Latest Regulatory Developments in the Fight Against Economic Crime

CE's Speech

01 June 2022

The Honourable Mahen Kumar SEERUTTUN, Minister of Financial Services and Good Governance,

Mr Mathew BEALE, Managing Director, The Comsure Group

Representatives of the Industry

Delegates and participants

Distinguished Guests,

Ladies and Gentlemen,

All protocols observed.

Good morning to you all,

First, please allow me to thank the organisers for inviting me to share my views on the latest regulatory developments in the fight against economic crime. The theme of this workshop comes at an opportune moment when the financial services industry is experiencing wholesale transformation. Everything is changing, the business environment, as well as the supervisory environment in which regulated entities operate. So do the risks they face. The fight against economic crime is a matter of concern for all.

Let us look around. Emerging technologies, global interconnectedness, new business models, all bring opportunities but also pose new threats. These threats come from a variety of sources. Cybercrime, through its common techniques such as phishing and identity impersonation is perhaps the oldest known form of risk. Today, with the evolution of financial services, threats that can lead to economic crimes are ambivalent. We have today threats posed by storing data, threats posed by going digital, threats posed by not properly engaging into AML/CFT practices. And what about regulations? They also evolve and adapt to that changing environment so that our financial services sector and its global business activities are driven by comprehensive legislations that are at par with international standards. We consider that it is of utmost importance for regulated firms to place governance, accountability and investment in compliance and controls at the heart of their operations to fight against economic crime.

In the fast paced evolution of financial services, I am of view that new regulatory developments are expected in the areas of AML/CFT compliance, Big Tech, Machine learning and AI and the virtual assets.

Ladies and Gentlemen,

We just exited the blacklists of EU and UK which were a consequence of our listing in the FATF grey list. We all together felt the strain and the climate of uncertainly for our jurisdiction while we were in these lists. You will recall that the FATF had put Mauritius on its grey list of "Jurisdictions under Increased Monitoring" and required us to address the strategic deficiencies in our AML/CFT framework. According to a recent Mckinsey & Company paper, there are a number of reasons for which financial institutions should make AML compliance their top priority.

- Firstly, deficiencies in AML/CFT framework may entail **regulatory actions**. I wish to mention here that during our last 2 cycles of AML/CFT onsite inspections, the

FSC has taken 29 enforcement actions and total administrative penalties exceeding 30 million Rupees have been imposed.

- Secondly, **threats are constantly evolving**. Criminals are using sophisticated means such as
    - splitting low-cost transactions that are difficult to detect;
    - using sophisticated technology and insider information to target technology weak spots; and
    - increasing number of fake merchants and service providers in the domain of eCommerce.
- Thirdly, there is an element of **reputational risk** if financial institutions are found to be in breach of AML/CFT requirements; I wish to highlight here that the FSC publishes the decision of the Enforcement Committee.
- Last but not the least, poorly implemented AML procedures lead to poor customer's experience. According to the same report of Mckinsey & Company, 1 in 3 financial institutions have lost potential customers due to inefficient or slow onboarding processes.

I wish to highlight here that during the FATF face to face meeting, we regulators demonstrated that our procedures for AML/CFT are sustainable and in the post exit phase, we will relentlessly stress on the need to have strong AML/CFT policies to effectively fight against economic crimes.

Ladies and Gentlemen,

The second area of financial services on which we will have new regulatory developments in the very near future is the advent of Big Tech in financial services. Big tech is yet another variant of the word fintech. We have heard about Reg Tech, we have heard about Sup tech, and now we are hearing of Big tech. So what is Big tech?

Traditionally, the word is derived from what we call the big conglomerates in the financial services area. Let us take a step backward when FinTech emerged. We used to call it “the unbundling of financial services” whereby we would have a small entity providing services in the whole value chain. And the traditional aspect of FinTech was more related to small players disrupting the market with one area of the financial services, payment intermediaries being the biggest example. However, what we have seen over the years is that a number of these services are now being offered by big technology companies, for example Amazon and Alibaba. And over time, there has been a number of takeovers of small players by big tech companies. Now, these have grown in size to gain systemic proportion and the challenge that regulators are facing is that the big tech companies might not be providing the services directly nor might they be involved within the territory, that is, there are not our licencees. The problem that arises is how are we going to regulate or how are regulators going to prevent what is called a regulatory arbitrage and how regulatory aspects are going to be applied uniformly on all entities.

If you have a large company, let's say a bank, a large insurance company, within your purview and licensed by the regulator, it is easy, whatever size it is to regulate and to bring it within the regulatory framework but when the services are being provided by big tech or a component, where there is dependency, this now becomes a problem.

The point I'm making is that in the industry, we will all be exposed at some point in time with a big Techs. If tomorrow you're doing any process or any application which runs on the cloud, there is a big chance that there will be dependency now on the big tech. Let me take an example. We have today office applications or databases running directly from the cloud. If someone develops a mission critical application which has dependency on database of the cloud, where do we delignate the responsibilities? Can there be an exploitation coming from the “unlicensed” part and who takes the responsibility?

Ladies and Gentlemen,

According to a recent FinTech note published in January 2022 by the IMF, the area where regulators now need to concentrate is what we call a hybrid mode of regulation. Traditionally, up to now, in the area of FinTech, and I have been a proponent of it, that a regulator regulates what we call an activity and not the technology behind. However, this applies for a number of small companies. With big tech, IMF now recommends to take time based approach.

- In the short term, it suggests to carry enhanced disclosures where *"the Big Techs will have to disclose activities including information and risks of business activities such as lending, consumer risks and firm obligations";*
- In the medium term, to come up with codes of conduct. These codes *"can address the spillover risks from unregulated activities to the financial sector and can be developed by industry but will require public-private collaboration";*
- And in the long term, a hybrid regulation is recommended which *"is a clear home/host split based on proportionate entity-based regulation and activity-based regulation with additional groupwide supervision."*

Ladies and Gentlemen,

The third aspect of financial services which it might pose threats and which might be used for economic crimes is the dependency we have on machine learning and artificial intelligence. These aspects are new. Yet they are being used and they are being commercialized. As a result, potential loopholes might lead to exploitation of these systems by the perpetrators of economic crimes.

As an example, according to another McKinsey and Company paper on *'derisking machine learning and artificial intelligence'*, algorithms that created a negative feedback loop, were blamed for the flash crash of the British pound by 6% in 2016. And at the same time, a self-driving car tragically failed to properly identify a pedestrian walking her bicycle across

the street. I don't mean that this is a financial crime. The point I want to raise is that the reliance on AI might lead to potential situations where the risks could be unveiled or exploited. And we as regulators we therefore need to understand what is behind the system and this area of regulations is now going to become more and more underscored by us.

According to an IMF paper, published in 2018, especially in the area of FinTech, it had already recommended that regulators need to be acquainted with the algorithm behind when it comes to FinTech and AI in the implementation of services. This means that, the reliance on these algorithms could make a financial institution potentially party to a financial crime without itself being aware of it.

A number of service providers sell these products as the state of the art and unquestionable black boxes for people to make use of. Of course, they work in a number of scenarios, but often AI leans on the underlying data and the regulations of the country. It is therefore important for financial institutions to ensure that they have a clear understanding and a process by process validation of all the actions under the system with the existing rules and regulations. Especially in these cases, it is important to very carefully harden the system through appropriate IT security systems.

Regulators view AI and machine related objects as being part of an outsourced system and therefore eventually it is the financial institution that will be responsible and accountable for the actions. It will not be surprising that in the coming years, economic crime perpetrators will increasingly attack structures that are built around these systems. Especially today we have got online onboarding, we have got remote onboarding and we have got remotely or decentralized authentication of transactions.

It is therefore very important to ensure that people who are onboarded, verifiable through reliable sources are natural persons behind those actions and not robots and machines doing those transactions.

In this area, the FSC has come up with the Robotic and Artificial Intelligence Enabled Advisory Services in June 2021 whereby the Rules mention that the board of directors of the licensee shall be responsible to ensure that the licensee has at all times:

a) adequate policies, processes and controls to ensure that the algorithms continue to perform as intended;
b) a robust framework for the design, monitoring and testing of the algorithms through periodic and random reviews; and
c) competent officers for developing and reviewing the methodologies of the algorithms, even if such functions are outsourced.

Ladies and Gentlemen,

Finally, let me come to virtual assets. This is an area where we have a number of regulatory developments at this very moment at the Commission. As you all know, the Virtual Asset and Initial Token Offering Services Act 2021, came into force on 7th February 2022. This act is aimed at licensing and supervision of the virtual assets providers to mitigate financial crime risk at jurisdiction level. For the Commission, this is an area of focus and development.

I will share with you that at this point there exists more than 10,900 active cryptocurrencies with a global market capitalisation of approximately 1.3 trillion US Dollars. New concepts such as tokenization and Metaverse are becoming more and more conspicuous. All these are so new and luring to the customers that the risks of financial crime are also very prominent.

There was a time when the virtual assets were being traded anonymously are related to crime and the dark web, but these days, institutional investors have come in this area. It is very important to ensure two things:

- First, is that the risks of money laundering of the conversion of fiat money into crypto and perhaps back into fiat money is minimized.
- Second, we need to identify who are the people behind it and at the same time, it is important, given the initial connection of the cryptocurrencies with the world of crime and the dark web, to ensure that the reverse also doesn't take place.

In this respect, whilst things are already evolving, the FSC has already amended its AML/CFT Guidance Notes for Virtual Asset Service Providers & Issuers of Initial Token Offerings in February 2022. We are also working on a number of regulations attached to the virtual assets. The whole idea is to ensure that we have a regulated and enabling environment for these activities to take place and for the regulator, to be able to exercise its powers when it comes to service providers. I would like to seize this opportunity to send a message that according to the VAITOS Act, service providers already operating in these areas had until 7th May 2022 to come forward and apply for a license with the FSC. At the same time, I would like to inform the consumers of virtual assets and services that dealing with people who are not licensed is a big risk they are taking and would potentially be involved in unlawful transactions.

The Commission is working in this direction will come very soon with a series of awareness programs to educate not only the consumers but also service providers on the need to have properly regulated virtual assets activities and to protect our jurisdiction from illicit flows of funds, whether they are from the fiat or from the virtual areas.

Dear Audience

To conclude, I wish to highlight that managing regulatory requirements is no doubt of major concern to all regulated and large scale businesses, as the risks of non-compliance are hugely significant and impactful. Given the importance of compliance and adoption of

an adaptive compliance culture, there is a need to break down silos and focus on developing a proactive and holistic compliance framework supported towards the following pillars which are:

- Governance
- Internal Audit
- Fraud detection
- Cyber security
- Compliance function infrastructure, including Training.

These pillars lie at the heart of the risk-based approach underpinning current AML/CFT regulatory frameworks and can be considered as regulatory obligation that has been drawing increased scrutiny by supervisory authorities. The overall effectiveness of a country's AML/CFT regime requires recognition of the important synergies that exist between AML/CFT, prudential and business conduct supervision and between supervisors and judicial/law enforcement authorities.

With this, I thank you for your kind attention.

Dhanesswurnath Thakoor
01 June 2022