FSR GPS Podcast Series
Episode 1 – Once more into the Breach

Michael Vrisakis	Hi everyone. I'm Michael Vrisakis, a Partner in the Herbert Smith Freehills Financial Services Team. Welcome to our podcast series called the FSR GPS. This series focuses on topical and emerging issues in financial services regulation which we think are the most strategic and important issues for our clients. Feel free to suggest topics you would like us to cover in the future but for now, we hope you enjoy today's episode.
Andrew Eastwood	Hi, I'm Andrew Eastwood, a Partner in the FSR practice at HSF with a focus on contentious regulatory issues.
Edward Einfeld	Hi, I'm Ed Einfeld and I'm a part of HSF's disputes practice with a focus on FSR Investigations and Litigation.
Tamanna Islam	And I'm Tamanna Islam, a Senior Associate with FSR Advisory expertise. So this episode is called "Into the Breach" and we will discuss the breach reporting regime and the industry's experience with it since implementation in November 2021. From our conversations across the industry, it is clear that breach reporting is now even more of a focal point than it was previously, and there continues to be uncertainty around legal and regulatory expectations. We have also recently had some updates from ASIC on its Reg Guide 78 on breach reporting and we think there continues to be a need for further guidance. One threshold issue that many people were concerned about before the new reporting regime commenced is how to determine when an investigation has commenced which starts the 30-day reporting trigger. Andrew, what has the experience been since introduction and what has ASIC been saying about this?
Andrew Eastwood	Well Tamanna, one of the key concerns that was raised in relation to the old breach reporting regime was that some licensees were taking far too long to investigate breaches and that lead to an important change in the new regime, specifically that, if there is an investigation into whether a significant

breach of a core obligation has occurred, and that investigation continues for more than 30 days, then that itself must be reported to ASIC.

Now the term investigation is not defined in the legislation which has meant that licensees and their advisers like us, have had to seek to reach a principal position as to when an investigation starts. And I don't think there is a consistent position across the industry on this. To some extent that's to be expected. The explanatory memorandum to the new regime expressly stated that what constitutes an investigation is likely to vary significantly depending on the size of the licensee's business and their internal systems and processes and the like.

So what guidance have we been given? Well, that same explanatory memo referred to an investigation as being a searching enquiry in order to ascertain facts. And we have been given some helpful guidance in that memo and in ASIC's updated regulatory guide to the effect that the following are unlikely to constitute the commencement of an investigation.

First, merely entering a suspected compliance issue into a risk management system. Second, the mere receipt of a detective control such as a complaint or a whistleblowing disclosure. Third, preliminary steps and initial fact-finding enquiries in relation to the nature of the incident, completed over short timeframe and conducted as an initial response to detective controls. And fourth, business as usual enquiries such as routine audits or other internal compliance review processes.

Now, there's some ambiguity about some of those points and I think beyond that, one of the most important things for licensees in this space is to be internally consistent as to when they say that an investigation commences. So with a number of licensees that we've worked with, we've sort to understand their typical process following the identification of an incident or issue, and determine when in that typical process an investigation will usually be taken to commence.

Tamanna Islam

Yeah, thanks Andrew. Some really useful points to consider there particularly around the importance of contextualising an investigation in a licensee's typical incident identification and escalation processes.

Shifting focus a little bit now, the breach reporting regime includes a number of deemed significant breaches which are automatically reportable regardless of significance. Ed, how have you seen the industry manage this aspect of the regime?

Edward Einfeld

Thanks Tamanna. It certainly is a long list of provisions that are automatically reportable. Some larger entities we work with maintain a list of deemed significant provisions which requires regular updating. Others approach this on a case-by-case basis. So we work with clients on both of these approaches including helping clients manage a list and providing guidance on making the case-by-case assessment.

There are two types of automatically reportable provisions that raise particular issues given how broad the obligation is. The first is misleading or deceptive conduct, and the second is the obligation under section 912A to do all things necessary to ensure that financial services are provided efficiently, honestly and fairly.

For misleading and deceptive conduct, the low bar for this can result in numerous breach reports for what may be essentially minor errors in describing a product or service. For example, on a website in circumstances where no one may have read it.

Another issue which has arisen in recent cases is whether incorrectly charging fees or failing to provide a promised discount to a client is itself misleading or deceptive conduct. These issues and others have seen institutions focus more closely on whether there is, in fact, misleading conduct. Rather than jumping straight from an error or misdescription to a conclusion of misleading conduct, we see licensees undertaking a more holistic analysis having regard to the communications as a whole and the overall engagement between the licensee and the customer.

Licensees are also discovering there are some important steps to take when assessing a breach of certain provisions that are deemed significant breaches, particularly in the context of criminal offence provisions. For example, not all defective disclosure failures are automatically reportable once you take into account the fault elements for a contravention, for example. So in this regard, it is important to understand the underlying elements of the provision you are assessing before determining that there's a breach.

Tamanna Islam

And what about the efficiently, honestly, fairly obligation you've just mentioned. We've seen this obligation over the last few years become a key enforcement tool for ASIC, particularly since it became a civil penalty provision back in 2019.

Andrew Eastwood

My experience, Tamanna, under the old breach reporting regime was that too often I saw licensees reporting a breach of the efficient, honest and fair obligation without much, if any, analysis. It was sort of seen as a fallback when something had gone wrong, that the conduct couldn't be pinned to any other more specific breach. And it didn't really have a sting attached to it given that at that time, the efficient, honest and fair obligation wasn't a civil penalty provision.

Now that it is, I'm seeing a lot more rigorous analysis being conducted as to whether there really is a breach of that efficient, honest and fair obligation and the area is not straightforward. Just in the last year, we've had a couple of very important court judgements on the obligation which have emphasised amongst our things, that perfection is not required. Errors in businesses, the sizes of banks and other large financial institutions will always occur. So in one case, there are apparently 7 million occasions when a fee was charged when it ought to have been waived but the court placed that figure in the context of the fact that the waiver had been correctly applied on over 600 million occasions and that raises squarely one of the most challenging issues which is how issues of materiality air on the assessment of whether there has been a breach of the efficient, honest and fair obligation.

Tamanna Islam

Yeah, thanks Andrew. There certainly has been some interesting case law on the assessment of breaches of both obligations recently. While we're on the topic of ASIC and ASIC's expectations as well, they've been on the public speaking circuit and issued a few public statements and reports regarding the approaches taken by reporting entities. What have been their key concerns with compliance to date?

Edward Einfeld

One of ASIC's principal concerns has been the variation in practice between different institutions and this was the impetus behind the release of the updated Regulatory Guide 78 in April this year. A key issue identified is how licensees are reporting the number of reportable situations or the number of instances related to a reportable situation. Given that the number of reportable situations and instances can be included in ASIC's public reporting, this can be a somewhat sensitive assessment. So ASIC has acknowledged that the various approaches taken don't enable it to obtain adequate, meaningful insights, in its words, to meet its needs. The regulatory guide provides some additional guidance on this, but ASIC has

---

said it needs to consult more to provide further guidance. And we understand there's currently no appetite for legislative changes.

In the meantime, the new guide contains an example of a broadly advertised but incorrect offer for a discount which is viewed by a thousand people, but only applied for by 200. ASIC says that the total number of clients affected is 200. But the number of instances to be reported should be 1,000.

Andrew Eastwood

That's right, Ed. ASIC also indicated that, as expected under the new regime, there's been a substantial increase in the number of reports being lodged. We've gone from 2,435 breach reports in the year from 1 July 2020 to 30 June 2021 under the old regime, to 8,829 in the nine months from 1 October 2021 to 30 June 2022. Now the number of reports coming in has meant that ASIC does not have the ability to review each and every report. They've been asking financial institutions in that context to contact ASIC through their relationship managers and the like in respect of very material breaches that ASIC would consider it needs to know about.

But whilst the number of reports has gone up dramatically, somewhat remarkably only 6% of the licensee population lodge reports in that 9-month period from 1 October 2021 to 30 June 2022. ASIC noted that this is significantly lower than expected and clearly believes that some licensees, particularly those who are smaller or mid-sized, are not reporting when they should be; ASIC says it's undertaking a range of activities to strengthen compliance with the regime and I think there's going to be a real focus on those licensees who are submitting no or a surprisingly low number of reports.

Tamanna Islam

Yeah, I think that's right Andrew and we're seeing this variation in approach not just across licensees based on size but also sector. In our experience, we've probably seen the highest increase in reporting across the insurance sector, both in life insurance and general insurance. One reason for this I suspect is the complexity of these businesses and the immense volume of products and distribution arrangements they are managing. From a breach reporting perspective, misleading or deceptive conduct, unsurprisingly, remains a large source of breach reports.

As you mentioned a little earlier Ed, the threshold for misleading or deceptive conduct is quite low which means that in the insurance sector, the breach reporting regime is picking up all sorts of administrative errors such

---

as one call centre rep failing to give a general advice warning or some other prescribed disclosure to a customer. Or, as you rightly mentioned earlier, an insurer failing to apply a premium discount accurately to a customer.

This raises some interesting questions touched on by Andrew earlier around some of the recent case law commenting that perfection is not required for a breach of the EHF obligation. Human error, as we know, is an inherent part of running a business and the Federal Court is now recognising that absolute perfection is not expected by customers or, in fact, the courts. But it remains that misleading or deceptive conduct is a deemed significant breach with a relatively low trigger point. And so, regardless, these incidents are now required to be reported to ASIC as significant breaches.

Another area with a relatively significantly volume of breach reports in our experience is in the context of disclosure. With most of the disclosure requirements under Chapter 7 now being attached to a civil penalty provision, isolated instances of disclosure deficiencies are now also required to be reported. A good example of this is where a licensee fails to insert a piece of prescribed disclosure into advertising. Under the old regime, this incident would not typically be treated as significant or reportable unless the issue was more sort of widespread or systemic. But because failure attracts a civil penalty, a single incident is now reportable.

And while we're on the topic of insurers, the other element of this is insurers as well as super trustees and banks have the added element of how APRA may view a particular incident and, in fact, whether there is a breach that is reportable to APRA. Before the new breach reporting regime came in, there was, in fact, greater consistency in what was required to be reported to ASIC versus what was required to be reported to APRA.

Ed, what are you seeing in the joint regulated space as between APRA and ASIC on breach reporting?

Edward Einfeld

Well Tamanna, a primary area of overlap is in relation to breaches of prudential standards. So most financial institutions are aware that there's a gap between the reporting regimes under the Banking Act, superannuation legislation and insurance legislation on the one hand and under the Corporations Act on the other. And that can have the effect that an investigation into a breach of a prudential standard might technically be reportable to ASIC before it's reportable to APRA.

The effect of this is that financial institutions need to consider ASIC reporting timelines when they're conducting investigations into breaches of

---

prudential standards, both in relation to the timing of the report but also the materiality or significance of a breach. The breach reporting regime contains a sensible provision exempting an entity from having to report both to APRA and ASIC, and this is going to impact on the content of the report to APRA, which you may want to meet in order to meet the requirements of that exemption.

We're also seeing closer coordination between the regulators and AFCA. So this includes, for example, AFCA referring matters to ASIC as well as ASIC determining its enforcement priorities after identifying issues that are giving rise to a series of AFCA disputes. In some cases we're also aware of AFCA reporting some matters to APRA.

Tamanna Islam

Yeah, really interesting Ed. I think it's also important to bear in mind that ASIC and APRA are two very different regulators. And because of APRA's role as the prudential regulator, many APRA-regulated entities will, in fact, raise or flag certain incidents with APRA from a supervisory perspective whether or not a breach is formally reportable. So that's just another interesting point to bear in mind. So I guess to round us out for today, Andrew and Ed, what do you think are the biggest existing or looming issues to watch out for? And what will ASIC's key areas of focus be over the next 12 months?

Andrew Eastwood

Well Tamanna, I think it will be important to see how ASIC develops its regulatory position on the unresolved questions that were deferred for further consultation when ASIC issued its updated regulatory guide in April this year. As we've discussed, the question of what constitutes misleading or deceptive conduct and whether each instance should continue to be automatically reportable is clearly still front of mind as an unresolved policy issue, and I guess we're hoping to see more guidance on that point in the next 12 months.

Edward Einfeld

For my part, I think that licensees need to be on the lookout for the trends that are likely to drive breach identification. So Andrew referred earlier to the fact that ASIC is a little dismay that the comparative lack of reporting of some entities, and it's going to be looking to take action to try to correct that which may include some high-profile enforcement action. One trend licensees should have front of mind is the recent call to arms by ASIC and the ACCC on ESG disclosures which has most firms reviewing what they

---

have said about their products and services. We've seen from ASIC's recent litigation in this space that any representations about environmental credentials that has not been properly substantiated can result in enforcement action. There's a great variety of opinions in this space as to what is and isn't misleading and, really, this could be a topic for a whole other episode. Thanks very much for joining us today.

You have been listening to a podcast brought to you by Herbert Smith Freehills. For more episodes, please go to our channel on iTunes, Spotify or SoundCloud and visit our website herbertsmithfreehills.com for more insights relevant to your business.
