Regulating for the future: Innovation, disruption and cyber resilience

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

AFR Banking & Wealth Summit 2016 (Sofitel Wentworth, Sydney)
6 April 2016

CHECK AGAINST DELIVERY

Welcome

Good morning everyone. It is great to be here at the AFR Banking & Wealth Summit to talk about *Regulating for the future: Innovation, disruption and cyber resilience*.

You might say that we are in a time of rapid evolution – or perhaps a new revolution.

The First Industrial Revolution used water and steam power to mechanise production; the Second Industrial Revolution used electric power to create mass production; and the Third Industrial Revolution used electronics and information technology to automate production.

Now Klaus Schwab, Executive Chairman of the World Economic Forum, has said that we are right in the middle of the Fourth Industrial Revolution – the digital revolution.

While digital innovation is not a new phenomenon, the scale, breadth, speed – and potential – of this innovation is unprecedented.

We are now surrounded by mobile devices and data, and we are seeing many new developments in areas such as robotics, self-driving cars and smart buildings.

In financial services we are seeing automated financial advice (robo-advice), new developments in payments and the potential of distributed ledger (or blockchain) technology.

Consumers have a lot to gain from technological innovation. Technology has made possible new products and services that streamline our lives, make things more convenient and lower costs.

At the same time, changing consumer demographics, consumer engagement and behaviour are forcing businesses to change the way they design and deliver products.

We are seeing incumbents being disrupted by agile, innovative competitors who can often deliver value with greatly improved quality, speed, or price.

We are also seeing the development of the 'sharing' economy which is disrupting existing industry structures – and is underpinned by technology enabled platforms.

In financial services, fintech is not only transforming the way consumers operate and manage their finances, it is disrupting the traditional banking industry.

We used to think about fintech as something that wasn't a big deal – something new that would operate on the edges and wouldn't really shift the customer base.

But now the evolution of fintech is being embraced rapidly by consumers, who see the clear benefits it brings – like improving ease of payments, improved speed and convenience and lower costs.

Technology and innovation is disrupting and reshaping the world we live in. It is against this backdrop that I would like to talk about three things:

- what innovation and digital disruption means for ASIC
- how ASIC is responding to digital disruption, and
- how regulators need to position themselves for the future.

What digital disruption means for ASIC

What does digital disruption mean for ASIC?

Digital disruption brings opportunity. Digital disruption, by its nature, is not change by evolution. It is radical in the way it changes the landscape.

In financial services, businesses are seeing the potential for new ways of creating and sharing value with technologically savvy investors and consumers.

New digital strategies continue to challenge traditional business models, disrupting financial services and markets and changing how they interact with investors and consumers, across a range of platforms and devices.

What is fundamentally important in all of this is thinking critically about the implications of digital disruption.

Often disruptive businesses have innovative business models that may not fit neatly within existing regulatory frameworks or policy.

And, over recent years, there has been significant growth in the number and severity of cyber attacks around the world.

While digital disruption brings great opportunity, it also brings risks. We see digital disruption as one of the key challenges to achieving our strategic priorities of:

- investor and consumer trust and confidence, and
- fair, orderly, transparent and efficient markets.

How ASIC is responding to digital disruption

So how is ASIC responding?

In our four year Corporate Plan,[1] released in August last year, we set out how we are responding to our key challenges, including digital disruption and cyber resilience.

To respond to digital disruption and cyber resilience, we are continuing to focus on:

- promoting cyber resilience and identifying potential cyber attacks in markets through real time market monitoring
- ensuring compliance with licensing obligations
- taking steps to help industry take advantage of the opportunities on offer, by ensuring that investor and financial consumer trust and confidence is not compromised – for example through our Innovation Hub, and
- monitoring overseas developments on regulating fintech such as the proportional approach evolving in many jurisdictions, such as China.

I would now like to talk in a bit more detail about two particular ways that ASIC is responding:

- through our Innovation Hub, and
- our work on cyber resilience.

ASIC's Innovation Hub

At last year's Annual Forum, I announced ASIC's Innovation Hub, which is designed to foster digital innovation and help innovators navigate our regulatory system.

I would like to give you an overview, one year in.

Since the Innovation Hub was established, we have:

- started work on 100 matters relating to 76 entities, including licence applications and requests for guidance
- established internal taskforces into automated financial advice (robo-advice), digital marketplace lending, equity crowdfunding and distributed ledger (blockchain)
- issued tailored guidance on robo-advice and marketplace lending
- presented at fintech meet-up events to discuss our Innovation Hub and our approach to new business models, and

[1] ASIC, Corporate Plan 2015-16 to 2018-19: Focus for 2015-16.

- established ongoing fintech dialogues with international regulators and independent organisations working on innovation issues. I will talk about a particular example of this later.

Cyber resilience

Turning to cyber resilience.

Cyber threats are no longer an abstract notion, or just an IT issue. There has been significant growth in the number, sophistication and severity of global cyber attacks in the last few years.

With the risk and sophistication of cyber attacks growing faster than traditional firewall and antivirus technology can keep up, financial services organisations need strategies to prevent, detect and respond to cyber risks.

The cyber environment is agile and evolving constantly and cyber resilience strategies need to be equally agile and evolving.

The impact from a cyber attack can be severe. A cyber attack could undermine trust and confidence in the resilience of the financial system.

Because we see cyber risk as a key threat to our strategic priorities, ASIC is seeking to assist our regulated population in their efforts to improve their cyber resilience.

In March 2015, we published our Cyber Resilience Health Check Report,[2] to help our regulated population improve cyber resilience by:

- increasing awareness of the risks
- encouraging collaboration between industry and government
- providing health check prompts to help businesses consider their cyber resilience, and
- identifying how cyber risks should be addressed in the regulatory context – including considering broad oversight of cyber risks.

We encourage organisations to use the NIST Framework – the US National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity.

Following the release of our Cyber Resilience Health Check Report, last month we also released our Cyber Resilience Assessment Report,[3] which sets out 11 important practices for cyber resilience.

We acknowledge that complete cyber security can never be achieved, however a comprehensive and long-term commitment to cyber resilience is essential to retain investor and financial consumer trust and confidence.

[2] Report 429 *Cyber resilience: Health check* (REP 429).
[3] Report 468 *Cyber resilience assessment report: ASX Group and Chi-X Australia Pty Ltd* (REP 468).

Regulating for the future

As regulators, we cannot afford to sit back and relax into thinking that things will continue in the way we have become accustomed.

We must constantly be alert to new developments – both the opportunities and risks. We must continue to improve the way we do things – adapting constantly with the pace of change.

The financial sector will continue to evolve dynamically as a result of the ongoing rapid advancements in technology.

One of the consequences of digitisation is the explosion in the quantity of data generated by financial firms.

This means that we need to focus more on 'RegTech' – using data and technology to assist with regulation and compliance – by developing technological systems that are both agile and adaptable.

It also means we need to enhance our capabilities, which includes ensuring we have staff with the relevant skills and expertise to be able to use data more efficiently.

We now have a focus on skills in data analysis and analytics so we can better utilise the data available to enable us to achieve our strategic priorities.

Work underway at ASIC

Some of the work we have already been doing in positioning ASIC for the future include implementation of:

- Market Analysis Intelligence (MAI) that provides ASIC with sophisticated data analytics to identify suspicious trading in real time and to have a greater chance of detecting market misconduct
- a new online regulatory compliance portal, Market Entity Compliance System (MECS), that provides market entities with tools and information to assist them in complying with a number of their regulatory obligations, and
- our FAST2 program that aims to improve technological and data integration within ASIC, particularly misconduct and breach reporting, which will enhance our ability to operate in a new regulatory environment.

Work in the international space

Innovation in financial services is not limited by national borders. We are addressing the international dimension in a number of ways. Let me outline two.

The first is the work the International Organization of Securities Commissions (IOSCO) and the Financial Stability Board (FSB) are doing in this space.

Both have flagged fintech as a key priority warranting a co-ordinated multilateral response. IOSCO is working to better understand the benefits and risks fintech poses to the markets its members regulate. The FSB is doing the same in relation to the benefits and risks fintech poses for financial stability.

Though it is early days, the evolving thinking in both groups is in-line with our approach domestically – that is, working to harness the opportunities while mitigating the risks.

The second, and particularly exciting way, we are addressing the international dimension is our direct work with key international regulators to encourage innovation across borders.

A great example of this is the Co-operation Agreement,[4] we signed with our UK counterparts, the Financial Conduct Authority (FCA), before Easter – the first of its kind internationally.

The Cooperation Agreement sets up a framework under which our Innovation Hubs refer innovative fintech businesses to each other. It also commits us to share information about fintech innovations.

What this means is that when our Innovation Hub refers a business we have helped domestically (and which wants to enter the UK market) to the FCA, the FCA has agreed to provide a contact point, assistance through the authorisation processes and assistance for the first year of operation.

We have agreed to do the same for businesses referred to us by the FCA.

We will also share information about emerging trends and developments and the regulatory issues we are seeing in this space.

So, the Cooperation Agreement benefits our innovators wanting to expand to other markets by providing a path to get there. It also helps us to keep up to date in a rapidly changing space.

Conclusion

In conclusion, I want to say that technology is just a tool. It is an enabler.

None of this technology, innovation or disruption takes away the need for fundamental values. The future of regulation is likely to be more principle-based.

Just as regulators will need to be more agile and flexible, so too will regulation itself.

But this also places a greater responsibility on industry to ensure that they develop and sustain a customer-focused culture.

I have been emphasising the importance of culture as a key driver of the conduct of firms. If public trust takes a hit, a firm's social licence to operate can be jeopardised.

[4] Innovation Hubs Co-operation Agreement between Financial Conduct Authority and Australian Securities and Investments Commission, 23 May 2016.

We want to position ourselves for positive change and growth, while ensuring that the way we behave and the values we hold mean that investors and financial consumers can have trust and confidence in our financial system.

Not only that, but we want to see that financial institutions – whether they are incumbents or new start-ups – have their customers interests at the centre of their business.

In this digitally-enabled world – perhaps our Fourth Industrial Revolution – businesses need to create a culture that their customers can believe in.

Thank you.