Encik Abu Hassan Alshari Yahaya: Future proofing compliance – responsibility and response-ability

Speech by Mr Encik Abu Hassan Alshari Yahaya, Assistant Governor of the Central Bank of Malaysia (Bank Negara Malaysia), at the 9th International Conference on Financial Crime and Terrorism Financing (IFCTF) "Future proofing Compliance: Responsibility and Response-ability", Kuala Lumpur, 5 October 2017.

* * *

It is a great pleasure for me to be here today among industry leaders and experts. As we approach the end of this conference, I would like to thank all of you for your participation and contribution in making this year's IFCTF a success. I believe that the various sessions and the topics discussed in the past two days have provided significant insights and understanding towards strengthening our risk management and capabilities to mitigate the vulnerabilities from threats of money laundering and terrorism financing. I would like to commend CONG and AIF for the continuous effort and initiatives in enhancing the capacity and capability of the financial industry, to improve the industry's response to financial crime and terrorism financing.

As highlighted yesterday, countries are still facing fundamental challenges towards effective implementation of AML/CFT measures. Weak legal, regulatory and supervisory framework and inadequate risks understanding would have cascading effects, not just on compliance with international standards, but towards effective implementation of AML/CFT measures in achieving the intended outcomes. While efforts can be made to strengthen the legal and supervisory framework, from the financial industry perspective, strong understanding of risks and effective application of risk mitigation, including commensurate application of the AML/CFT measures are critical for the meaningful conduct and practices of financial institutions. This is particularly important in the conduct of CDD and transaction monitoring that will facilitate strong financial intelligence and reporting, to achieve the enforcement objectives.

Authorities are committed to continuously enhance the current legal and supervisory framework. At the same time, financial institutions and other reporting institutions must be robust in their current practices and compliance.

Technological Development

Everyone agrees that technological advancement is moving at a pace far greater than ever before. For the financial industry to maximise the overall benefit of this progress, we must acknowledge both the advantages and the risks of such rapid technological advancement while keeping abreast with the latest innovations. New devices, software, applications and inventions will continue to emerge. The challenge is for us to keep pace and ensure that industry players understand the potential benefits as well as the risk they bear. As the financial industry evolves into digital, it is inevitable that the industry becomes vulnerable to various new threats and risk factors, especially in the domain of financial crimes and terrorism financing.

In the effort to mitigate these risks, it is important that we embrace technology and use it to our advantage in order to strengthen our defences against financial crimes and terrorism financing. There are many areas in which the industry could benefit from the latest in technology.

1. Firstly, the enhancement of transaction monitoring and reporting system through the use of advanced big data mining and analysis method. The advancement in artificial intelligence and machine learning enables us to collect and analyse data in a way that was not possible before. This allows us to gain new and important insights that will contribute significantly to the prevention of financial crimes. Furthermore, the ability to tap into vast amount of information also helps promote better client management which would encourage wider

financial inclusion and tailored customer service;

2. Secondly, the use of technology to complement and support the compliance function especially in the area of higher risk. A good example of this is demonstrated through the use of digital verification to overcome challenges surrounding non-face-to-face verification and transaction. Online identification recognition and biometric verification such as facial, voice and fingerprints recognition offer a new layer of security and potential increase in efficiency for the financial sector. Such advanced systems have the potential to strengthen the existing framework and process to minimise fraud and error.

It is all too common to view technology as a disruption and a threat to the way we are used to doing things. Nevertheless, when technological change is managed appropriately and its related risks are mitigated, we can turn it into an enabler of progress for the financial industry. There is always a group of people who are relentless in their criminal pursuit of economic profit at the expense of others. It is only through our collective efforts that we can manage this negative externality of technological advancement.

Challenges posed by Cryptocurrency for AML

As all of you are aware, the next frontier in the financial industry is the advancement in blockchain technology that allows the existence of cryptocurrency. With the global market capitalisation now standing at approximately US$160 billion[1], cryptocurrencies could become a major part of the financial system that offers new and exciting opportunities as well as challenges for the industry and regulators. However, cryptocurrency is vulnerable to criminal abuse due to the anonymity it provides to its users and its ability to facilitate cross-border transactions, potentially allowing illicit funds to be transferred globally without a trace.

We have seen a range of actions taken by regulatory bodies across the globe in order to manage this risk, ranging from total prohibition, partial regulation, to full legalisation. Each country will need to make an assessment of risks and rewards in its own unique context. We are also in the midst of making such an assessment and we do so with an objective that has and will always remain steadfast – that is to balance between safeguarding our economy and allowing room for innovation and progress.

Increasing Threat of Cyber crimes

Let me now touch on the increasing threat of cyber-crime. We have seen a double digit growth in cyber-crime in the past decade. By 2019[2], cyber-crime could reach up to US$2 trillion, which is three to four times the total banking asset in Malaysia[3]. Domestically, we saw persistent increase in cyber security incidents reported to the Malaysia Computer Emergency Response Team with the majority of these cyber incidents being related to fraud and intrusion. The threat is imminent not only in the private sector, but also in the public sector.

Enhanced security framework and proper mitigating strategy and action plan is vital in order to manage the risk and alleviate the impact of any potential attack. A research done in 2016 in the US showed that only 37% of the financial services industry have a Cyber Security Incident Response Plan. I believe that our financial industry needs to be in greater state of preparedness on this.

Emerging Terrorist Financing Threats

Terrorism financing continues to pose significant threat to the financial industry, with larger ramifications that reverberate to political stability and the loss of lives. Importantly, the terrorism financing threat continues to evolve alongside technology. While traditional methods such as mule accounts and cash smuggling continue to be the main feature of terrorism financing, terrorist organisations and actors have not been slow in exploiting new technologies and financial

products. Social media platforms, online crowdfunding websites and e-wallet services are increasing in popularity among terrorists to gather their resources, especially with the increasing trend in remote radicalisation and “lone-wolf” actors. These platforms have enabled a more direct and faster approach in seeking out sympathisers for donations. There is also evidence of the use of new financial products such as prepaid shopping gift cards and online game platform credits to transfer funds to finance terrorist and terrorist-related activities.

A more dynamic and intelligent system, based on real-time data analytics supported by artificial intelligence and machine learning would be useful in detecting and halting such transactions. Importantly, we need to have the capability to detect the interconnectedness between terrorism financing and other crimes including robbery, fraud, kidnapping and drug trafficking.

Threats of proliferation financing

Every jurisdiction has a vital role to play in hindering the proliferation of weapons of mass destruction. We must be attentive to the various methods of circumventing sanctions relating to proliferation financing. Our monitoring and detection systems must be dynamic to incorporate changes in our environment. There are many documented cases of sanctions circumventions due to lapses in the system. This includes deficiencies in establishing beneficial owners which allows sanctions to be circumvented through conduits such as real estate firms and shell companies. Accounts opened with inadequate customer due diligence or transactions without appropriate screening are loopholes that can be exploited. These serve as important reminders that we must be wary and alert at all times in the daily operations.

Responsibility

Collectively, the roles and responsibilities that we have, extend beyond the scope of our individual organisations. Prevention of financial crimes and terrorism financing is an important element to fortify the agenda of monetary and financial stability of the country. Complying adequately with international standards and best practices is consistent towards instilling confidence among stakeholders on the integrity and credibility of our financial system. More importantly, keeping financial crime and terrorism financing in check helps contribute towards the country’s security and stability, which is an important catalyst to a balanced economic growth and development.

Allow me to share some of the ideas and expectations with regard to the responsibilities of compliance officers.

As we are all aware, the requirements imposed are now moving towards principle-based rather than that of prescriptive or rule-based. This provides institutions with the authority or freedom to develop their own internal policy that commensurates with their risk and profile while upholding the policy intent. Thus, it is up to compliance officers to support the institutions to develop such comprehensive policies and to ensure they are properly implemented within the institution and by all relevant staff. The compliance office should also be proactive in providing accurate and proper information for their clients, especially the general public, on the intent and requirement of their policies to avoid misrepresentations of regulatory requirements and the institutions’ own business decisions.

Compliance officers should be proactive in recommending efforts and initiatives within the institutions and industry that could contribute towards the prevention of financial crimes and terrorism financing. Apart from standing guided by specific instruction and detailed direction from regulators, compliance officers are encouraged to introduced new or proactive measures, within the ambit of the law.

Similarly, the requirement now emphasises on measures that commensurate with risk. The application of the risk-based approach (RBA) should have a meaningful application in action. Misinformed RBA could lead to unjust financial exclusion, economic cost to institutions, or

sanctions by the authority.

The efforts by private sector are vital as they form a part of the country's assessment towards compliance to international AML/CFT standards. They are assessed under Immediate Outcome 4 on whether RIs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions. I wish to highlight that, based on Mutual Evaluation Exercise conducted on 38 countries so far, majority of the private sector within these countries, including developed countries are still unable to demonstrate the characteristics of an effective system; namely understanding risks, comprehensive internal control and compliance programme including application of customer due diligence on suspicious transactions reporting.

I would like to echo the discussion during the Plenary session yesterday that an effective anti-financial crime programme requires concerted efforts from every line in the institutions, be it the first, second or third line of defence. It also demands collaborative efforts by other functions within the institutions, including an updated IT system and infrastructure, comprehensive and continuous staff training programmes, and good understanding of risks. Most importantly, the oversight and support from senior management and Board of Directors of the institutions.

Before I conclude my speech, allow me to share with you some developments from the regulatory perspective that you can expect in the near future.

As you may be well aware, our national ML/TF risk assessment (NRA) is currently in progress and is expected to be concluded by year end. The results of the assessment will be accompanied with some guidance from regulators. This should be used as a basis in your institutional risk assessment to eventually align your operations on a risk-based approach.

You can also expect introductions and amendments to AML/CFT policies, in response to the NRA as well as to new areas relating to cryptocurrencies and e-KYC.

From the enforcement perspective, another notable change to expect in the next year is the publicising of financial penalties imposed on financial institutions and information on misconduct resulting in penalties.

With the increase in the number of investigations by law enforcement authorities, you should expect more significant demand for information and collaboration from your institutions. Needless to say, timely and accurate responses are highly required and of paramount importance. A sound public-private partnership is essential to achieve the ultimate objective of an effective AML/CFT regime.

On that final note, I would like to once again thank CONG, AIF and all of you here for attending this conference. I wish you all the best and let us all contribute hand-in-hand towards building a safer and more secure environment.

Thank you.

---

1 Forbes (2017) www.forbes.com/sites/cbovaird/2017/08/27/cryptocurrencys-total-market-cap-has-risen-nearly-800-this-year/#7e89e36b67c7.

2 www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.

3 RM2.5 trillion (USD633billion).