FINANCIAL ADVICE ASSOCIATION AUSTRALIA

Friday 1 March 2024

Cyber Security Legislative Reforms

To whom it may concern,

The Financial Advice Association Australia (FAAA)[1] represents 10,000 financial advisers across the country in every suburb and town. They are charged with guiding and securing the financial futures of millions of Australians from all walks of life and all stages of their financial journey from study to careers to retirement and beyond.

As a result, advisers also take carriage of an extensive array of personal and confidential data about their clients. This information includes but is not limited to:

- Salary
- Assets and liabilities
- Investment decisions
- Health records, including previous medical conditions
- Sensitive interpersonal information about partners, children or significant others, and
- Career prospects.

It goes without saying that in the wrong hands, the circulation of this data could be very damaging to the personal lives of these clients and also to the advice business themselves.

Advisers have various obligations and responsibilities under a range of different regulatory regimes to collect and protect the data of their clients. That said, doing so, is a chief concern for many advice licensees and practices. This is an important issue that the licensees in the financial advice sector

[1] The Financial Advice Association of Australia (FAAA) was formed in April 2023, out of a merger of the Financial Planning Association of Australia Limited (FPA) and the Association of Financial Advisers Limited (AFA), two of Australia's largest and longest-standing associations of financial planners and advisers.
The FPA was a professional association formed in 1992 as a merger between The Australian Society of Investment and Financial Advisers and the International Association of Financial Planning. In 1999 the CFP Professional Education Program was launched. As Australia's largest professional association for financial planners, the FPA represented the interests of the public and (leading into the merger) over 10,000 members. Since its formation, the FPA worked towards changing the face of financial planning, from an industry to a profession that earned consumer confidence and trust, and advocated that better financial advice would positively influence the financial wellbeing of all Australians.
The AFA was a professional association for financial advisers that dated back to 1946 (existing in various forms and under various names). The AFA was a national membership entity that operated in each state of Australia and across the full spectrum of advice types. The AFA had a long history of advocating for the best interests of financial advisers and their clients, through working with the government, regulators and other stakeholders. The AFA had a long legacy of operating in the life insurance sector, however substantially broadened its member base over a number of decades. The AFA had a strong focus on promoting the value of advice and recognising award winning advisers over many years. The AFA had strong foundations in believing in advocacy for members and creating events and other opportunities to enable members to grow and share best practice.

take very seriously and are already devoting significant time and resources to manage. Financial advice is largely a small business sector, with a predominantly self employed business model. Whilst in some cases, advisers may be authorised by larger institutions, there are an increasing number who are self licensed or working within small licensees. Responding to cyber risk and crime has particular additional challenges for the small business sector that needs to be carefully considered. FAAA believes that cyber crime is a critical issue that requires a comprehensive Government response and we therefore are broadly supportive of measures to improve the visibility and oversight of cyber security incidents. We are supportive of a proactive response, and one with flexibility to learn from past experiences.

In the context of the field that we operate within, we will focus our feedback on Measure 2, regarding ransomware reporting. The FAAA is broadly supportive of there being better and more agile reporting by businesses of ransomware attacks and for clearer guidance around the security of critical infrastructure that the financial services industry operates under. The guidance for these responsibilities, in so far as it affects financial advisers, usually sits with the product providers themselves: superannuation funds, investment platforms, investment managers and life insurers. The FAAA engages with the representative bodies of these product providers to understand the key issues and to guide our members on how best to work with these data management and cyber crime requirements.

As evidenced by the high-profile incidents of Medibank and Optus, Australia is vulnerable to cyber-attacks and our economy should not be recalcitrant to change or adopting further appropriate reporting.

Most financial advice practices would meet the ATO definition of small business as featured in the consultation paper and attacks on these small businesses are limited. While it is true that some 80% of businesses have faced ransomware software attacks, only approximately 500 such attacks in 2021 eventuated in demands for payment for stolen data. We support, with appropriately scoped obligations, the reporting of ransomware payments.

Whilst we support the mandatory reporting regime proposed for ransomware, we are also strongly supportive of a no-fault, no-liability model. This will help to make it easier to report and to reduce the anxiety that may have been generated in reporting such situations to the Government.
We would also suggest that the requirements need to exclude any report of those types of cyber security emails that claim to have hacked an individual or a company's website, where payment has been demanded, however there is no evidence that there has been any loss of data.

We believe that the consultation questions below give scope to the genuine concerns that some have about cyber-security reporting protocols as proposed. If further information is sought on any of

the issues raised, please do not hesitate to get in contact with George John, Senior Manager, Government Relations and Policy at [redacted]

Yours sincerely,

[redacted]

General Manager
Policy, Advocacy and Standards
Financial Advice Association of Australia

FINANCIAL ADVICE ASSOCIATION AUSTRALIA

MEASURE 2

8. What mandatory information should be reported if an entity has been subject to a ransomware or cyber extortion incident?

The FAAA is supportive of the information that is listed on page 15. This appears to be a sensible list of information expectations. We would however suggest the addition of a data field for the number of clients impacted, if this is known.

The FAAA agrees with the consultation paper that at a certain point this information becomes burdensome for small businesses to produce. If it is expected that the number of these attacks was to increase, making the information both easy to collate and quick to distribute should be the guiding principles. Many of our members run and operate small businesses who have limited spare capacity. It would be a failing of the regime if reporting such an incident was seen as either oppressive or futile.

We would also support a model where there was the avoidance of duplicate reporting for entities that have other reporting obligations. This might include financial advice licensees who already have breach reporting obligations to ASIC.

It would also be necessary to enable some of this information to be left out of the initial report if it was not readily available or provided at a later point in time.

9. What additional mandatory information should be reported if a payment is made?

The, FAAA is happy to be guided by specialists in this area, however we would support the collection of information on how the payment was made, and any additional information that might help to identify who the criminal party is or what means they used to collect the ransom. We would appreciate that once such a report has been made, further questions may be sought by authorities and that answering these would continue to be covered by the no-fault and no-liability principles.

10. Which entities should be subject to the mandatory ransomware reporting obligation?

As stated below, we believe that this regime should apply to all commercial businesses, where client data is at risk. The FAAA also holds the view that any payment should be reported if the proposed no-fault and no-liability framework is enacted. Paying a ransom, we would suggest, represents a drastic and dramatic further step in the regular course of events of a ransomware attack and as such should be reported. Financial advice licensees take the issue of data security very seriously and it would be disheartening to know that some of these events would possibly happen in a vacuum with little to no government oversight. We are happy to suggest that based on the current projections of

payments made that all organisations who have engaged in the aforementioned acts should be part of a reporting regime. Financial advice practices are a prime example of the fact that the size of a business is in no way related to the nature of data kept or potential for hazard or harm.

11. Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?

FAAA believes that if the information to be transmitted under the reporting obligation is to be limited in scope than all businesses should be required to report. We would however suggest that the implementation of this new reporting regime be staged, to allow smaller businesses more time to prepare. Importantly, reporting should be optional for these smaller businesses during this staged commencement phase.

Should the Government choose to provide an exemption for small businesses, then we would suggest that small business should not be prevented from reporting, if they are willing to do so.

12. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?

FAAA would hold that as close to live information, would, on the surface, appear most beneficial but that, especially in the case of small businesses, may be limited by capacity to make such a report.

72 hours is a very tight timeframe for a small business. Particularly if this timeframe includes the weekend. Normally these matters will require some investigation and could require the appointment of a cyber security specialist. In financial services, breach reporting to ASIC allows for a 30 day timeframe. This would normally require undertaking detailed analysis of the issue and the compilation of more information than would be required for this ransomware reporting, so we would suggest that this would be the outer limit. Whilst a week would be a reasonable timeframe, it might be sensible to provide a longer timeframe for smaller businesses (possibly two weeks). Clearly businesses would be encouraged to report as soon as possible.

13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident to Government?

FAAA notes that the consultation paper gives no clear advice on paying a ransom other than to "strongly discourage" but notes that there "may be some circumstances" where a payment is made. This speaks to the fast-changing cyber-security environment. If no clear line can be made about such payments, businesses, especially small often family-owned ones, should not be held liable for making what they believe is the best decision for their business on the basis of the information as it

is before them. It would be a disappointing outcome for our members if they were to be punished for not only this decision but then also trying to make the best of a bad situation and alerting authorities. It should be noted that the consultation paper does not adequately explain what no-fault and no-liability mean. This should be made clearer. In the context of some recent scandals with cyber security attacks on large Australian corporations, it is difficult to so easily attribute a no-fault and no-liability model to these businesses, however in the case of small businesses, this is very appropriate.

14. How can the Government ensure that the no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?

As mentioned above, financial advisers already have a range of responsibilities to protect the data and identities of their clients. Some of this is further covered by the government's expansive AML/CTF requirements.

It is also important to recognise that businesses caught in a cyber crime or ransomware matter are subject to significant reputational damage. Particularly for large businesses, the consequences of this are likely to be greater than the consequences of any regulatory enforcement.

15. What is an appropriate enforcement mechanism for a ransomware reporting obligation?

Whilst we note the suggestion of a civil penalty regime, we are also conscious that some civil penalty regimes can involve very significant fines. That should not be the case for small businesses. Potentially the enforcement regime should involve a relatively small penalty. An alternative to a civil penalty regime would be an infringement notice payment. This would be more straight forward and avoid the need for a court case (which would be required for a civil penalty provision matter).

16. What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, with whom, and in what format?

We believe that public reporting is important for businesses and individuals to understand the prevalence of cyber crime and ransomware matters. This reporting would not need to be at the entity level and in fact would be better if it was summarised at the industry, sector and company size level. These factors would need to be considered in finalising the reporting obligations.

Factors that would be important to include are the number of consumers involved, the type of incident, the type of risk prevention failing and the cost of any ransomware payments.

We are conscious that there are potential implications in this reporting, including the risk that it could encourage further participants in this space, or if the information provides any insight into how this

type of crime is most effectively acted upon. This would necessitate careful consideration of what to report and how to report.