ASIC

Australian Securities & Investments Commission

Why breach reporting is important

A speech by Peter Kell, Deputy Chairman,
Australian Securities and Investments Commission

Risk Management Association (RMA) Australia CRO Forum

16 September 2014

Introduction

Thank you all for having me here today.

As risk professionals, you are not only important gatekeepers for your organisation, but you also play a key role in upholding the resilience of our financial system. At the core of our financial system is trust and confidence in our markets, institutions and financial services firms. You play an important role in maintaining this trust.

Today I want to focus on breach reporting by financial firms. The law requires financial services licensees to report breaches of the law to the regulator, but it has become increasingly apparent that this is not happening in a consistent manner across the industry. We are aware of some financial services licensees not reporting breaches to us in a timely manner.

So today I'm going to outline what ASIC expects from licensees in relation to breach reports, and the work that we're doing with the industry to raise standards on this issue.

Before I talk about breach reporting, I'd like to briefly talk about:

- ASIC's role and the environment in which we operate; and
- the role of risk professionals in promoting a culture of compliance within their firm.

ASIC's role and our environment

Markets cannot perform their fundamental purpose—funding the real economy and in turn economic growth—if consumers and investors do not have trust and confidence in them. This was a clear lesson from the GFC.

Making sure Australians have trust and confidence in our markets and financial services providers is at the heart of everything we do. It is what drives the excellent men and women who work at ASIC.

Our environment

We are living in a time of rapid innovation and change. Change brings opportunity, but also risk.

In this environment, the key external challenges for ASIC—as Australia's integrated financial services and markets regulator—are:

- structural change in our financial system through the growth of market-based financing, which is largely driven by growth in super;

- financial innovation-driven complexity in products, markets and technology. Much of this is driven by digitisation of our economy; and
- globalisation.

While these developments are all challenges, they also present opportunities to fund economic growth. Industry and regulators need to continue working together to harvest the opportunities while mitigating risks to consumer trust and confidence.

These issues are squarely on the agenda for the Financial System Inquiry, as it considers how best to deal with the needs of the financial system for Australia going forward.

ASIC's response to external developments

So, how does ASIC respond to these challenges?

We do this through our strategic priorities of:

- promoting investor and consumer trust and confidence;
- ensuring fair, orderly and transparent markets; and
- providing efficient and accessible registration.

In achieving our strategic objectives, a key aspect of what we do is identifying and dealing with those who break the law. That is, holding gatekeepers to account. We do this 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, which I will talk about a bit later; and
- reports from the public and from whistleblowers.

We *understand* trends and risks by analysing the intelligence we receive.

And, depending on our resources and powers, we *respond* by:

- educating investors (this is through ASIC's award winning financial literacy work, largely conducted under our MoneySmart program).
- providing guidance to gatekeepers;
- disrupting harmful behaviour;
- conducting surveillances on gatekeepers;

- taking enforcement action, which can be:
  - punitive;
  - protective;
  - preservative;
  - compensatory;
  - corrective; and/or
  - a negotiated outcome; and
- lastly, by 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 the law, we will do all that we can to ensure the ramifications are severe. Of course, the vast majority of organisations comply with the law and will have nothing to worry about.

Culture

My second topic for today is culture.

Lessons from the GFC, and from ASIC's experience in administering and enforcing our financial services and markets law more broadly, tell us that culture matters. And it matters in very concrete ways—for example, in remuneration and incentive structures for employees, and in the way that products are designed and marketed. If a licensee has a poor culture of compliance, there are likely to be breaches of the law. Poor culture also undermines customer trust and confidence in a licensee. Ultimately, this will impact the licensee's bottom line.

More broadly, sector-wide cultural problems destroy consumer trust and confidence in the whole sector. And in the financial services sector we see clearly that the problems created by poor culture can have a very long tail due to the long-term nature of products and services. This is an issue the financial planning industry is facing at the moment.

Risk professionals and culture

As I mentioned at the start of my speech, as risk professionals you are not only important gatekeepers for your organisation, you are also important gatekeepers in our financial system.

A key part of your gatekeeper role is ensuring that your organisation has a good culture of compliance. The tone is undoubtedly set from the top—by the board and executives like many of you in the room today.

Where appropriate, incorporating culture into your organisation's remuneration framework can be an effective way of entrenching culture in an organisation. For example, gate-openers for performance incentives can be tied to adhering to a company's culture, rather than just being sales based.

ASIC's consideration of culture in our regulatory actions

At ASIC, where we see that business models and incentive structures undermine a focus on better consumer outcomes we are likely to examine that organisation more closely. This includes the organisation's culture on breach reporting, which I will talk about shortly. An organisation's culture will also affect what regulatory outcome we pursue. The poorer the culture, the stronger the action we are likely to take.

Our goal is to address both the immediate and the underlying causes of a compliance failure.

Breach reporting

Now I'd like to move on to the main topic for today—breach reporting and our expectations of licensees in reporting breaches to us.

In particular, I'd like to talk about:

- why breach reporting is important;
- when breaches must be reported;
- what ASIC does with breach reports; and
- our current focus on breach reporting and the review we are undertaking to ensure that breach reporting requirement are consistently complied with across industry.

Why breach reporting is important

There is a clear expectation in the Australian financial services regime that participating firms will play a role in identifying and reporting market problems. As a result, the law requires the timely reporting of significant breaches to ASIC.

This is not a new requirement. In fact, ASIC's policy on breach reporting is set out in Regulatory Guide 78 *Breach reporting by AFS licensees* (RG 78), which is available on our website. However, due to some notable recent problems with breach reporting we have renewed our focus on this issue.

Section 912D requires licensees to notify ASIC in writing of any significant breach, or likely breach of certain financial services laws. The report must be

lodged as soon as practicable, and in any event within 10 business days of the licensee becoming aware of the breach or likely breach.

Breach reporting is an important part of the regulatory framework. ASIC has highlighted deficiencies in the approach to breach reports in several enforcement actions we have undertaken in recent times against both large and small firms. Reporting to ASIC in a timely way helps us identify and rectify problems with individual businesses. It also helps us to identify and assess emerging risks.

When breaches must be reported

Licensees must give written breach reports to ASIC as soon as practicable, and in any case within 10 business days of:

- becoming aware of either:
  - the breach—if the breach has already occurred when the licensee discovers it; or
  - the likely breach—that is, where the licensee becomes aware that they will no longer be able to comply with an obligation before the breach has actually occurred.
- the licensee determining the breach or likely breach could be significant.

To be clear, this means a licensee should not wait until after it has completed a full investigation to satisfy itself that the breach or likely breach is significant.

We have recently written to the Institute of Internal Auditors Australia (IIAA) to highlight these issues around timing, after they sought guidance from ASIC about breach reporting.

In this letter to the IIAA we highlight that licensees should not wait to report until:

- the breach (or likely breach) has been considered by the licensee's board of directors or legal advisers;
- they have taken steps to rectify the breach; or
- in the case of a likely breach, the breach has in fact occurred.

By all means, firms should consider what they may need to do to rectify a breach. However, they should not wait until then to report to the regulator. We have seen instances where efforts to rectify a breach, even if well intentioned, have taken so long that they have compromised ASIC's ability to investigate and take action once the incident was finally reported. This is a highly undesirable outcome for both the regulator and the financial services sector.

When does a licensee become aware of a breach?

In our view, this is when a person responsible for compliance becomes aware of the breach or likely breach. We expect a licensee's internal systems to ensure that the relevant people become aware of breaches in a timely and efficient manner.

To ensure compliance with the breach reporting requirement, licensees should have a clear, well-understood and documented process for:

- identifying breaches or likely breaches;
- ensuring that the people responsible for compliance are aware of those breaches;
- determining whether identified breaches are significant;
- reporting to ASIC those breaches or likely breaches that are significant;
- rectifying the breach or likely breach; and
- ensuring that arrangements are in place to prevent the recurrence of the breach.

The bottom line is: if in doubt, report the breach to ASIC. Err on the side of caution. We are happy to work with licensees who take their breach reporting obligation seriously.

Not reporting significant breaches is, of itself, likely to be a breach of the breach reporting requirement. It indicates that a licensee's compliance arrangements may be inadequate.

What does ASIC do with breach reports?

We carefully assess all breach reports we receive. Some reports will lead to formal enforcement action, but most will not. Why then are breach reports important?

Breach reports are useful for ASIC, and ultimately for the market, even where further action is not taken. Given we have limited resources, breach reports assist us to make better decisions about which matters we should prioritise for investigation. Such reports help us to determine:

- whether there are patterns of misconduct within an individual firm or across a market sector; and
- whether the firm in question has robust systems in place for identifying and reporting problems.

They are, in other words, a valuable source of intelligence, even if an individual report lodged with ASIC does not generate an enforcement outcome.

In most cases where we take no further action arising from a breach report, we find that the licensee is already working on or has rectified the breach. In such cases, we will generally notify the licensee that we do not intend to make further inquiries about the matter.

Timely and clear breach reports will ensure a more measured and constructive response from the regulator. However, I should note that if the breach is serious or systemic then rectification may still need to be accompanied by more formal regulatory action.

Where further action is taken by ASIC, it may include:

- working with the licensee to improve their compliance procedures;
- conducting a formal surveillance to see if there is a systemic compliance problem; or
- taking enforcement action against an individual within the firm (or who previously worked for the firm); or
- taking regulatory action against the licensee.

We take a number of factors into account in deciding how to respond, including:

- the timing of the matters included in the report;
- the plan for rectifying the compliance failure;
- whether the consequences, particularly to consumers, are able to be dealt with comprehensively;
- the culture of reporting breaches in the organisation and the quality of their breach reports; and
- whether the breach suggests there are more significant compliance issues within the business.

Inadequate or late reports indicate to us that the licensee may have problems with their own compliance culture.

In some cases, a breach report may indicate a need for technical relief from the law or a no action position where there is no consumer detriment or market harm. In these cases, we are happy to work with licensees on their relief or no action request.

Why are we focusing on breach reporting?

Breach reporting is a key source of market information for ASIC. As I mentioned before, it forms part of our ‘detect, understand and respond’ approach.

At ASIC we recognise that for all licensees, but especially larger firms, things will go wrong from time to time. Breach reporting is a measure of how effectively firms respond to problems. Is the response timely and transparent? Or is it slow and confused or, worse, covered up?

We have highlighted in some recent actions that some AFS licensees are not reporting breaches to us in a timely manner as required under the Corporations Act. Sometimes this is because of a failure in their compliance systems. Other times, it is because of a 'liberal interpretation' of the breach reporting obligation. Either way, we see it as a problem.

There is a clear community expectation that financial services firms need to take responsibility and play a role in lifting industry standards, and part of this comes from timely identification of problems within the industry.

This is why we are now focusing licensees and their compliance with breach reporting requirements. It is also a red flag to us that there may be other cultural or compliance problems with the licensee. Non-compliance is a criminal offence.

We have publicly flagged in recent submissions to inquiries that there is scope to consider whether a civil penalty regime is desirable for failure to breach report.

What we are doing?

ASIC is announcing a review of breach reporting by financial services licensees. ASIC will be reviewing and examining the breach reports we have received, including:

- who they are from;
- what is reported; and
- the timeliness of the reports.

We will then conduct a proactive review of some of the licensees we've identified as having a high risk of non-compliance.

For these licensees, we will be looking to engage with them to ensure the robustness of their processes for:

- identifying breaches;
- escalating breaches within the organisation; and
- reporting breaches to ASIC.

If we consider a licensee's processes for complying with the breach reporting requirement are inadequate, we will consider taking regulatory action. This includes pursuing an enforcement outcome.

And, as I mentioned before, a breach of s912D is a criminal offence.

Conclusion

I hope my talk today has given you an understanding of ASIC's focus on breach reporting. We expect such reporting to be timely and to occur within a coherent compliance framework. This should be a standard part of the business of financial firms in the Australian market.