Highlights of the strategy document include the implementation of a legal framework that will allow for the identification and prosecution of cybercrimes, strategies for online child protection, data protection, privacy and lawful interception, and awareness creation to all stake holders. It also introduces a special focus on protecting **critical national information infrastructure (CNII).** The NFIU houses one of the most critical national information infrastructures with over 4TB of data. The National Cyber Security Strategy is up for review in 2020.

b) The passing of the Cyber Crimes (Prohibition, Prevention, Etc) Act 2015, which provides for an effective, unified and comprehensive legal, regulatory and institutional framework for the prohibition, prevention, detection, prosecution and punishments of cybercrimes in Nigeria. The related offences include offences against critical national information infrastructure, system interference, interception of electronic messages, email and electronic money transfers, tempering with critical infrastructures, cyber terrorism, identity theft and impersonation, spamming etc. Other Acts of parliaments include the Advance Fee Fraud and other Fraud Related Offences Act and the Money Laundering Prohibition Act 2012 as amended.

c) The creation of the **Nigerian Computer Emergency Response Team "ngcert"** under the Office of the National Security Adviser is a critical milestone which coordinates other law enforcement agencies across the nation to enhance the fight against cybercrime. "ngcert" also advocates for the creation of localised "cert" teams in order to optimize swift response to incidence reporting as they occur.

d) In June 2018, the Central Bank of Nigeria issued a draft framework regulating minimum requirements to increase cyber security across Payment Service Providers (PSPs) and Deposit Money Banks (DMBs) which was finalised and took effect from 1st January 2019. The framework was developed based on the existing Cybercrime Act of 2015.

e) The Nigerian Communications Commission (NCC) offers monthly national cyber security awareness which is carried out annually in order to create responsiveness towards providing the public with knowledge and safety of the use of internet.

f) The National Information Technology Development Agency (NITDA) is the Nigerian agency vested with the powers and responsibilities of regulating the IT industry with a stand of knowledge base and IT driven economy. Section 6(I) of the act states that "….advise government on methods of promoting the

development of information technology in the country which includes introducing appropriate information technology legislation to enhance national security and the vibrancy of the industry. This section conveys the task to hold on to national security issues as it affects the cyberspace. The establishment of the department of cyber security department of the agency is tasked with issuing guidelines, regulatory frameworks to Ministries, Departments and Agencies (MDAs) in order to further secure the countries cyber space. In this regards NITDA has encouraged all MDAs to establish Cyber Security Desk Officers who will serve as the first point of distress call before escalation to incidence response officers.

g) The Nigerian Financial Intelligence Unit (NFIU) is consistently collaborating with law enforcement agencies (EFCC, NPF (SFU), etc) in provision of proactive intelligence to initiate investigations and providing response to requests to support ongoing investigations involving cybercrimes and other illegal activities. The NFIU also has temporary freezing powers if funds are suspected to be proceeds of illegal activities which include cybercrimes. The NFIU is the central body in Nigeria responsible for requesting, receiving, analysing and disseminating financial intelligence reports and other information to all law enforcement, security and intelligence agencies and other relevant authorities. The Mission of the Unit is to safeguard the Nigerian financial system from the exploitation of financial crimes, and to contribute to the global fight against money laundering, terrorism financing and other related crimes through the provision of credible financial intelligence.

h) The Cybercrime Advisory Council is responsible for advising Government on measures to prevent and combat cybercrimes, threats to national cyberspace and other cyber security related issues.

The function of the council is in line with provision of Sec 43 of the Cybercrime (Prohibition, Prevention, etc) Act, 2015.

Members of the council include the NFIU, Federal Ministry of Justice, Federal Ministry of Finance, Ministry of Foreign Affairs, the Central Bank of Nigeria (CBN), the Economic and Financial Crimes Commission(EFCC), Nigeria Police Force (NPF), Defence Headquarters (DHQ), Nigeria Customs Service (NCS) Galaxy Backbone, National Identity Management Commission (NIMC), NITDA, Defence Intelligence Agency (DIA), ICPC, Department of State Services (DSS), Nigerian Communications Commission (NCC), etc. The Office of the National Security Adviser is the coordinating agency presiding over the Cybercrime Security Council meetings which hold a minimum of four times annually.

## CHALLENGES/OPPORTUNITIES

Despite the counter measures taken against cybercrimes, a number of challenges still exist in the Nigerian cyberspace which are not limited to;

- Relevant stakeholders have limited knowledge on cybercrimes and how to tackle them.
- Law enforcement officers investigating electronic related offences lack the technical skills and also the appropriate technological tools and services to successfully investigate and trace footprints of cybercrime.
- On the use of computer-generated evidence, Section 84 of the Evidence Act, 2011 provides for the admissibility of statements in documents produced by such computer systems. However, the Act still needs further amendment as it does not cover for ways of admission and preservation of digital evidence.
- Rise in virtual assets service providers in the country which are not currently under direct regulation.
- Concealment of the true owners of cryptocurrencies deepening the challenge of establishing beneficial ownership.
- Limited or ineffective inter-agency collaboration
- Limited or ineffective multilateral collaboration amongst the financial intelligence unit, law enforcement agencies, private sector and the judiciary

## RECOMMENDATIONS

- Provision of training and technical assistance in building cyber security skills within the Law Enforcement Agencies to get better understanding of activities of cyber criminals and hands-on with equipment and technologies that are likely to be found at cybercrime scenes.
- The need to have Judges and Law Enforcement Officers that are technically sound in understanding cyber terminologies, appropriately interpreting the law on cybercrimes and keeping up with the trends of cyber environment.
- Corporate training and security certifications are also expected to reduce to the barest minimum vulnerabilities and threats and understanding of cyber-attacks. The need for all sensitive government agencies to undergo Information Security Management Systems (ISMS) or ISO 27001 certifications.
- The need for local and international collaboration between private, governmental and civil society in intelligence and data sharing and other international treaties on cyber security is paramount.
- In view of the pace, ease and occurrence of cyber-laundering, there is need to address the operational responsiveness of the financial

intelligence unit, law enforcement agencies, private sector and the judiciary

- Continuous public awareness on preventive measures against cybercrime.