ASIC

Australian Securities & Investments Commission

The importance of trust in a digital world

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

Stockbrokers and Financial Advisers Conference (Sydney)
25 May 2017

CHECK AGAINST DELIVERY

Introduction

Good morning and thank you very much for having me at the Stockbrokers and Financial Advisers Conference today.

I want to talk to you about the importance of trust in a digital world.

The *Harvard Business Review* has identified trust as a critical strategic asset of a business.[1] I think it is important for businesses to reflect on how they build and maintain this trust.

So, today I have three points I would like to talk about:

- the rate of technological change we are experiencing today that is unprecedented – this is the fourth industrial revolution
- how this speed of change is impacting the way that consumers interact with businesses, including how we build and maintain trust in them
- what this means for businesses today, and what it means for us as regulators.

[1] D Prahalad, 'Why trust matters more than ever for brands', *Harvard Business Review,* 8 December 2011.

Technological change

We live in an era where technology is changing our lives at a rate that many of us are grappling to keep pace with. Artificial intelligence – or AI – is at an early stage, but it is developing faster than we once expected. We are on the cusp of machines that can understand the world and respond effectively.

The combination of internet-connected networks and machine-learning algorithms is setting the platform for forward leaps in the ability of machines to understand spoken, written and visual communications. With technological improvements in speech and image, AI is moving towards ever-increasing personalisation applied to, for example, education and medicine. For instance, the fascinating ability to now use holographic learning to teach doctors anatomy.

AI applications in financial services have the potential to improve consumer outcomes across a variety of channels. For example, apps can create consumer value by automating and optimising personal savings. You can even imagine a personal financial concierge who automatically helps you optimise your spending, savings and investment based on your own personal habits and goals.

Across financial services, technology is enabling the development of new products and services that can meet consumer needs more efficiently, and more cheaply. It has application to trading strategies – it is conceivable that AI may be able to predict the rise and fall of the share market more effectively than humans can. We have already seen the role of algorithms in high-frequency trading (HFT), which I spoke about recently at a conference at Oxford University.

We have seen an explosion of investment in fintech activity over the last couple of years. In 2016, global investment in fintech companies hit $24.7 billion. It’s clear that fintech is a big part of where the future of finance is heading.

Not to forget the emergence of distributed ledger, and its potential to disintermediate and remove significant costs from the financial system.

We are starting to see the reinvention of the banking model, with talk of ‘ecosystems’ that are not just focused on financing. The potential of businesses such as Facebook, Amazon and WeChat in this area is immense.

We also see the challenges of fiat digital currencies that could reshape banking and payment systems dramatically.

The impact of digital on trust

Driven by evolving technology, incumbents are seeing their business models challenged by new digital entrants. At the same time, their behaviour is being magnified in real time through the 24-hour news cycle, social media and the crowd.

But I don't think the issue is just about the challenge of keeping up with technological developments – or managing the media or the crowd. The overall question is much bigger.

In times gone by, goods and services were associated with people, not organisations. Previously, people personally knew those with whom they conducted business. Industrialisation distanced people in this relationship as goods became mass manufactured.

Digitalisation has distanced us even further from the human face of business, as processes and interactions are increasingly online and automated. The types of transactions that consumers engage in today, online and through apps, actually require a high level of trust. So, the question is this:

- How do we approach the issue of trust when we don't have a human face to interact with?
- For business, how do we adapt to create and sustain trust in a different world that is driven by digital transformation?

Building trust with customers has become a far more challenging endeavour than it previously was. I'd like to touch on three points today that I see are central to maintain consumer trust in a technological environment.

- data access and use
- cyber resilience
- accountability.

Data access and use

Privacy is a big issue with the potential to impact on trust. There are risks data will be stored, used and shared with others against the wishes, or reasonable expectations, of those providing the data. There are critical questions about the extent to which data should be gathered, analysed and used.

The digital revolution has given companies the technologies to collect enormous amounts of data about its customers. We can use data analytics to create new knowledge and insights, affecting how this data is used.

Managing and protecting privacy and data use will become an important measure of how much customers and stakeholders trust the companies they deal with. Transparency about what information is being collected, and what it will be used for, will be critical.

Cyber resilience

The growing use of technology to capture, store and analyse data increases the risks of that data being misused, and the systems used to capture and store that data being subject to cyber attacks. Cyber resilience is only going to grow in importance as we connect more of our physical life to the internet.

Cyber security features high on the agenda of leaders across all sectors. In recent weeks, cyber crime has captured international headlines yet again.

The average cost of cyber crime to Australian companies is now estimated to be over $5.6 million per incident. The increasing incidence, complexity and reach of cyber crime can destroy a company's value overnight – dragging its share price and reputation down with it. For consumers, it directly relates to how safe their data is in your hands, as well as can you deliver a seamless service that meets their needs despite the digital threats to your business?

Late last month, ASX launched the *ASX 100 Cyber Health Check Report* (PDF 5.17 MB) in collaboration with ASIC, Government and industry. One of the key trends identified in the report is that while companies are managing cyber risk better, there's still more to do.

Our own ongoing reviews of the cyber risk management of financial intermediaries indicate significant differences in the cyber security approaches of some of the largest organisations in our markets. Some of the biggest issues are:

- interdependency recognition
- transparency of disclosure of attacks
- measuring resilience.

Accountability

The rise of automation and journey towards AI raises the serious question about what might go wrong, and if it does, who will be accountable? We need to make sure we do not neglect this issue of accountability. Firms need to be held accountable in the same way they would for any breach.

Algorithms and AI, just like any system, are an enabler, but not a replacement for human judgement. For any algorithmic system, there needs to be a person who is responsible for its design – and its outcomes.

Automated decisions must be able to be meaningfully explained to customers, to the regulator, and to any other interested stakeholders. The algorithms will need to be transparent so their decisions can be challenged, and not just be considered opaque 'black boxes'. If and when algorithms make mistakes, whether because of data errors in their inputs, or because of issues with their design, there need to be avenues for redress.

We cannot use technology platforms to simply shift risk to the consumer. We need to make algorithms align with and reflect human values and expectations of behaviour.

What does this mean for business and regulators?

What it means for business

So what does this mean for business?

Word-of-mouth and reviews (i.e. the ‘crowd’) have become increasingly influential in consumer decision-making. Personal recommendations have been effective in driving attitudes towards a brand and purchase behaviour, but social media has now magnified and intensified the power of these recommendations. The power of consumer reviews and positive word-of-mouth can help build and maintain trust in a company’s brand.

On the flip side, social media and the 24-hour news cycle mean that companies are increasingly held to account for any perception of poor behaviour. If they are not behaving in the right way, the crowd will let them know, if not the headlines – often with damaging effects on their brand and reputation. Transparency and communication is also key.

We have seen recent examples of crises that have been poorly managed, and this can damage consumer trust in a brand. With this in mind, how do companies ensure positive word-of-mouth, while minimising the damage of negative media and customer dissatisfaction?

Creating a sustainable business today is not only about the quality of the product or service that is delivered. It is also about the quality of a firm’s conduct, both internally and externally. As I described, a company will be judged on how it deals with the data it collects on its customers, how it manages its cyber security, and the accountability mechanisms it has in place.

If the conduct of a business and its values are not aligned with customer outcomes, it is easy to see how a trust deficit will emerge, and this will impact its long-term sustainability. Trust must be built through a company’s brand and reputation – which is a logical result of how it treats its customers and looks after their interests.

What it means for ASIC

What ASIC has done recently in our four-year Corporate Plan is set out our view of ‘what good looks like’ in each of the sectors we regulate. For market intermediaries, we think a good business would:

- ensure their conduct and behaviour support the integrity of Australia’s retail and wholesale markets
- act professionally and treat investors fairly, including by managing confidential information and conflicts of interest appropriately, and
- have effective risk management structures and internal supervision (e.g. cyber security).

In particular, we are focused on the management of confidential information and conflicts. The timely and accurate flow of information about companies and financial products is vital to the fair, efficient and transparent operation of financial markets, and the trust that investors have in those markets.

Our Report 486 *Sell-side research and corporate advisory: Confidential information and conflicts* (REP 486) identified shortcomings in the way some licensees identify, handle and manage situations where staff obtain material, non-public information. It also identified instances of poor management of conflicts between research and corporate advisory within licensees.

We will soon be consulting on updated guidance for sell-side research. This guidance will supplement rather than replace our existing guidance in Regulatory Guide 79 *Research report providers: Improving the quality of investment research* (RG 79). The proposed guidance will set out our expectations of how licensees should handle material, non-public information and manage conflicts of interest when providing research. In particular, the guidance will propose:

- strengthening the arrangements licensees have in relation to the identification, handling and management of material, non-public information
- placing restrictions on interactions between research analysts, corporate advisory and issuing companies during the capital raising process
- recommendations in relation to the structure and funding of research
- emphasising the role and importance of appropriate compliance and control functions.

We consider these measures enable us to strike an appropriate balance between research analysts' contribution to a firm's decision to underwrite a transaction and maintaining the integrity of research, in particular reducing the risk of pressure being place on research analysts in relation to valuation information.

Supplemented guidance should assist licensees involved in sell-side research and corporate advisory to comply with their regulatory obligations and foster trust in the integrity of our financial markets.

As regulators in this fast paced environment, we are keeping our eyes on the transformative changes on the horizon. We are engaging with these trends, and understanding them, so we understand what the risks are to trust and confidence.

Our guiding principle is maintaining sensible and appropriate regulation that fosters consumer trust and confidence in financial services. ASIC has always had a focus on not standing in the way of technological change that may improve outcomes across the financial system. We are focused on harnessing the opportunities of innovation, while ensuring that investors and consumers can have trust and confidence.

Conclusion

We are living in a time where innovation and evolving technology is the new norm. We are living with new possibilities that were previously unimaginable.

In this world, our efforts must be squarely focused on fostering trust and confidence. And we must always remember that trust will not be given automatically – it must be genuinely earned.

