ASIC

Australian Securities & Investments Commission

Conquering the new frontier: Regulating for growth in the digital age

A speech by Greg Medcraft, Chairman,
Australian Securities and Investments Commission

The Bloomberg Address Sydney

26 November 2014

CHECK AGAINST DELIVERY

Introduction

Ladies and gentleman, thank you for having me here today. It's a privilege to be here speaking at a Bloomberg event. Bloomberg is an organisation known for the integrity of its reporting and, when you are covering financial markets, that is important.

For me personally, after three decades in investment banking, Bloomberg is an organisation that has been a continual presence in my life in one way or another. Thank you for giving me the opportunity to address you.

My topic today is 'conquering the new frontier: regulating for growth in the digital age' – and it is a new frontier, because our lives are being transformed by innovation. In particular, through the digitisation of the 'real' world.

Our financial services and markets are no different. As we emerge from the global financial crisis with a focus on economic growth, success requires that we harvest the opportunities from the digital age, while also mitigating the risks.

With this in mind, I want to talk about:

- ASIC's role
- the environment in which we operate
- digital disruption, and
- cyber security.

ASIC's role

ASIC's fundamental objective is to allow markets to allocate capital efficiently to fund the real economy and, in turn, economic growth. This contributes to improved standards of living for all Australians.

Making sure Australians have trust and confidence in our markets is at the heart of everything we do. It is what drives the excellent men and women who work at ASIC, and do so for good reason.

Our dynamic environment

I'd like to move on to my next topic – the dynamic environment in which ASIC operates. We are living in a time of rapid innovation and change, and this is only likely to increase. Change brings opportunity, but also risk.

In this age of innovation, the five key external challenges I see for ASIC, as Australia's integrated financial services and markets regulator, are:

- Getting the right balance between a free market-based system and investor trust and confidence issues, with a particular focus on
  - deregulation, and
  - ensuring that the participants we regulate have a culture, and systems, that emphasise the best interests of their customers.
- Digital disruption to existing business models and channels, which I will talk about later.
- Structural change in our financial system through the growth of market-based financing, which is largely driven by superannuation.
- Financial innovation-driven complexity in products, markets and technology. Much of this is driven by the digitisation of our economy.
- Globalisation, which affects technology, markets and products.

While these are all challenges, they also present opportunities to fund economic growth, by providing greater:

- access
- competition, and
- efficiency.

Industry and regulators need to continue working together to harvest the opportunities while mitigating the risks.

So how does ASIC respond to our challenges in ensuring people have trust and confidence in our markets? We do this through our strategic priorities of:

- promoting investor and financial consumer trust and confidence
- ensuring fair, orderly and transparent markets, and
- providing efficient and accessible registration of participants in the financial system.

In achieving our strategic objectives, a key aspect of what we do is identifying and dealing with those who break the law. ASIC is a law enforcement agency, 70% of our regulatory resources are devoted to surveillance and enforcement.

We hold gatekeepers to account to the best of our ability through our 'detect, understand and respond' approach. Let me unpack each of these:

- we 'detect' misconduct and the risk of misconduct by gathering intelligence through:
  - surveillance, both proactive and reactive
  - breach reporting
  - reports from whistleblowers and the public, and
  - data gathering and matching (e.g. our MAI surveillance system)
- we 'understand' by analysing the intelligence we receive, and
- depending on our resources and powers, we 'respond' with the right nudge by:
  - educating investors through ASIC's award-winning financial literacy work, largely conducted under our MoneySmart brand
  - providing guidance to gatekeepers
  - communicating the actions we take
  - disrupting harmful behaviour, for example, our work in stopping misleading advertising
  - taking enforcement action, such as sending criminals to jail, removing bad apples from the industry and securing compensation for investors, and
  - providing policy advice to Government.

We do the best we can with our resources and powers to catch those who break the law. For those who intentionally break it, we will do all that we can to ensure the ramifications are severe. Of course, the vast majority of people comply with the law and have nothing to worry about.

Digital disruption

Now, I'd like to move on to my next topic, digital disruption.

Traditional business models are being disrupted by new digital strategies at an accelerating pace. This change is being driven by innovations in mobile, video and networking technologies.

Innovators that were once the disrupters are now facing disruption themselves. For example, alternative payment systems, like PayPal, are facing potential disruption from crypto-currencies and prepaid cards.

Other examples of digital disruption in the financial services sector include peer-to-peer lending, crowdfunding and robo-advisers – and, in or markets, high-frequency trading and dark liquidity.

The great drawcard of these disruptions is the opportunities they bring. There is the potential for new and unimagined forms of:

- intermediation – like crowd-funding, and
- in some cases, disintermediation – here crypto-currencies come to mind.

Both regulators and industry must work together to harvest the opportunities, while mitigating the risks. At ASIC, we are keen to facilitate innovation where it does not compromise investor and consumer trust, confidence or stability.

Digital disruption does not change the outcomes we achieve, but it will change how we achieve them. We are increasingly relying on technology to detect and respond to misconduct. For example, our Market Analysis Intelligence (MAI) system allows us to gather and match data to detect suspected misconduct in real time.

Digital disruption offers new forms of access, greater competition and greater efficiency. It provides business with new ways of creating and sharing value with their customers.

I believe the disruptors that will end up succeeding will be those that provide a demand-driven offering, which puts the customer's interests at the core of what they do.

Cyber security

A key risk of the digital age is cyber crime. This is my final topic – cyber security.

Advances in technology have led to the rise of cyber crime around the world. The links between market players and infrastructure means that the impact of a cyber attack can spread quickly and has the potential to dangerously affect:

- the integrity and efficiency of global markets
- the protection of investors, and
- ultimately, trust and confidence in the financial system.

An example of the sobering effect of cyber crime occurred earlier this year when 76 million household and seven million small business accounts were reported to be compromised in a cyber attack on JP Morgan Chase in the United States.

Cyber crime is a systemic risk. It is no surprise that it has captured the interest of global policy makers, including the:

- International Organization of Securities Commissions (IOSCO), through my chairmanship, and

- Financial Stability Board, who flagged their concerns with the Group of 20 Leaders in Brisbane recently.

So, how do we counter the threat of a cyber attack? It is all about cyber resilience through risk management. Risk management systems must be granular enough to ensure a good level of resilience in an organisation. Boards should also be alive to the risk of a cyber attack as part of their risk-oversight role. Cyber crime is a global problem that requires a global solution.

For critical infrastructure, we must focus on developing a consistent language to communicate the relative level of an organisation's cyber resilience. The US *Framework for improving critical infrastructure cyber-security* is a good starting point.[1] It provides a scalable analytical framework to help organisations manage cyber risk. Importantly, it also provides a methodology for communicating the maturity of an organisation's cyber resilience, ranging from partial – that is, ad hoc risk management – to adaptive – that is, an organisation that actively adapts to a changing cyber landscape and responds to evolving threats in a timely matter.

At the regulator level, IOSCO is working on a range of projects to guide coordinated regulatory responses. We are working with the Committee for Payment and Market Infrastructure on guidance to improve the way financial markets infrastructure should be addressing cyber risk.

IOSCO's policy committees are also considering the guidance they might be able to provide. For example:

- how cyber risks are managed by participants in a range of sectors
- disclosure about how those risks are managed, and
- enforcement – improving how members co-operate in investigating and responding to cyber attack, in particular, sharing information under IOSCO's *Multilateral Memorandum of Understanding*.

Conclusion

I'd like to conclude with the observation that regulating for growth in the digital age requires industry and regulators to work together to harvest opportunities while mitigating risks.

To be successful, we must both be agile and always have an eye on the future – otherwise we will be left behind.

Thank you.

[1] National Institute of Standards and Technology, *Framework for improving critical infrastructure cyber-security*, 12 February 2014.