LAUNCH OF THE CYBER SECURITY DIRECTIVE FOR FINANCIAL INSTITUTIONS

A SAFER DIGITAL FINANCIAL INDUSTRY

SPEECH BY

DR. MAXWELL OPOKU-AFARI,

FIRST DEPUTY GOVERNOR, BANK OF GHANA

BANK OF GHANA HEAD OFFICE, ACCRA

OCTOBER 22, 2018

Honorable Minister of Communications, Mrs. Ursula Owusu-Ekuful,

Second Deputy Governor, Bank of Ghana,

Members of the Board, Bank of Ghana,

Heads of Banks,

Members of the Ghana Association of Bankers,

Members of the Ghana Association of Savings and Loans,

Members of the Ghana Association of Microfinance Institutions,

Members of the Chartered Institute of Bankers,

Staff of Bank of Ghana,

Distinguished Members of the Press,

Ladies and Gentlemen, all protocols observed.

1. Good afternoon Ladies and Gentlemen. It is a pleasure to welcome all of you to the Bank of Ghana and I deem it a great honour for having such august audience joining us for this special occasion. As we are all aware, today marks another significant milestone in the history of Ghana's financial sector as we launch the Cyber Security Directives for Financial Institutions.

2. After careful consideration on issues regarding cyber security and its implications on financial intermediation, the Bank chose the theme "A Safer Digital Financial Industry" to launch the Cyber Security Directives for two main reasons. First, we envisage that this theme will shape the strategic direction in terms of cyber security of the banking industry and to the larger extent, the entire financial sector. And secondly, it signals the collective efforts of stakeholders to address the

canker of cyber threat and all other actions that exploit vulnerabilities of the financial systems and processes.

3. Currently, technology is intertwined with our everyday lives. It is re-defining business processes, promoting greater interconnectedness between countries and peoples, enhancing skill development and innovation, and more broadly, breaking down perceived barriers in every sector. In the banking sector, for instance, technology has taken a center stage in the financial intermediation process. Recently, key developments within the intermediation process include the growing importance of FinTechs in delivering financial services as well as the introduction of electronic payment platforms to enhance interoperability. In effect, the continuous role played by technology has had considerable impact on the operations of financial institutions and

ultimately driven policies aimed at promoting financial inclusiveness for growth and poverty reduction.

4. In all of these developments, financial services remains critical and the Bank of Ghana has established, as a major policy priority, the development of a sound financial system with strong individual component institutions. The idea is to position the sector as a major growth driver, to support an inclusive broad-based economy with the full implementation of new higher minimum capital requirements by the end of this year. We know that banks are working strenuously to meet this requirement which would help establish a banking industry that is well capitalized to support the much needed economic transformation Ghana needs.

5. As the Bank of Ghana pursues this objective, alongside strengthening the regulatory and supervisory environment to restore confidence and promote stability and integrity of the banking sector, it is important that we also take concrete steps towards implementing cyber security measures to combat financial crime. Through the Bank's monitoring systems, we have observed the daily attempts by cyber criminals to bypass security controls and exploit vulnerabilities within the cyber and information security defenses of financial systems. We cannot ignore the fact that the increasing use of technology with its attendant interconnectedness has enabled some of these challenges.

6. Globally, risks associated with cybercrime on financial systems have increased, notable among them are the financial disruptions arising from cyber-incidents in Bangladesh and

Malaysia. Indeed, cyber-attacks have the potential to pose systemic risk by disrupting business operations within the financial sector. For Ghana, the threat is growing. A recent study in 2016 disclosed that there were more than 400,000 Malware incidents, 44 million Spam incidents, and 280,000 Bot incidents within Ghana's financial industry.

7. With this background and the complexities associated with the advancement of technology, it is imperative that the Bank of Ghana takes steps to counter these threats to ensure the integrity and operational security of the financial system. It is in this regard that the Bank of Ghana has developed the Cyber Security Directive for Financial Institutions. The objectives of this Directive are to ensure an uninterrupted financial intermediation process through a robust and resilient

financial sector and also to boost the trust and confidence of consumers in the banking industry.

8. Ladies and Gentlemen, we will all agree that the resilience of the financial sector is largely dependent on the soundness of financial institutions and the robustness of the financial market infrastructure. The Cyber Security Directive for Financial Institutions does not fall short of addressing these objectives. Among others, the Directive seeks to establish the conduct and operational guidelines for the cyber and information security environment. Specifically, it sets out procedures for governance, risk management, internal audit, asset management, cyber defense, and cyber response, among others.

9. All of us in the industry have key roles to play in the implementation of this Directive. One unique characteristic of this directive is the required active involvement of senior management executives and boards of financial institutions. All banks are to appoint a Cyber and Information Security Officer (CISO) who would advise senior management and the board on cyber security issues, and also formulate adequate measures to manage cyber and information security risks.

10. A key component of the measures to be deployed by the CISO is the training and education of all stakeholders. Colleagues, it takes an individual to click on an email attachment for a virus to be introduced into the system of an organization, but the whole organization and sometimes the entire nation may also suffer the unintended consequences of this singular action. Therefore, another crucial element of the

Directive is the creation of an enabling framework for the efficient information sharing among stakeholders, for example between financial institutions and regulators, and among financial institutions as well.

11. In line with the National Cyber Security Awareness Month (NCSA) therefore, the Bank of Ghana is today, launching the Cyber and Information Security Directive for the financial industry. Subsequent to this launch, banks would be required to follow an implementation schedule to ensure that effective cyber security controls are in place to counter any threats of cybercrime.

12. Ladies and Gentlemen, as I conclude this speech, I would like to reiterate the need for collaboration among key stakeholders in the fight against cyber-crime. We need not

only implement these Directives, but also collaborate with each other in the industry to overcome the threats of cybercrime. As bankers, we must incorporate cyber security in our daily activities and imbibe these Directives in the policies and procedures of our individual financial institutions. Cyber threat is continuously evolving, and as custodians of the financial sector, let us all embrace the Cyber Security Directive and work assiduously to ensure its success.

13. Thank you for the attention.