



Lawcadia®

gadens

State of Financial Services Breach Reporting in Australia

Insights from the first 6 months of the
new AFSL & ACL regime

Research Partner

CORE|DATA
research

Contents

Introduction	3
The regime	4
About the research	5
The need for change	6
Impact on industry	7
Stress & anxiety	9
More breaches reported	11
Different types of breaches reported	13
Is the regime achieving its purpose?	14
Do those who need to know, actually know?	16
Investment in systems, processes & resources	18
Optimism for the future	19
Acknowledgement	20

Introduction

Lawcadia and Gadens are pleased to present the results of the inaugural State of Financial Services Breaching Reporting in Australia. The first of its kind in Australia, the statistics and insights gathered in this report address what has become a significant pain point in the financial services industry.

AFSL and ACL holders are required to self-report noncompliance of laws to ASIC and are subject to civil and criminal penalties if they do not.

Of course, depending on the matters reported, they are subject to legal proceedings, licence changes, reputational issues, and individual consequences when they do.

This report is a culmination of a combined passion and desire to advocate for the financial services industry, who have faced significant challenges to meet enhanced breach reporting obligations since they came into effect on 1 October 2021.

Over the past 6 months, anecdotal evidence has suggested an industry struggling to meet and maintain the onerous compliance demands, however, there was no independent data or research established to effectively shine the light on the challenges reverberating through financial services organisations.

Further, ahead of mid-year, when ASIC will publish breach reporting statistics for organisations, there has also been great deal of angst across the sector.

Australian headquartered legal technology company Lawcadia, and Gadens, a national law firm with a leading financial services regulatory practice, considered it essential to quantitatively and qualitatively understand the ramifications of the new breach reporting obligations to legal, risk and compliance teams.

We wanted to add real value to our clients, by giving unique insights upon which practical measures can be taken.

In January 2022, we commissioned CoreData Research, an independent research firm, to conduct an industry-leading research study to understand the key challenges, potential benefits, and how the industry has received the new regime.

This research reveals:

- A **marked increase in breach reporting** for AFSL and ACL holders.
- A suggestion that **ACL holders may be lagging behind AFSL** holders in reporting.
- Particular **increases in breach reporting around misleading & deceptive conduct, and advice-related failures** e.g., failure to provide a “general advice warning”.
- Widespread **acceptance that changes were needed** to how financial services organisations identified, assessed, and remediated breaches.
- Broad agreement that the **mandated approach is excessive**.
- A **low level of confidence in the new breach reporting regime meeting its stated objectives**, and **ASIC’s ability to administer the new regime effectively and fairly**.
- A significant **increase in compliance and resourcing costs**, and greater **adoption of technology solutions** to assist in meeting obligations.
- A **toll on mental health** with a high level of stress and anxiety experienced by legal, risk and compliance professionals tasked with planning, implementing and administering the regulatory requirements.

We want to thank the 160 respondents from financial services organisations who participated in the survey and the eight regulatory, risk and compliance leaders who generously provided their valuable time to share insights and their personal experiences via in-depth interviews. Without your generosity and support, this important study would not be possible. We hope that you find the research report insightful and relevant, and encourage you to reach out to us if you have any queries or comments.



Sacha Kirk
Co-Founder & CMO
Lawcadia



Liam Hennessy
Partner
Gadens

The regime

The new breach reporting obligations implement recommendations from the *Financial Services Royal Commission and are included in the Financial Sector Reform (Hayne Royal Commission Response) Act 2020*. These obligations require AFSL and ACL holders to self-report specific matters to ASIC and allow ASIC to detect noncompliance behaviours early and take action where appropriate. The regime is completely new for ACL holders.

The primary shift under this new regime is to a more expansive scope of “reportable situations” (i.e., matters that must be reported to ASIC), and the introduction of “deemed significant breaches”. Largely gone are the days of subjective assessments of the “significance” of a particular issue, with the decision of whether a matter is reportable to ASIC or not hinging on that assessment. There is now far more prescriptive rigour around what is reportable to ASIC.

“Deemed significant” breaches, which must be reported to ASIC irrespective of the number of customers affected, the quantum of loss, or broader impact to compliance frameworks, include:

- breaches that constitute the commission of an offence and the commission of the offence is punishable on conviction by a penalty that may include imprisonment for:
 - a. three months or more if the offence involves dishonesty; or
 - b. 12 months or more in any other case;
- breaches of a civil penalty provision (if the provision is not exempted under the regulations);
- for AC licensees, breaches that constitute a contravention of a key requirement under s111 of the National Credit Code;
- breaches that amount to misleading or deceptive conduct; or
- breaches that result, or are likely to result, in material loss or damage to clients.

Instead of the subjective test previously utilised to determine whether a breach had occurred, breaches are now automatically deemed significant and reportable within 30 days if they contravene any one of thousands of relevant Australian civil or criminal penalty legislative provisions. A useful flow chart of the regime can be accessed in the footnote below.¹

If a licensee does not report all “reportable situations” to ASIC, they may be subject to both civil and criminal penalties for every instance of failed reporting. For larger licensees where there may be hundreds of reportable situations occurring annually, the quantum of fines that are able to be levied by ASIC are significant.

AFSL and ACL breach reporting can have hugely consequential impacts on organisations and individuals.

Court proceedings, loss or variations of licences, adverse media attention and individual career impacts have been the result of breach reports.

Particularly in the current environment when ASIC’s mantra is “*Why not litigate?*”, the level of concern with the dramatic increase in the scope of reporting across the whole financial services industry is understandable.

¹ <https://www.gadens.com/legal-insights/breach-reporting-workflow-chart-afsl-acl-licensees/>

About the research

Gadens and Lawcadia commissioned research firm CoreData to undertake research into the impact and perceived effectiveness of mandatory breach reporting requirements of the *Corporations Act*, which came into effect in October 2021.

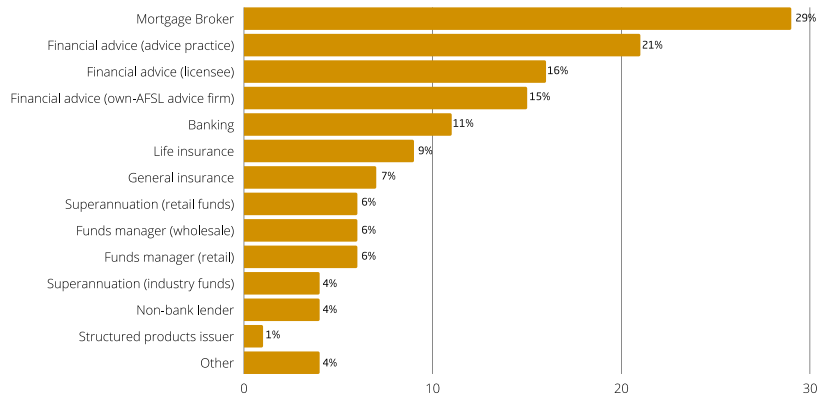
A detailed online survey conducted by CoreData in March 2022 received 160 valid and complete responses from respondents that hold compliance and compliance-related roles in the financial services sector. These participants were screened for appropriateness.

The survey was supplemented by eight one-on-one interviews with CoreData, conducted in April 2022 with selected survey respondents via Teams or Zoom. Most were institutional employees.

160 industry professionals responded

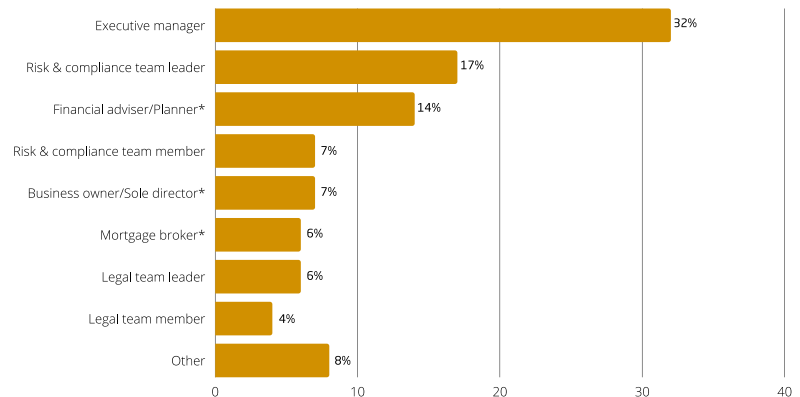
8 one-on-one interviews conducted

In which sector of the financial services industry is the entity by which you're employed?



* Multiple response allowed
n = 160, Overall

What best describes your role within your organisation?



* Additional option from other mentioned answers
n = 160, Overall

Note: Percentages in all data charts have been rounded to the nearest whole number.

About CoreData Research

CoreData Research is a global specialist financial services research and strategy consultancy, founded in 2002 and headquartered in Australia, with operations in Sydney, Perth, London, Boston and Manila.

It provides clients with bespoke and syndicated research services through a variety of data collection strategies and methodologies, along with consulting and research, database hosting and outsourcing services.

The need for change

There is widespread acceptance across respondents that changes were needed to how financial services organisations identify, assess, report, and make good on breaches.

“Clearly there was a problem... it’s unacceptable to be aware that you’ve been charging dead people fees and then not remediate that for years. I mean, this is terrible wrongdoing.”

Chief Risk & Governance Officer

“It’s definitely beneficial for the industry... Especially if it helps to identify any systemic issues or systemic breaches, and the regulator is made aware of it, the licensee can address it and they can rectify it, remediate it. I think it’s going to be good.”

Head of Compliance

“There was some startling statistic ASIC released at one point that AFSL holders were taking four years to notify breaches on average. I mean, that’s appalling.”

Deputy Chief Risk Officer, Head of Compliance & Regulatory Risk

“Whoever provides [financial services] for money, has to do it transparently. So, I absolutely support the changes, both in the area of Regulatory Guide 271 in regards to complaints, and the reporting of breaches to ASIC.”

Legal Counsel

However, there is equally a belief that the Government’s approach to the existing mandatory breach reporting regime for AFSL and ACL holders is excessive. It is important to note here that Treasury was the policy creator, and not ASIC per se.

“[This is a] sledgehammer to crack a walnut.”

Deputy Chief Risk Officer, Head of Compliance & Regulatory Risk

“It just isn’t as efficient as it could be, and it isn’t putting a spotlight on the things that really matter. It dilutes that by wanting all these other things that are unimportant. And I just worry that particularly for... AFSLs, that it’s really taking them away from the real issues. I think the pure time and energy that’s being put into it, it’s just not warranted and I’m not sure that it’s adding much value, to be honest.”

Head of Compliance & Conduct

Impact on industry

The research has found that the impact of the breach reporting obligations is being felt within financial services organisations in multiple ways. An initial ramp-up in workload occurred as organisations digested the content of their new obligations and mapped out implementation plans, and as they developed internal policies and procedures.

Key statistical findings from the survey of 160 industry respondents highlights that:

53%

of respondents cite the complexity of the new rules as a source of challenges, along with almost half (46%) who cite resourcing as an issue.

37%

of respondents identify training of staff as a complexity caused by the obligations, and about a third (33%) say there are issues related to systems for implementing and administering the rules.

55%

of respondents say the breach reporting regime has led to an increase in how much their organisation is spending on compliance.

A significantly increased workload has continued in the aftermath of the new rules coming into play, as organisations grapple with the tasks of identifying incidents, and then investigating and assessing these incidents to determine whether they are required to be reported against thousands of Australian civil and criminal penalty provisions.

“I think the largest problem that we have with this is the amount of additional work that’s involved with the new regime...but the main problem we have an issue with is ‘deemed significant’. They’ve set the bar too low in my view, and we’re having to report a number of issues that to be perfectly honest are rats-and-mice-type matters, because they fit within ‘deemed’. So, they’re deemed significant but, to be perfectly honest, they’re not at all particularly material or what I would consider significant in a non-technical sense.”

Head of Compliance & Regulatory Affairs

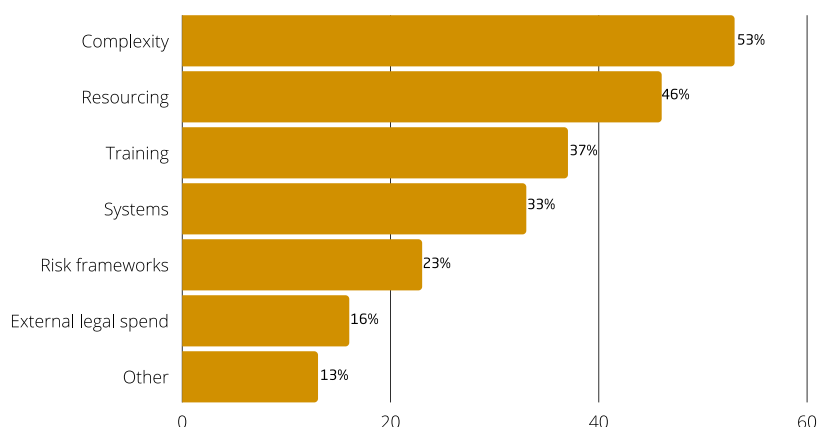
“It did require a large amount of time being directed towards getting ready for all those changes that took place throughout October and the big one really, was the mandatory breach reporting. Unfortunately, the other stuff doesn’t stop, so it wasn’t a matter of replacing what I was doing. You’ve still got to keep doing all of the other stuff that you do, unfortunately. So, as a result of having to prepare and get ready for all these regulatory reforms, it required working overtime, working late nights, working on those weekends, to make ends meet.”

Head of Compliance

“The way it’s drafted [there] are all of the things that if you trip up on in any one of these provisions, then you have to report a breach, regardless of materiality, regardless of impact, regardless of who is affected. ASIC haven’t gone, here’s a definitive list, which would be helpful.”

Chief Risk & Governance Officer

What issues and challenges are you facing?



* Multiple response allowed
n = 160, Overall

Stress & anxiety

The qualitative interviews revealed a high level of stress and anxiety experienced by the individuals responsible for preparing, implementing, and administering the new rules, with reports of increased workload, and uncertainty over both the operation of the rules as well as determining what volume of breach reports might be considered “normal” compared to peers and competitors.

This is especially so in cases where ASIC is publicly reporting this data in June 2022. Some raised concerns that ASIC may find itself deluged with junk data as a result of this uncertainty, and as a result of organisations reporting breaches just to be on the safe side.

Interviewees also spotlighted a need for more data and insights on breach reports to help them form views more quickly on which incidents do and do not warrant further detailed assessment or further investigation, and which ultimately need to be reported.

For now, individuals responsible for implementing the obligations report a heavy and often highly manual process of identifying incidents, investigating, and determining which need to progress to reporting.

The tools to respond to the enhanced AFSL and ACL breach reporting regime, given the complexity, scale and importance are lacking in the industry.

Expert insight

These findings are interesting in the context of upcoming potential licensing changes e.g., CASSPr licences for the crypto industry.

The stresses and pressures currently felt by those in the financial industry is against the backdrop of the governance, custody, risk and compliance frameworks those organisations have built over decades – especially the AFSL holders.

Those in new industries which are likely to be brought into the fold of the financial services regulatory regime will no doubt have similar if not higher levels of trepidation.

“

“Look, in the beginning, I have to say it was extreme. Extreme. Absolutely. I think for most of us in the team, I would say that we sort of are all in agreement when we say that we’d never had a more difficult time at work, in a workplace. It was very extreme, because we had significant regulatory change, outside of mandatory breach reporting.”

Head of Compliance & Conduct

“I personally find it extremely stressful. I’m finding it really, really difficult. My team are so, so busy with the increasing complaints, that they have little to no capacity to deal with incidences and breaches, so it primarily sits with me... It’s getting difficult to resource up. And you know, as the team leader it’s my responsibility to get it done so I just have to get it done. That’s a big issue.”

Deputy Chief Risk Officer, Head of Compliance & Regulatory Risk

“I feel worried. I feel concerned. I feel scared. Same as our CEO and our team members as well... They understand that even one big compliance incident can catch attention from the regulators, from the community, which can cause massive reputational damage to a business like us. So, everyone’s just scared.”

Head of Compliance

”

Compounding the stress and anxiety experienced by legal, risk and compliance professionals in responding to and meeting the requirements of the regime, is the concern that other important issues might fall through the cracks.

“Another risk and concern out of this is because once something gets reported to a regulator, even though to be perfectly honest its quite [minor], in some cases, it then gets bumped higher up the list of things to fix. We’ve got to get it fixed by a certain date and there’s a desire not to have that date too long which means that sometimes there can be, in my view, probably an improper prioritisation of addressing that issue, rather than something that is probably more significant even though not necessarily reportable. And don’t get me wrong either, we would still be investigating these issues. We would still be remediating these issues. I’m just concerned that at times it mucks up the prioritisation of what gets done when.”

Head of Compliance & Regulatory Affairs

“In the first sort of three months, I think we’ve really, really struggled and we’re just sort of getting over the line and what I mean by that is, kind of just keeping the lights on, in the BAU world and then fulfilling our obligations under the [mandatory breach reporting] requirements. I think that’s gotten a little bit easier over time.”

Head of Compliance & Conduct

Expert insight

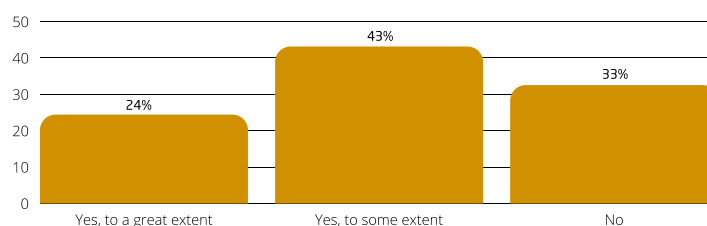
The other important areas of compliance indicated here may include overlapping regimes which also require breach reporting, and where troubles can arise, such as the Banking Executive Accountability Regime / Financial Accountability Regime, AML/CTF regime and OAIC regimes.

Given that an AFS and ACL holders breach report may (and most likely will) overlap with one or more of these regimes, these areas of focus cannot be neglected lest other regulators become activated.

67%

of respondents say the new breach reporting obligations are distracting or diverting resources away from other important areas of work and compliance issues.

Is compliance with the new breach reporting regime distracting you or diverting resources away from other important work areas and issues?



n = 160, Overall

More breaches reported

The critical quantitative insights from the breach reporting regime are set out below. They offer AFSL and ACL holders a unique indication of what to expect when ASIC releases its public statistics in June 2022, and an early chance to benchmark with the broader industry given the breadth of respondent organisations to the study. Practical decisions can then follow, which has been Gadens' and Lawcadia's aims in commissioning this independent research for the financial services industry.

The research findings highlight that:

- Almost nine out of 10 (86%) respondents said that before the breach reporting obligations came into effect, they were reporting fewer than five breaches each month.
- Since the obligations came into effect, however, that figure has dropped to around seven in 10 (71%).
- The proportion of over 160 respondents reporting more than five breaches a month has jumped from fewer than one in 20 (4%) to almost one in five (19%).
- Roughly the same proportion of respondents (10% and 11% respectively) do not know how many incidents are being reported.

In other words, the introduction of the breach reporting obligations has led to a noticeable increase in the number of breaches being reported.

Importantly, only AFSL holders were subject to the breach reporting regime prior to 1 October 2021. The increases relate to them, as ACL holders have no prior benchmark; they are reporting for the first time.

26%

of respondents surveyed are reporting more breaches than they expected to.

“

“It’s that civil penalty and imprisonment qualifier that brings technical breaches into the reportable sphere, that I think is the glitch in the reform. So, first of all, it actually takes a lot of effort to figure out if you’ve breached one of those provisions. The ‘misleading and deceptive’ one’s pretty obvious, and there’s a few others there; but there’s other stuff where you might trip over it, and you may not know, either. I’d love to have a chat with whoever drafted that provision, because I’d like to know if they sat down and researched all of the civil penalty units under Commonwealth law. I’d be really curious to hear.”

Compliance Manager

”

As the qualitative interviews revealed, apart from incidents that are obviously non-reportable and those that are unquestionably reportable, there is a grey area where incidents are being reported “just in case”.

In addition, there is a significant amount of work being carried out on the investigation and assessment of incidents that are ultimately deemed non-reportable, simply so that the decision to not report can be effectively defended if later challenged. This time spent investigating is proving to be a significant impost.

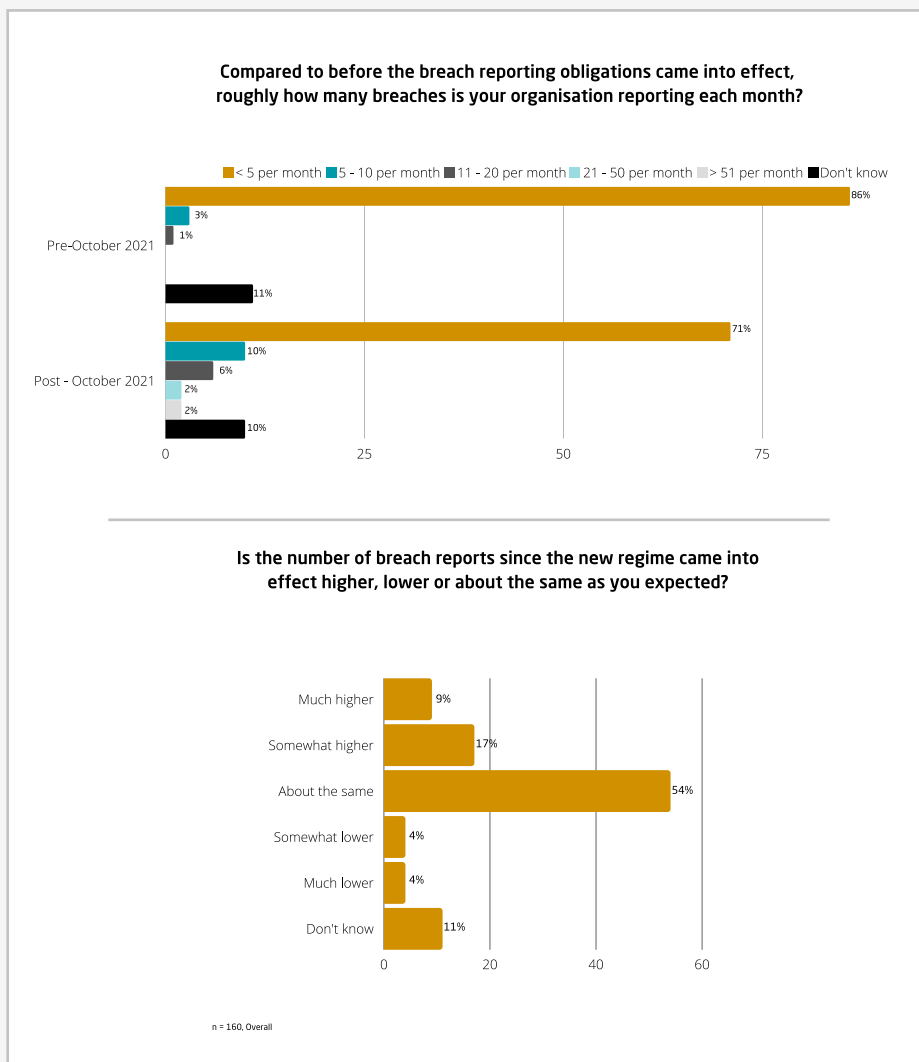
In terms of expectations amongst the industry, while just over half (54%) of respondents say the number of incidents being reported is about the same as they expected it would be, more than a quarter (26%) are reporting more breaches than they expected to.

“[It] all takes time and is still nothing compared to the time that it has taken us to get to from say, 100+, 200+ incidents down to 15 that are reportable. Because all of those that didn’t end up being reportable, some of them - say half - may have not been a lot of effort because it may be very clear right from the start that they weren’t going to be reportable. But, the other - say, 50% - [take] quite a bit of work. Investigation. Speaking to the business. Understanding the incident. Then assessing it against the legislation. Sometimes having to seek legal advice. That’s all very, very time consuming.”

Head of Compliance & Conduct

“It’s causing, especially for smaller organisations, significant pressure, resourcing pressure to try to not just simply be across all possible incidents that are going on, but the investigatory work that’s required.”

Senior Compliance Manager



Different types of breaches reported

The respondents surveyed were asked about the type of matters generative of their breach reports from 1 October 2021. Gadens and Lawcadia saw value in not only identifying the quantitative trends of AFSL and ACL breach reporting under the new regime, i.e., increasing or decreasing, but also specific aspects to assist licence holders in directing their focus to these problem areas.

Interestingly, in terms of the types of issues generative of breach reports under the new regime, the greatest proportion of reports have arisen from:

- Advice-related issues (23%), suggesting the provision of “general advice” and “personal advice” is a particular pain point in the financial services industry
- Misleading and deceptive conduct issues (18%)
- Conduct issues (14%)
- Administrative and legislative issues (11%)
- “Material loss or damage” inflicted on consumers (9%)

Unsurprisingly, respondents indicated that they are now reporting on behaviours or events under the new regime that they would not have reported prior to 1 October 2021.

Of the issues that are now being reported, almost one third (30%) of respondents have reported misleading and deceptive conduct issues, followed by conduct (28%), advice-related issues (27%), and material loss and damage (21%).

“Previously, we didn’t have these obligations. None of our incidents were ever considered for reportability. If we had serious issues, [we] may have had conversations around whether we thought those were worth discussing with ASIC. So, for us, that has definitely changed. Now, every incident that we look at, we’ll look at with that lens and that consideration and assessment. And also, our number of incidences increased because we now require things that weren’t considered an incident before, to be considered incidents and to be raised as incidents...purely so that they can be assessed for reportability.”

Head of Compliance & Conduct

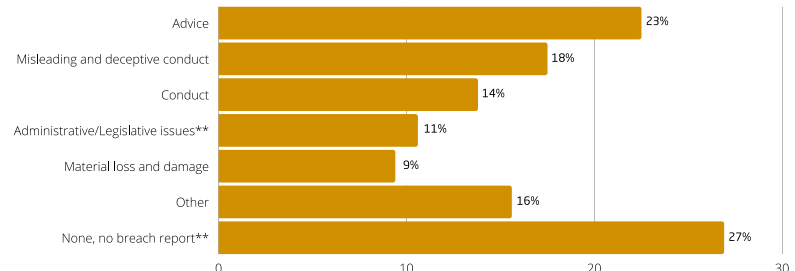
Expert insight

It is unsurprising that of the breaches reported to ASIC, “misleading and deceptive conduct” under s. 12DA of the ASIC Act, followed by “material loss and damage” to consumers, are prominent.

That is because s. 12DA is a strict liability provision where organisations do not need to have misled the consumer in order for it to be satisfied, e.g., an incorrect fee statement quickly corrected arguably still triggers the section.

Additionally, “material loss and damage” is to be assessed from the consumer’s perspective, not the licence holder, and takes into account monetary loss and time-based loss. If a client only has \$55 in their account, and they lose \$22.50 to an erroneous fee, arguably, that should be reported as a breach.

What are the most common kinds of behaviours or activities that have led to breach reports?



**Multiple answers allowed
** Additional option from other mentioned answers
n = 160, Overall

Is the regime achieving its purpose?

The research has revealed a sharp divergence in how effective the industry believes the new rules are. For example, roughly a third (31%) of survey respondents say they believe the new reporting obligations are not at all effective in meeting their stated objectives, while around a quarter (26%) say they believe the new rules are completely effective.

Around four in 10 (39%) believe the obligations are not at all effective in improving consumer protection, while again, roughly a quarter (24%) believe they are completely effective. Around four in 10 (43%) believe the rules are completely ineffective in improving consumer outcomes in the form of better products and services, while two in 10 (20%) say they are completely effective. These results occur against the backdrop of an industry grappling with significant influx of regulatory changes post Royal Commission.

31%

of respondents surveyed say they believe the new reporting obligations are not at all effective in meeting their stated objectives.

“All of this energy spent on this stuff isn’t improving consumer outcomes.”

Chief Risk & Governance Officer

“The benefit to it is that it’s going to hold licensees accountable to a higher standard.”

Head of Compliance

“If you’re finding breaches right now, I think overall, it’s got to have a better outcome for the customer because, ideally, if you’re doing the things that you should be doing, then that should have a flow-on effect, and it should mean that customer outcomes are better overall. Is it happening right at this moment? I think it’s early to say because we [only] went live in October.”

Head of Compliance & Conduct

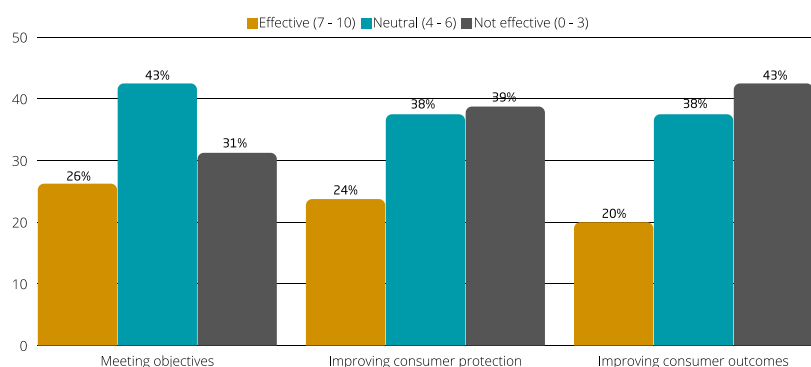
Expert insight

ASIC is an incredibly proficient adopter of RegTech, and the new enhanced breach reporting regime is no different – our understanding is that its capability in processing large amounts of data through its new purpose-built breach reporting portal is appreciable.

Respondents appeared to focus on whether ASIC has the resourcing, and budget necessary to respond to all breach reports meaningfully – in particular in circumstances where many are not objectively very serious.

We think this is a valid, though potentially separate point from its capacity to parse the data and focus on particular industry areas of concern.

On a scale from 0 to 10, where 0 means “not at all” and 10 means “completely”, how effective do you believe the new breach reporting regime is in...?



Text shown to respondents: The Explanatory Memorandum to the Financial Sector Reform (Hayne Royal Commission Response) Bill 2020 says: “Breach reporting is a cornerstone of Australia’s financial services regulatory structure. Breach reports allow ASIC to detect significant non-compliant behaviours early and take action where appropriate. It also allows ASIC to identify and address emerging trends of non-compliance in the industry.”

n = 160 Overall

Crucially, around half of survey respondents (51%) do not believe that ASIC can administer the new regime effectively and fairly across all financial services providers.

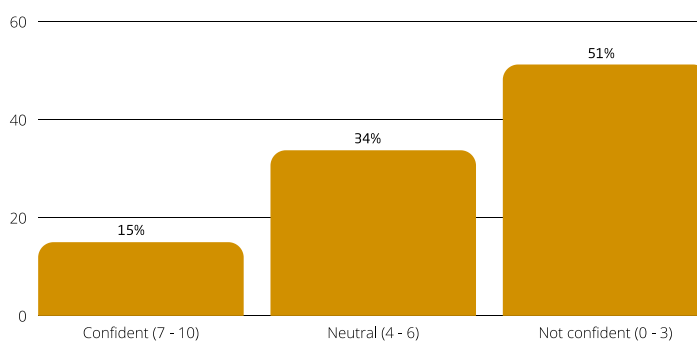
In comparison, only around one in seven (15%) believe the regulator will be completely effective.

The qualitative interviews highlighted the concern that the volume of breach reports being made to ASIC may overwhelm the regulator and may not help ASIC in pinpointing emerging areas of genuine or significant non-compliance, which is one of the core aims of the legislation.

“I think there is a risk in the quality of what’s submitted and the quantity as well. If someone is submitting heavy volumes, there might be a misguided perception that it is an outlier institution, and that there are a lot of problems there, because we’ve got all these other institutions not reporting as many matters. ASIC needs to be careful of that.”

Senior Compliance Manager

On a scale from 0 to 10, where 0 means “not at all” and 10 means “completely”, how confident are you that ASIC can administer the new regime effectively and fairly across all financial services providers?



n = 160, Overall

“I understand ASIC are absolutely creaking under the workload. I believe they got in some AI tech that was supposed to help them triage this stuff. They must be floored with the number of reports that are coming in. So, it’s not giving them useful data either. It was supposed to inform their regulatory and enforcement approach, but it’s not doing that. So, it’s generating heaps of junk and heaps of work, and I don’t think it’s generating much useful intel for the regulator.”

Deputy Chief Risk Officer, Head of Compliance & Regulatory Risk

“Given that it’s new for us, it’s a matter of not wanting to over-report or under-report.”

Head of Compliance

51%

of respondents do not believe that ASIC can administer the new regime effectively.

Do those who need to know, actually know?

The enhanced breach reporting regime is complex, large, and there are civil and criminal penalties for non-compliance if tight timeframes are not met. One of the themes of the research has been the criticality of AFSL and ACL holders in investing in their governance, policies, procedures, and systems to detect, triage, analyse, and report breaches.

Accordingly, it is fascinating that around half (51%) of respondents overall rate their understanding of the new obligations as moderate, low or very low. Concerningly for ACL holders, these overall levels of understanding are broadly reflected among mortgage brokers, where 54% rate their understanding as moderate, low or very low.

Perhaps most surprisingly, the greatest lack of clear understanding of the obligations is most pronounced among financial advisers who are employed in advice practices that do not hold their own AFSL, where almost three quarters (74%) rate their understanding as moderate or lower. That statistic will be of deep concern to AFSL holders who utilise corporate authorised representative arrangements to expand their distribution channels.

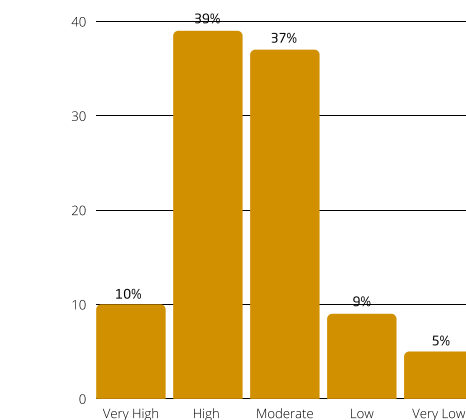
51%

of respondents overall rate their understanding of the new obligations as moderate, low, or very low.

“So, the fundamental issue is the lack of clear information about what is reported. So, it then just takes so much time to make the assessment and then some of it, where there is a [judgement] element, you’ve got to then create more busy work, because you’ve got to write your justification and support it. Maybe get external legal advice and then you know, you kind of go alright - if anyone ever came and looked at this, is it good enough? Is this adequate? But I think that was one of the outcomes they wanted, right? They wanted people to be more worried about this, than they have previously were.”

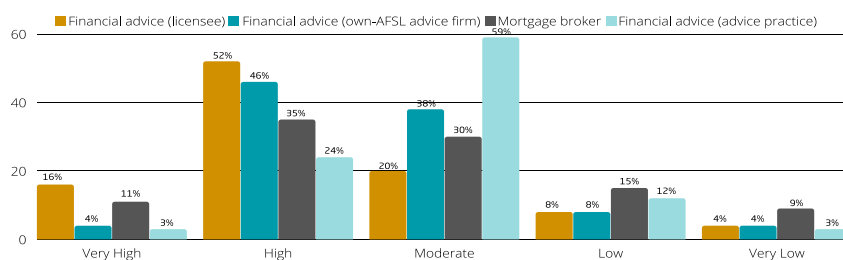
Chief Risk & Governance Officer

How do you rate your level of understanding of the new breach reporting rules?



n = 160, Overall

How do you rate your level of understanding of the new breach reporting rules?



n = 25, Financial advice (licensee); 24, Financial advice (own-AFSL advice firm); 46, Mortgage broking; 34, Financial advice (advice practice)



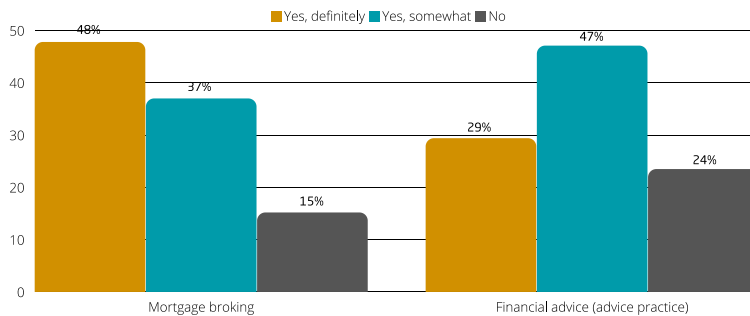
Indeed, for advisers operating under corporate authorised representative arrangements, the results are suggestive that more robust arrangements are required as around a quarter (24%) do not believe they have been adequately trained or informed by their AFS licensee to monitor for breaches. The same proportion do not believe they have been adequately trained on how to report breaches when they occur.

However, encouragingly, most (94%) believe definitely, or somewhat that their licensee can competently handle a breach when it is reported to them, and more than eight in 10 (82%) believe their licensee will support them in resolving the issue, should they report a breach.

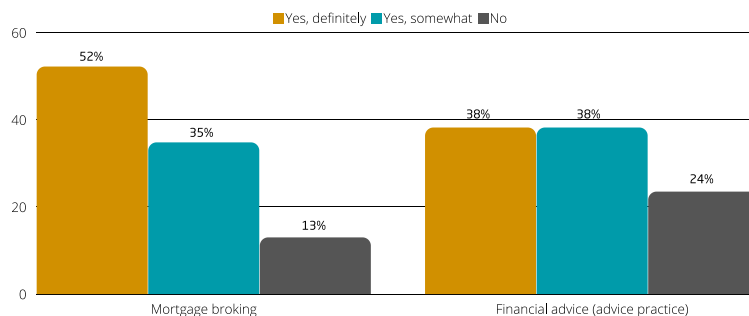
94%

of participants believe their licensee can competently handle a breach when it is reported to them.

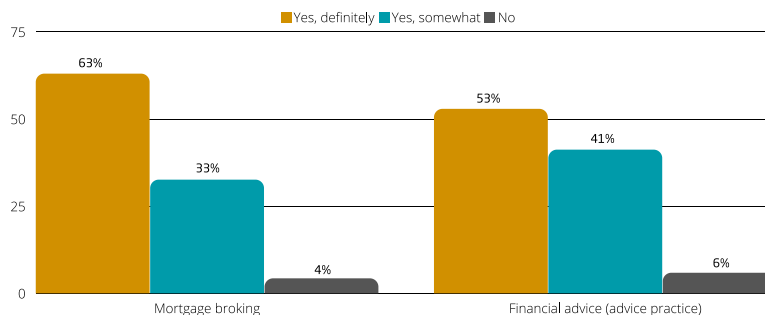
Do you believe you've been adequately trained or informed by your licensee about how to monitor for breaches?*



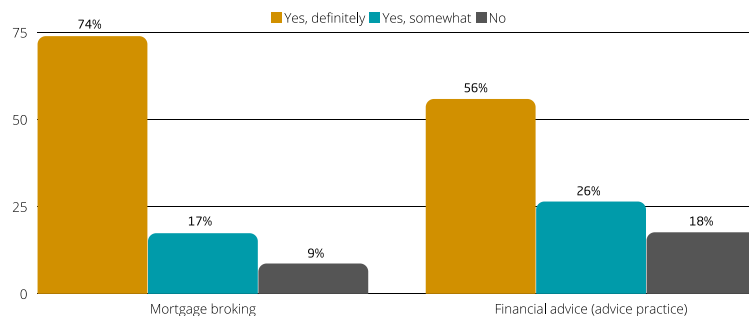
Do you believe you've been adequately trained or informed by your licensee about how to report breaches when they occur?*



Are you confident your licensee can competently handle a breach you report to it?*



Are you confident your licensee will support you in resolving the issue should you report a breach?*



* Asked to mortgage brokers or financial advisers (advice practice)
n = 46, Mortgage broking: 34, Financial advice (advice practice)

Investment in systems, processes & resources

The preparation, implementation and now the administration of the breach reporting obligations has put immense additional pressure on compliance functions. There is a prevailing theme throughout the research that the industry has struggled to find the tools to effectively respond to the increased demands that the enhanced breach reporting regime has placed on them. Still further, that potentially the jury is still out on ACL holders who are experiencing the breach reporting regime for the first time.

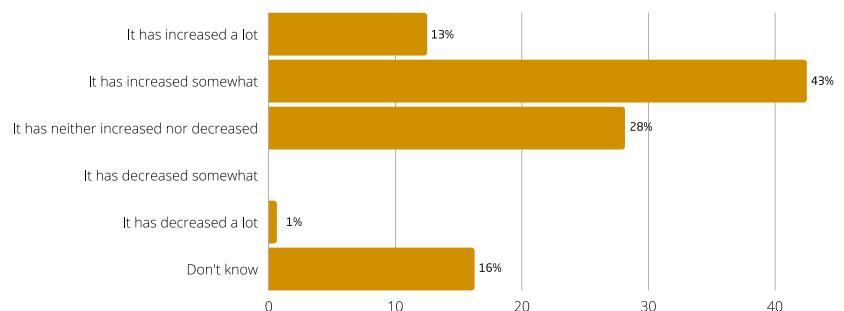
80%

of respondents surveyed invested additional time and money in process optimisation, people, RegTech systems and non-legal advisers and consultants to deal with the increased compliance burden.

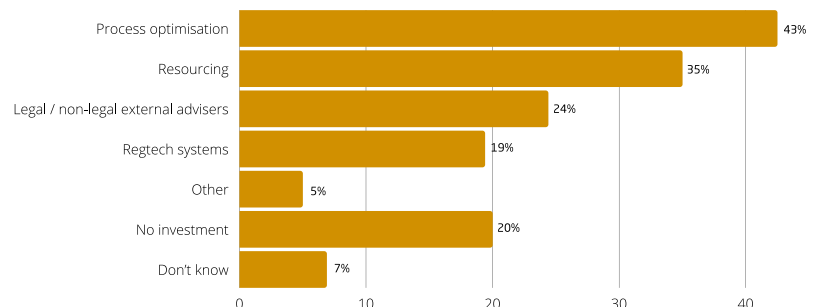
“There is a certain amount of ... typical ASIC: ‘We won’t tell you what compliant looks like, but we know non-compliant when we see it’. I don’t disagree with the premise that AFSL holders should be obligated to report their own breaches. I think that is actually a cornerstone of regulatory enforcement, but it’s not doing any of the things [it was intended for]. I think it’s predicated on the assumption that all financial services licenses have incredible tech that helps them deal with all this stuff. And the reality is, most of them don’t. The market hasn’t got this intel yet, so it’s incredibly heavy lifting for compliance staff, and people make mistakes. They just do. Service delivery, growth and experience teams, contact centre teams, everybody makes mistakes.

Deputy Chief Risk Officer, Head of Compliance & Regulatory Risk

How has the new breach reporting regime affected the amount your organisation spends on compliance?



What systems and processes are you investing in specifically in response to the breach reporting rules?



* Multiple response allowed
n = 160, Overall

Optimism for the future

There are significant challenges with the enhanced breach reporting regime for AFSL and ACL holders. The complexity, number of legislative provisions to consider, resourcing challenges and tools to manage compliance are but a few. Still, there is also hope that compliance will become less onerous as the new provisions are bedded down.

More guidance from the regulator, in the form of published breach reporting statistics and case studies of where incidents have been correctly identified, assessed, and reported (as well as case studies illustrating incidents that do not need to be escalated to a report) are seen as critical in helping improve the efficiency and effectiveness of administering the new obligations.

Whether this is likely to transpire remains to be seen, given that with every case study and guidance note the regulator publishes, there is the risk of unintended consequences, and a limiting of the scope of enforcement as ASIC has many other challenges.

“You have to be careful about comparing yourself, because you will never know the ins and outs of something that’s been reported, and so you have to be careful to form your own view around whether something is reportable or not. But I think where it’s really helpful is that it gives you some insight into what others are doing and how you measure against that, because at the end of the day, the last thing you want to be, is an outlier and to be under-reporting and to be seen to be under-reporting, even if that’s not what you think you might be doing. And that’s constantly our concern. We don’t want to compare ourselves, but also, it kind of is important in a way to do that because otherwise, how do you know how you’re truly going? You might think you’re doing great, and you’re absolutely on track, but the regulator might have a different view on that.”

Head of Compliance & Conduct

“It’s just very difficult to implement in practice, particularly when you’re not resourced. It’s a one-size-fits-all regime, so you’ve got a whole lot of variation in resources and capability across the industry. I really think ASIC could be more helpful. Like in terms of in the Australian economy, how are our mutual resources best spent dealing with this issue? Rather than having everybody in a bank reinventing the wheel and trying to come up with their own approach, really you know, it would make more sense if ASIC provided a little bit more guidance and direction here.”

Chief Risk & Governance Officer

Acknowledgement

About Lawcadia

Lawcadia is a legal technology company headquartered in Brisbane, Australia, with clients including corporate and Government legal and compliance teams and over 160 law firms. A unique multi-sided award-winning platform that utilises intelligent workflow automation and BI reporting, Lawcadia can provide process and technology-driven solutions to solve specific pain points in the legal, regulatory and compliance environment. From legal and breach intake, matter management, outside counsel collaboration and document automation through to assessing financial services breach reporting and post-breach review, Lawcadia has best-practice legal operations and regulatory compliance workflows, as well as the capability to create your own.

Lawcadia is committed to continuous improvement and working actively with our clients to deliver intuitive, easy to use technology that delivers measurably positive results.

- 🔗 lawcadia.com
- ✉️ enquiries@lawcadia.com

About Gadens

Gadens' national Financial Services Regulatory team continues to advise leading banks, insurers, superannuation firms, crypto firms and other financial services clients about regulatory compliance, licensing, and responding to increasing regulatory inquiries. We are at the forefront of the significant developments in this sphere, including advocating for what form changes to the laws should take.

Exceptional technical legal advice is a given. Gadens' Financial Services Regulatory team is different to other firm's practice, with a focus on how we deliver value. Whether in our weekly blog on regulatory updates (<https://regulatorsweeklywrap.blog>), our RegTech solutions for breach reporting, with Lawcadia (see below) or teaching the next generation of lawyers at university courses we have created, demonstrating innovation, delivering practical value and upholding integrity are our signature hallmarks.

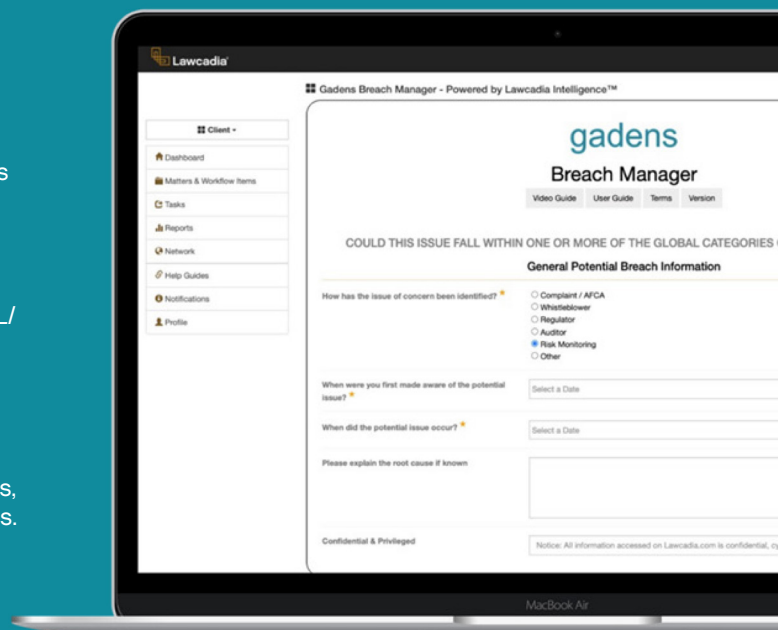
- 🔗 gadens.com/service/banking/regulation-and-compliance
- ✉️ liam.hennessy@gadens.com

Gadens Breach Manager

In April 2021, Gadens launched the Gadens Breach Manager, powered by Lawcadia. This first of its kind, cloud-based RegTech solution streamlined the information collation, assessment, and reporting process of potential regulatory issues to one online platform, allowing financial services institutions across the country to ensure defensible, timely and cost-effective compliance with the new and newly important regimes, including BEAR/FAR, ADI, AFSL and ACL obligations, AML/CTF, Privacy and Design & Distribution.

With over 2000+ civil and criminal penalty provisions worked into the platform, and at a low monthly cost (with no legal fees, unless matters are outsourced), the Gadens Breach Manager is used daily by banks, insurers, superannuation funds and other financial services clients.

- 🔗 breachmanager.gadens.com
- 📺 Watch a video introduction and demonstration





Lawcadia®

gadens

Research Partner

CORE|DATA
research

© Copyright 2022 - Lawcadia and Gadens.