ASIC
Australian Securities & Investments Commission

Dealing with fraud: A regulator's perspective

A speech by John Price, Commissioner,
Australian Securities and Investments Commission

Association of Certified Fraud Examiners Melbourne Chapter annual seminar
(Melbourne, Australia)
10 November 2015

CHECK AGAINST DELIVERY

Thank you for that introduction and for the opportunity to speak here today.

It seems fitting that the theme for today's conference is 'tales from the trenches' given we are at the Melbourne Cricket Ground (MCG), where many great sporting battles have unfolded.

Today I would like to cover a few topics, including:

- the role of ASIC and others in the financial system in detecting and dealing with fraud
- our experience in matters the community might think of as fraud – including risk factors that might be apparent in some matters with the benefit of hindsight
- where the future may take us when considering fraud.

Detecting and dealing with fraud

Role of ASIC

In talking about detecting and dealing with fraud perhaps I should briefly start with the role of ASIC. As you are probably aware, ASIC's role in Australia is as a regulator of our financial services and markets – and this covers not only our various stock exchanges and markets but also those who develop, sell and advise on investment and credit products.

Our goal is ensuring that the financial services and markets we regulate operate to fund the real economy and drive economic growth. In doing so, we contribute to improved standards of living for all Australians. But we can only achieve this if investors, financial consumers and those needing capital to build their businesses have trust and confidence in our financial services and markets.

We are working towards our goal through our strategic objectives to:

- promote investor and financial consumer trust and confidence
- ensure fair, orderly, transparent and efficient markets
- provide efficient and accessible registration and licensing.

To achieve these objectives, detecting misconduct and enforcing the law is important. That is why 70% of ASIC's regulatory resources are devoted to surveillance and enforcement.

Of course, ASIC is only one of the regulators of financial services; other regulators include the Australian Prudential Regulation Authority (APRA), the Australian Taxation Office (ATO) and the Australian Transaction Reports and Analysis Centre (AUSTRAC). Each regulator has a different mandate and set of objectives. But, interestingly, in my experience all of these regulators may come across matters that the community may think of as fraud. So while there is often an overlap in priorities between regulators, we do work together and share information if and when needed.

Similarly, ASIC is just one of many law enforcement agencies that investigate crime, including white collar crime like fraud. For example, ASIC is a member of the Heads of Commonwealth Operational Law Enforcement Agencies (HOCOLEA). Apart from ASIC, the membership of HOCOLEA includes the Australian Federal Police, the Australian Crime Commission and the Attorney-General's Department.

All of this is a long way of illustrating that fraud is a very broad concept and a key area of interest of many Government agencies. That in itself raises challenges around coordination and information sharing, and I will return to that thought in my concluding comments.

Definition of fraud

So what exactly is fraud? Well it may surprise you to know that, despite ASIC's law enforcement role, there is no definition of fraud in the key legislation we administer – the *Corporations Act 2001* and the *Australian Securities and Investments Commission Act 2001*.

However, perhaps the most useful description of fraud I have seen comes from an auditing standard that notes:

> Fraud means an intentional act by one or more individuals among management, those charged with governance, employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage.
>
> (Auditing Standard ASA 240 *The auditor's responsibilities relating to fraud in an audit of a financial report*)

Just reflect for a moment on what a broad range of behaviours and misconduct that the term covers. It is little wonder that many regulatory agencies have an interest in this topic.

Despite the level of regulatory attention to this issue, I think it is critical to appreciate that a focus on the role of regulators is, in my view, looking at the problem of fraud the wrong way around.

The auditing standard I mentioned also makes it clear that:

> The primary responsibility for the prevention and detection of fraud rests with both those charged with governance of the entity and management. It is important that management, with the oversight of those charged with governance, place a strong emphasis on fraud prevention, which may reduce opportunities for fraud to take place, and fraud deterrence, which could persuade individuals not to commit fraud because of the likelihood of detection and punishment. This involves a commitment to creating a *culture* of honesty and ethical behaviour which can be reinforced by an active oversight by those charged with governance.

Remember those words about culture – I will return to them later.

Dealing with fraud

The standard goes on to set out what auditors might do to detect fraud in financial reports – including giving examples of various fraud risk factors such as incentives, opportunities, attitudes and rationalisations.

Simplistically, what the auditing standard tells us is that management of a firm or business have the frontline role in preventing fraud, with those charged with governance and people such as auditors often playing an important checking role. I would add that regulators have an overarching role, both looking at the actions of management and also those people who play that important checking role – people that ASIC often refers to as 'gatekeepers'.

Gatekeepers have been described by academics as 'reputational intermediaries' who pledge their reputation to protect the interests of dispersed investors who cannot easily protect their own interests.

Academics argue gatekeepers can play an important role in:

- verification, certification, approval and recommendation of products and services offered to investors
- monitoring of compliance by entities and their management through their privileged access to information
- performance of a private supervisory role through the detection and deterrence of misconduct. In some cases, that can include fraud.

Of course, there are some issues with how the academic theory on gatekeepers translates in practice. For example, it can be difficult to externally monitor a gatekeeper's performance, and history tells us failures can go unchecked. Nonetheless, ASIC recognises that gatekeepers play a beneficial role in the regulatory system. This is because they help industry perform what can broadly be described as a self-regulatory or co-regulatory role.

Identifying who the gatekeepers are in the financial markets can also be imprecise – but ASIC takes a wide view of the term. Broadly, we consider the term 'gatekeepers' includes advisers (e.g. accountants), auditors, directors, liquidators, custodians, product manufacturers and distributors, market operators, and brokers.

So what does ASIC do to supervise gatekeepers like directors, accountants and auditors? In short, we have a number of risk-based surveillance programs to monitor conduct of people in the financial services sector. Like all publicly funded agencies we have finite resources, so we need to be selective in what we do.

For that reason, in considering where we focus our surveillance activities, we need to consider how best to target misconduct. We use risk-based filters to focus on the particular types of transactions or firms that we want to look at, and we have ongoing financial reporting, auditor and other surveillance programs to provide an additional level of assurance that gatekeepers are doing their job and to try to identify possible frauds. For example, in the past we have conducted surveillance to assess the possibility of fraud among hedge funds.

But, specifically, there are a few things we will look for from gatekeepers as regards spotting frauds:

- For auditors, we expect them to have obtained reasonable assurance (not absolute assurance) that the financial reports as a whole are free of material misstatement. In particular, that means obtaining sufficient and appropriate audit evidence, making sure professional scepticism is exercised and not unduly relying on the work of other auditors and experts.
- We also expect financial services licensees, credit licensees and auditors to report suspected contraventions of the law to us, and we have policy guidance about what this entails.
- And for all gatekeepers we expect them to act with honesty, diligence, competence and independence (i.e. to manage their conflicts).

Finally, it would be remiss of me not to mention financial literacy. It is a key regulatory tool to help prevent fraud. After all, what better way is there to stop consumer and investor fraud than giving those people the tools to help themselves?

Of course, no regulatory system can deter all fraud, and we recognise that there is often an expectations gap about what people expect in terms of fraud detection compared to reality. This expectations gap applies to both gatekeepers, like auditors, and regulators alike. It was perhaps best set out by a representative of the relevant audit professional body in the United Kingdom who said:

> It appears to me to be the … opinion of an unenlightened public … that an auditor must have failed in his duty if a fraud has been effected, whether it is eventually discovered or not.

That statement was made in 1885 and even a cursory review of academic material shows extensive writing on the audit expectation gap today, so it seems fair to assume that it has not gone away.

But what some recent examples show to me is that the damage of fraud to the regulatory system, investors, and also to any advisers or other gatekeepers who fail to see it means this is an area where everyone needs to be vigilant and improve. So let me move now to consider our own experience in dealing with issues around fraud and some possible risk factors to consider.

ASIC's experience in dealing with fraud

Common themes in fraud

I have already mentioned the audit standard dealing with fraud that I believe is an excellent starting point for considering whether something is amiss. But, for the next little while, I wanted to speak about some other common themes that I have observed from corporate or other failures where fraud has been alleged:

- *The dominant personality* – For example, if any one director has undue control over a listed company's assets and affairs, there is an increased risk of:
  - the company being party to non-commercial transactions, which favour that director's interests
  - the company not making full and fair disclosure of its financial position
  - the company's funds being misused or stolen.
- *The role of non-executives in a business* – Non-executives must be active in carrying out their duty of ensuring that directors and management are accountable for the management of the company. They must follow up on matters that come to their attention and require explanation.
- *Senior executives must be vigilant* – Senior managers have an independent responsibility to report concerns as to improper behaviour by directors or other managers.
- *Effective internal controls are essential* – Internal controls comprise the systems, methods and procedures adopted by management to assist in achieving efficient conduct of its business, adherence to management policy, safeguarding of assets, and the prevention and detection of fraud and error. Internal control procedures commonly include checking the arithmetical accuracy of the records, preparation of reconciliations, using control accounts and trial balances, approval and control of documents, conducting cash, security and inventory counts, limiting direct physical access to assets and records, and comparison of results with budget.
- *Gatekeepers (including auditors) must maintain an independent outlook and fulfil all their responsibilities* – Ineffective gatekeepers may substantially increase the risk of fraud. This was highlighted in recent years in a report by a Parliamentary inquiry into the collapse of Trio Capital, a firm that provided services for superannuation and other investments.

Preventing fraud

So what, then, are some protections to prevent fraud?

First, I think a business needs to spend the time in making sure it has the right culture. ASIC is concerned about culture because, together with financial incentives, it can be a key driver of conduct within the financial system and we regulate that conduct. Given that there often is a strong connection between poor culture and poor conduct, we consider poor culture to be a key risk area with respect to our role in taking enforcement action against poor conduct.

My position is pretty simple: Good culture should not mean mountains of red tape and armies of compliance staff. Rather, it is about people acting ethically and doing the right thing. If you have this, the need for a lot of internally driven rules falls away.

So what are some of the things that ASIC looks for when thinking about these issues? Let me mention three things:

- *Communication* – Expected conduct and behaviours in a firm need to be clearly articulated. It starts with 'tone from the top' and should permeate through the organisation.
- *Challenge* – Existing practices need to be challenged and employees should be encouraged to escalate potential practices or behaviours of concern. That means, in particular, effective programs to encourage and protect whistleblowers.
- *Complacency* – Boards should not become complacent about managing conduct risk (including the risk of fraud); it should be an ongoing process that is continually reviewed, enforced and validated.

More specifically, it may be helpful to ask the following sorts of questions:

- Does the firm have policies and tools available to staff and supervisors on what is acceptable and not acceptable conduct?
- Are customer complaints taken seriously and resolved in a timely manner?
- Has the board has approved a remuneration framework that rewards good, not 'neutral', conduct?
- Are there regular reviews of escalation process in place within the business?
- Do independent functions – such as legal, compliance, risk management and internal audit – have independent reporting lines (i.e. independent of the business they support)? This is often critical in ensuring the right issues are escalated.
- And, for the all-important question, what is ASIC planning to do in this area? A key thing is that more than ever we are intending to build concerns around culture into our existing risk-based surveillance reviews. We want to share information with boards and management when ASIC's surveillance suggests they want to do the right thing but there may be cultural problems within their firm that they are not aware of.

The second key protection against fraud is that the gatekeepers that work with and, in some cases, monitor the activities of businesses need to be vigilant and display professional scepticism in the work they do. For businesses, spending more money on good advisers and gatekeepers may ultimately be far cheaper than the money lost and reputational damage that occurs through a fraud.

Finally, the overall regulatory system needs to be operating in such a way that creates a credible deterrent to people committing fraud. That means when people weigh up the chances of being caught and the consequences of being caught it is just not worth them taking the risk of doing the wrong thing. This is not something that businesses will have direct control over, but I am pleased to note that as part of the Government's recent response the Financial System Inquiry, undertaken by David Murray, it is planned to undertake a comprehensive review of the penalties that apply for breaches of the law that ASIC enforces next year.

The future

The future consultation around corporate penalties is probably a neat way to move into a discussion about what the future may hold on these issues more generally.

I want to talk about two trends in particular that may not normally be associated with any discussion about fraud – those trends are globalisation and digital disruption.

Globalisation

A key opportunity presented by globalisation is allowing the free flow of capital across world markets. At the same time, misconduct across borders, such as the manipulation of financial benchmarks, undermines market integrity and stability. That makes it all the more important that in the future ASIC maintains strong and effective relationships with other regulators so we can access information about misconduct when we need it. As a member of the International Organization of Securities Commissions (IOSCO) we have access to much information from overseas regulators, and negotiations are underway to expand that the information we can receive even further.

Digital disruption

The other key trend to mention today is digital disruption. Let me provide some context – global investment in financial technology (fintech) ventures tripled to US$12.2 billion in 2014, from US$4 billion in 2013. This is a fantastic growth story. But this innovation provides both opportunities and risks.

Technological change has also increased the risks of cyber attacks and cyber fraud. The number, sophistication and complexity of cyber attacks have increased markedly in recent years and are expected to accelerate in the future. In 2013, cyber attacks affected 5 million Australians at an estimated cost of A$1.06 billion. The estimated annual cost of cyber attacks to the global economy is more than US$400 billion.

The increasing incidence, complexity and reach of cyber misconduct can undermine businesses and destabilise our markets, eroding investor and consumer trust and confidence in the financial system and the wider economy

In response to the long-term challenge of digital disruption to business models and channels, we will highlight the importance of cyber resilience in the coming year to promote trust and confidence in the financial system and market integrity.

Cyber threats are increasingly diverse and sometimes unforeseeable. With the evolution of technology and global interconnectedness, this risk is constantly changing. Cyber attacks are considered a systemic risk to the financial system, especially attacks on essential or critical services like banking and payments services or financial market infrastructure. Hacking of share trading accounts is a topical example of cyber fraud we are seeing more of.

It is not possible for businesses or individuals to protect themselves against every cyber threat. However, we encourage firms and markets to improve their cyber resilience, particularly where exposure to a cyber attack may impact on individuals or market integrity.

So what is ASIC doing about this? We will focus on:

- promoting cyber resilience
- identifying potential cyber attacks in our markets through real-time market monitoring
- ensuring compliance with licensing obligations, including the need for adequate technological resources and risk management arrangements and disclosure obligations
- coordinating and engaging with other Government departments to identify cyber risks and build cyber resilience.

I want to be very clear, however. ASIC can provide guidance and encouragement – and we have even, in some cases, provided some tools based on international standards against which people can assess their cyber resilience – but the question of what is the right level of cyber resilience for any company or licensee depends very much on who you are and what you do. What we want to do is try to raise awareness and provide guidance about an issue that is not just a regulatory matter, but something that goes to the heart running your business. Make no mistake – just as business is moving into the digital age, so are those who would commit fraud.

Conclusion

I have covered a lot today, so let me summarise and make some final points. ASIC and many other regulators and law enforcement agencies are in the trenches dealing with fraud.

But it is not our battle alone. Businesses are at the front line in dealing with this issue. I would argue they have no better protection against fraud then ensuring they have the right culture in their organisation. Gatekeepers also play a key role in the battle. ASIC will do our best to make sure they are doing their job, noting they cannot provide absolute assurance against fraud.

Finally, when things go wrong regulators do need to be there to both detect the misconduct and take action against the guilty. If this is to work effectively it is very important that the regulatory system provides the right toolbox and the right deterrence through penalties so people are not tempted to do the wrong thing. In that light, ASIC welcomes the Government's recent response to David Murray's Financial System Inquiry. That response proposed various additional powers for ASIC and also a review of penalties in the legislation we administer.

It is also important that the many Government agencies interested in fraud and other serious financial crime have the resources to deal with it and can coordinate their activities.

To this end, the Government has recently provided A$127 million over four years for a Serious Financial Crime Taskforce. While not solely directed to fraud matters, this dedicated funding will enable agencies to work together to target serious financial crime while still ensuring agencies can continue to meet their individual priorities.

Under the taskforce, partner agencies will apply their combined capabilities to remove the wealth derived from criminal activity and prosecute facilitators and promoters of serious financial crime. Over the longer term, partner agencies will draw on their expertise and understanding of their environments to ensure the effective sharing of information and to put in place credible deterrent and preventative strategies.

Together we want to work together to ensure that crime doesn't pay.