INSTITUTE OF
PUBLIC
ACCOUNTANTS®

Comments to ASIC: CP 340 Breach reporting and related obligations

June 2021

03 June 2021

Niki De Mel
Strategic Policy Adviser
Strategy Group
ASIC

By email: BR.submissions@asic.gov.au

Dear Niki

CP 340: Breach reporting and related obligations

The Institute of Public Accountants (IPA) welcomes the opportunity to comment on CP 340: *Breach reporting and related obligations* and the draft revised RG 78 *Breach reporting by AFS licensees and credit licensees*.

The IPA is one of the three professional accounting bodies in Australia, representing over 42,000 members and students. Of these, approximately 900 operate in the financial advice sector. This number has been decreasing at an average rate of 13 per cent each year for the last two years. Three-quarters of the IPA's members work in or are advisers to small business and SMEs.

In preparing this submission, we have consulted with IPA members who work in the financial advice sector, as full and limited licensees.

Our comments below are mostly generic in nature, covering some of the issues raised in the questions in the consultation paper.

If you have any queries, please don't hesitate to contact Vicki Stylianou, Group Executive, Advocacy & Policy, either at [redacted] or mob. [redacted].

Yours sincerely

[redacted]

Vicki Stylianou
Group Executive, Advocacy & Policy
Institute of Public Accountants

Comments

Cost of compliance and implementation:

One of the IPA's main concerns is the cost of compliance for licensees and the cost of implementation for ASIC. Given the number of times we have commented on the lack of adequate resourcing for ASIC, we are not convinced that ASIC will have the capacity to adequately implement these requirements, which will undermine the policy objectives reflected in the Hayne Royal Commission recommendations.

IPA is also concerned that this may lead to an increase in the ASIC industry funding levy, which has already caused a significant amount of anxiety for regulated individuals. Advocacy to the Government and Treasury seeking a review of the funding model is ongoing.

We note (again) that costs cannot simply be absorbed by businesses, many of which are small professional services firms offering tax and advisory services as well as limited financial advice services. Passing on costs to consumers is also not practical and adds even more costs to an already prohibitively high-cost structure. We refer to ASIC CP332 and ongoing consultation.

We note the reference on page 18 of CP 340 under the heading 'regulatory and financial impact' that licensees do not incur 'unreasonable costs' in complying with these obligations. What does ASIC consider to be 'unreasonable costs'; and has ASIC taken the cumulative impact of costs into consideration? A RIS with a proper cost-benefit analysis with input from industry would be welcome.

IPA member comments fully support the above view on costs.

Guidance:

IPA believes that more guidance, case studies, scenarios and prescription are needed with respect to various concepts and requirements, including, 'core obligation', 'significant', reporting an 'investigation' to ASIC, 'material loss or damage', reportable situations involving 'serious fraud or gross negligence', 'knowledge', 'recklessness', 'reasonable grounds', and 'reporting to ASIC in a timely manner'. Guidance is needed wherever judgment is required. We anticipate that specific examples will be submitted by licensees.

IPA members have commented that:

- If individual licensing is implemented, then it would be very difficult to 'police' individual breach reporting as opposed to such reporting at a Licensee level. Guidance on how this should be implemented would be useful.
- Licensees would appreciate less ambiguity. A specific area would be the 'materiality' of the breach. This is ill defined and in the absence of clear guidelines, Licensees will tend to err on the side of 'over compliance'.

Member comments:

- In reality the current breach reporting regime has served the consumer well. Criticism has been voiced that the regulator itself was slow to act when concerns were voiced by consumers and the financial planning industry itself (eg Storm Financial, Mayfair 101 Funds Management).

- The recommendations from the Hayne Royal Commission impose many additional responsibilities on Licensees to those that currently exist. These additional requirements are more administrative in

nature and do not improve consumer outcomes by ensuring that Licensees and advisers act 'honestly, efficiently and fairly.'

- From an administrative perspective, Licensees will be required to adapt existing systems to give effect to the new breach reporting requirements. This will be more than a mere 'tick a box' approach as Licensees will actively assess, in more detail, the event of a breach or potential for a breach. This has the potential to create a significant administrative burden.

- Licensees will be under an obligation to review retrospectively a number of advices or activities of authorized representatives to ensure compliance with the breach reporting requirements.

- It could be argued that, in the context of a financial services industry struggling to evolve into a profession, these changes to the breach reporting requirements are not consistent with professional responsibilities of current Licensees who have met all of the recently imposed statutory and ethical requirements. In addition, if the cost of remediation is high, this may discourage breach reporting.

- There is evidence that PI insurance is becoming increasingly difficult to obtain and is increasing in cost. These additional requirements will add to the risk assessment by insurers, who may potentially increase premiums to compensate for risk. (IPA has an in-house insurance broker which has confirmed a tightening of the PI insurance market, meaning that it is becoming increasingly more difficult to obtain insurance (especially with financial advice services) and premiums are increasing significantly.)

Comments relating to draft RG 78:

- **Significance**: whilst draft RG 78 provides some examples of what will be deemed significant breaches, breaches that may be significant under the general test, breaches that may not be significant, and factors that determine whether a breach is significant, there will be many more instances in practice of what may or may not be covered under these categories, and what will be considered civil penalty provisions and/or relevant offences. We suggest that ASIC start compiling a list of other examples, and whilst this can never be exhaustive, it may be useful in providing more guidance to licensees.

  We note in accordance with the draft regulations which Treasury consulted on previously, that deemed significance for all civil penalty provisions (and certain criminal offences) means that almost all breaches will be considered 'significant' and reportable, regardless of their size or other factors that would currently be assessed in determining significance (eg impact on customers, number and frequency of similar breaches, etc). The legislation contemplates that regulations will be made to exclude certain provisions from deemed significance.

  We believe it will be critical to the practical application of the breach reporting system, to ensure that only appropriate breaches are 'deemed' to be significant. That is, IPA is of the view that this list needs to be further refined with a view to making it narrower and more workable in terms of what are genuinely significant breaches. There should be an ongoing assessment of the regulatory and cost burden imposed on licensees against the reporting of genuinely minor, technical, inadvertent, 'honest mistake', unproblematic, 'easily fixed' type breaches. Of course, the public interest is always paramount, but must be appropriately balanced. Our understanding is that Treasury will take a sensible approach and together with ASIC will make necessary and timely adjustments to the breach reporting system. It is also critical from the perspective of what breaches will need to be investigated or just reported to ASIC.

- **Investigations:** again, more examples would be useful in RG 78, noting that more instances will occur in practice. Further guidance should be included on when an investigation runs past the 30 days (and triggers the reporting obligation) as this, unlike when an investigation starts, is not necessarily a matter of fact and entails some level of judgment by the licensee.

- **Knowledge/recklessness:** we note a major change from the existing RG 78 which relies on when the person responsible for compliance becomes aware of the breach; to a situation in the draft RG 78 where ASIC will ascribe knowledge to anyone in the organisation who is acting within the scope of their actual or apparent authority. Whilst this may be consistent with the concept of 'recklessness' in the new breach reporting test, it will impose a significant regulatory compliance burden on licensees and introduces another level of ambiguity requiring clarity and specific guidance.

- **Compliance systems:** we fully support the inclusion on guidance on appropriate systems for identifying, recording and reporting breaches. However, not all licensees will have sufficient resources to implement and maintain systems to the same quality and ASIC should take this into consideration if assessing the efficiency of these systems. The main consideration should be effectiveness.

Case study: breach reporting in the accounting profession

We refer to NOCLAR (non-compliance with laws and regulations), which is essentially a mandatory professional standard imposed on professional accountants with a similar system of reporting actual or potential 'material' breaches of *all* legislation and regulations. A standard definition is,

NOCLAR comprises any act of omission or commission, intentional or unintentional, committed by a client or employer, including by management or by those charged with governance, or by others working for, or under the direction of the client or employer, which is contrary to prevailing laws or regulations.

All members of the three professional accounting bodies in Australia (IPA, CA ANZ and CPA Australia) must comply with NOCLAR, which emanated from the ethical standard setting body under the International Federation of Accountants (IFAC) (which is the major global governing body for the accounting profession).

The provisions under NOCLAR have proved difficult to interpret, apply and enforce in many situations which require judgment and are prone to subjective assessment. We suggest that ASIC may wish to consider this relevant example further in terms of the difficulty of making judgments in many situations in practice.

NOCLAR applies to all laws and regulations including, financial products and services, tax laws, environmental protection laws, public health and safety laws and so on. It requires professional accountants to assess the appropriateness of a response, including consideration of various factors, such as:

- is the response timely;
- has the matter been adequately investigated;
- what action has been taken to rectify, remediate or mitigate consequences;
- what action has been taken to stop NOCLAR or mitigate risk of re-occurrence; and
- has the NOCLAR incident been disclosed to the appropriate authority.

One major difference is that NOCLAR only has to be reported when the actual or potential breach has been assessed as 'material' and only then is an investigation and remediation required. The other major difference is that NOCLAR applies to the acts of others rather than to your own breaches as in the case of breach reporting to ASIC. NOCLAR allows the duty of confidentiality to be set aside – however, this may conflict with legislation in each jurisdiction in which it applies, which in turn presents its own set of issues.

However, given the similarities, we believe that NOCLAR may be a useful case study, including the approach to different types of guidance and practical application of a subjective standard. For more information, please refer to, NOCLAR.