REPORT 594

Review of selected financial services groups' compliance with the breach reporting obligation

September 2018

About this report

This report sets out the findings of our review of Australian financial services (AFS) licensees' compliance with their breach reporting obligation under s912D of the *Corporations Act 2001* (Corporations Act).

The purpose of this review was to consider selected financial services groups (financial groups), covering all their AFS licensees. Depending on the groups' diversity, these licensees provided services such as banking, superannuation, investment management, insurance, and financial advice. The review also examined whether:

- their breach reporting is adequate and effective;
- they comply with the breach reporting obligation; and
- they demonstrate elements of a sound breach-reporting culture.

Based on the findings, the report also provides 'what good looks like' to help AFS licensees improve their compliance measures and ensure they comply with the breach reporting obligation.

About ASIC regulatory documents

In administering legislation ASIC issues the following types of regulatory documents.

Consultation papers: seek feedback from stakeholders on matters ASIC is considering, such as proposed relief or proposed regulatory guidance.

Regulatory guides: give guidance to regulated entities by:

- explaining when and how ASIC will exercise specific powers under legislation (primarily the Corporations Act)
- explaining how ASIC interprets the law
- describing the principles underlying ASIC's approach
- giving practical guidance (e.g. describing the steps of a process such as applying for a licence or giving practical examples of how regulated entities may decide to meet their obligations).

Information sheets: provide concise guidance on a specific process or compliance issue or an overview of detailed guidance.

Reports: describe ASIC compliance or relief activity or the results of a research project.

Disclaimer

This report does not constitute legal advice. We encourage you to seek your own professional advice to find out how the Corporations Act and other applicable laws apply to you, as it is your responsibility to determine your obligations.

Examples in this report are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

Contents

A Executive summary

Role of breach reporting

1 All Australian financial services (AFS) licensees have a legal requirement to report to ASIC a significant breach that has occurred or is likely to occur as soon as practicable, and in any case within 10 business days of becoming aware of the significant breach.

> Note: AFS licensees that are co-regulated with the Australian Prudential Regulation Authority (APRA) may elect to report the breach to ASIC through one report to APRA.

2 Breach reporting is a core component of Australia's financial services regulatory structure, where AFS licensees act as the 'first line' of compliance. We have consistently highlighted the importance of breach reporting as part of an AFS licensee's compliance and risk management systems.

Recommended law reform for breach reporting

3 The Australian Government set up the ASIC Enforcement Review in 2016, which delivered recommendations for law reform, including for the breach reporting obligation in December 2017. The breach reporting recommendations included:

(a) implementation of a more objective test for significance;

(b) a requirement for AFS licensees to report to ASIC when they form a suspicion that a significant breach has occurred or is likely to occur, to encourage more timely reporting;

(c) a 30-day reporting requirement, triggered by the start of an AFS licensee's investigation;

(d) public reporting of breach reporting figures;

(e) the extension of the breach reporting obligation to Australian credit licensees;

(f) an increase to criminal penalties for failure to report as and when required; and

(g) the introduction of a civil penalty and an infringement notice provision in addition to the criminal offence.

4 The Australian Government has provided in-principle support for these proposed changes to the breach reporting obligation.

5 We support the proposed changes and their purpose of creating stronger and clearer rules for reporting breaches to ASIC.

6 Options for enforcement of breach reporting should not be limited to criminal sanctions. The current penalty provided for the offence of failing to

meet the breach reporting obligation—a maximum of 250 penalty units ($52,000) for a body corporate—is too low to have a deterrent effect.

7 We require a broad, effective range of enforcement remedies to enable ASIC to respond to the full range of types and severity of misconduct, from less grave to more serious breaches. There are significant variations in the seriousness of breach reporting failures.

8 For a contravention of the breach reporting obligation that does not involve a deliberate failure to report, we should be able to issue an infringement notice or apply for a civil penalty, set at a level that adequately deters an AFS licensee from contravening the provision.

9 Stronger criminal penalties should be readily enforceable for serious misconduct, such as deliberate delays or failure to report.

10 The ASIC Enforcement Review followed concerns we raised publicly that AFS licensees were not reporting in a timely and consistent manner. Delays in reporting were often caused by failures in compliance systems or subjective interpretations of the breach reporting obligation.

11 Further delays were caused by those responsible for determining whether a breach is significant not considering the matter until after a lengthy investigation. The subjectivity and ambiguities in the current legal requirements have limited the circumstances in which we can take enforcement action.

12 The findings of this review have confirmed and quantified our concerns that breach reporting is not timely or consistent and that the current rules are subjective and ambiguous. The findings underline the urgent need for the proposed reforms.

Breach reporting review

13 Between 2017 and 2018, we conducted a review into the current operation of breach reporting, using funding allocated in the 2016–17 federal budget to improve outcomes in financial services.

> Note: See *Budget 2016–17: Budget measures—Budget paper no. 2*, under the heading 'Australian Securities and Investments Commission—Improving outcomes in financial services'.

14 We selected the following 12 authorised deposit-taking institutions (ADI) and their associated AFS licensees for review (reviewed financial groups). Table 1 sets out all the reviewed financial groups, by major financial groups (four) and other financial groups (eight).

Table 1: The reviewed financial groups

Major financial groups	Other financial groups
Australia and New Zealand Banking Group (ANZ)	AMP Limited (AMP)
Commonwealth Bank of Australia (CBA)	Bank of Queensland
National Australia Bank Group (NAB)	Bendigo and Adelaide Bank
Westpac Banking Corporation (Westpac)	Credit Union Australia
	Greater Bank
	Heritage Bank
	Macquarie Group (Macquarie)
	Suncorp Group (Suncorp)

Note: The reviewed financial groups are financial services groups included in this report with an Australian ADI as one of its AFS licensees. The reviewed financial groups include nine banks, one credit union and two mutual banks.

15 Our review was a proactive surveillance of the current breach reporting practices of the reviewed financial groups and the extent to which elements of a firm's culture, systems and management supports its ability to meet its breach reporting obligation.

16 The purpose of the review was to consider whether the reviewed financial groups:

(a) had adequate and effective breach reporting processes;

(b) complied with the breach reporting obligation; and

(c) demonstrated elements of a sound breach management culture—for example, an environment:

(i) where incidents can be detected, raised and escalated quickly;

(ii) that prioritises the investigation of possible breaches;

(iii) where, once a significant breach has been confirmed, there are transparent communications internally and with ASIC; and

(iv) that ensures fair outcomes for consumers affected by a breach.

17 We structured our review around the key stages of the 'significant breach lifecycle'—from identifying potential issues, to reporting significant breaches to ASIC and rectifying the breach (including by way of remediating consumers). We explored possible reasons for delays within the breach reporting process.

18 The review covers a total of 715 significant breaches reported to ASIC by AFS licensees within the reviewed financial groups between 2014 and 2017.

19 We collected data on each significant breach from the reviewed financial groups' AFS licensees that had one or more significant breaches reported under s912D of the *Corporations Act 2001* (Corporations Act) between 2014

and 2017. Our findings are based on policies, case studies and other documents we reviewed, in conjunction with the collected data.

Note: 83 AFS licensees of the reviewed financial groups reported one or more significant breaches in this period.

Key stages of a significant breach

20 As part of the review, we collected dates to calculate the length of time taken for each 'key stage' of each significant breach reported to ASIC by the reviewed financial groups for the period between 2014 and 2017.

21 We have used data to calculate the average (referred to as 'mean' in figures) and median for all reviewed financial groups. We have isolated key stages to assesses potential bottlenecks, recurring themes and opportunities for improvement for reviewed financial groups.

22 Table 2 sets out the key stages of a significant breach. Key stages 1–3 (reporting stages) are common to each breach, while key stages 4–7 (rectification stages) may not be applicable to each breach.

Table 2: Key stages of a significant breach

Process	Stages	Report section
Breach reporting process	1 Identification of incident 2 Identification to investigation 3 Investigation to breach report	Section C
Breach rectification process	4 Communication with consumers 5 Payments to consumers 6 Process and/or system change 7 Accountability	Section D

23 Our findings and observations on a sound breach management culture are discussed throughout the key stages and are drawn together in Section E.

ASIC's key findings

24 Based on analysis of the data, selected documents, statements and case studies, we made the key findings set out in Table 3.

Note: In this report, we refer to calendar days unless we explicitly state 'business days'.

Table 3: Key findings of the breach reporting review

Finding	Why is this important?	What we found
1 **Delayed identification of incidents**	Delays in identifying incidents that, once investigated, are determined to be significant breaches increase the risk of consumer detriment and the likelihood that a breach becomes significant.	The time taken to identify incidents that are later determined to be significant breaches is the main reason why ASIC receives breach reports about long dated events or conduct. The major financial groups took an average of 1,726 days (median: 1,148 days) to identify an incident that was later determined to be a significant breach. The other financial groups took an average of 995 days (median: 600 days).
2 **Lengthy investigations leading to delayed reporting**	Delays in breach reporting caused by lengthy investigations undermine our ability to take timely and appropriate enforcement or other regulatory action, and further increase the risk of consumer detriment.	We received a quarter of breach reports after AFS licensees had spent 168 days or more investigating the breach. The major financial groups took an average of 150 days (median: 95 days) from starting an investigation to lodging a breach report. The major financial groups' average was double that of the other financial groups, which took an average of 73 days (median: 34 days).
3 **Failure to report to ASIC within 10 business days**	AFS licensees are legally required to notify ASIC within 10 business days of becoming aware of a significant breach.	Approximately one in seven significant breaches (110) were reported to ASIC more than 10 business days after the AFS licensee became aware of the breach. This was a systemic issue for one major financial group, NAB, accounting for 84 (approximately 76%) of these delayed breach reports.
4 **Delayed remediation for consumer loss**	AFS licensees must ensure that the financial services covered by their licence are provided efficiently, honestly and fairly: see s912A(1)(a). This requires fair and timely outcomes for consumers affected by significant breaches. The ability to remediate depends on AFS licensees identifying and investigating significant breaches on a timely basis. The remediation process should align with stated values, such as prioritising consumers and 'putting things right'.	For significant breaches that involved consumer financial loss, CBA, NAB and ANZ took an average of 352 days (median: 316 days), 265 days (median: 234 days), and 198 days (median: 140 days) respectively to make the first payment to consumers after ending their investigations. We identified historical documents from two of these major financial groups that referred to remediation for consumers as a 'distraction'. This is evidence of a misalignment in these two groups' cultures with their stated values of prioritising consumers. The fourth major financial group, Westpac, took substantially less time—an average of 69 days (median: 112 days)—which was more consistent with the other financial groups reviewed (average: 84 days; median: 111 days). For significant breaches that involved consumer financial loss, the reviewed financial groups took an average of 2,145 days (median: 1,525 days) from the first instance of the breach to make the first payment to affected consumers. Overall, consumers were out of pocket for an excessive period.

Finding	Why is this important?	What we found
5 Lack of effective and searchable incident and compliance systems	AFS licensees' provision of adequate resources for effective systems to record and investigate incidents are fundamental to a sound breach management culture. Accurate, complete, current, and timely recording of information is necessary to allow licensees to identify risks, investigate incidents, report to ASIC, and maintain oversight of the process.	Some AFS licensees' current systems had limited search functionality. This, in combination with a fragmented approach to recording information over many databases, inhibited the identification and investigation of a number of significant breaches. It also limited licensees' capacity to understand their overall management of breaches. This, in turn, limits the AFS licensees' broader lessons learned opportunities: see key finding 7 at paragraphs 410–451. Key information that we would expect to see in a breach report often could not be located by the AFS licensee on their system. The information was not always recorded in a searchable format and often resulted in a resource-intensive manual process to conduct investigations, reviews, audits and respond to our inquiries. In some cases, key information was not recorded at all and required licensees to re-interview relevant staff, if they were still employed.
6 Inconsistent reporting of significant breaches	AFS licensees are only required to report significant breaches. AFS licensees' interpretation of 'significance' is subjective, and therefore inconsistent. Inconsistent reporting leads to varying levels, and limitations on, a key source of intelligence and information for ASIC. It can also affect the opportunity for ASIC intervention or oversight.	The subjective nature of the tests of significance in s912D(1)(b) contributes to delays and inconsistencies in reporting significant breaches to ASIC. The reviewed financial groups assess significance from their own perspective in the absence of an objective test. A comparison of two major financial groups' data, NAB and Westpac, regarding significant breaches with consumer financial loss suggests that an inconsistent application by industry of what is 'significant' affects the number of reports made to ASIC. In the review period, NAB had the lowest median consumer financial loss per significant breach ($206,538.00 versus $1,407,010.84) and reported 6 times more breaches with consumer financial loss (121 versus 19) than Westpac, which had the highest median consumer financial loss per significant breach.
7 Underutilised lessons learned opportunities	The investigation and rectification of a significant breach presents a potential lessons learned opportunity for the AFS licensee, and possibly for other licensees within the financial group. It also provides an opportunity to remove or reduce weaknesses more broadly, to prevent other incidents from occurring.	Some AFS licensees have not always made the most of lessons learned opportunities. Licensees were too often reactive, limiting their focus to the immediate breach, and neglecting the lessons learned opportunity for the licensee (or broader group). In some instances, licensees narrowed, or attempted to narrow, the scope of investigations (and remediations). This appeared to be driven by an intent to make the process manageable. However, at times this was at the expense of more thorough investigations, and increased the possibility, if not likelihood, that such issues (or similar issues) affected a broader pool of consumers. Helpfully, however, licensees did undertake timely process or system changes in direct response to the specific significant breach.

Finding	Why is this important?	What we found
8 Elements of a sound breach management culture not demonstrated	A sound breach management culture will prioritise and support the ability of an AFS licensee to meet its breach reporting obligation. It provides a transparent and open environment that promotes breach identification, rectification, and reporting—where staff can raise and escalate incidents, investigations are prioritised and overseen by senior management, and where rectification and remediation are also prioritised.	In general, we observed that aspects of the reviewed financial groups' culture did not support the ability of AFS licensees to meet their breach reporting obligation. In many instances, the reviewed financial groups did not demonstrate elements of a sound breach management culture. Some of the reviewed financial groups did not give adequate priority to: • how breaches are detected, escalated and managed within the organisation, with a significant minority of staff being uncomfortable raising concerns or risks; and • how quickly consumers are remediated following a breach, which does not align with statements made by many of the reviewed financial groups, both publicly (e.g. values) and in internal documents (e.g. policies and procedures). In some cases, we also observed a limited and inconsistent level of oversight by and accountability of senior management across the key stages of a significant breach.

Note: Findings 1,2 and 4 display both an average and a median. An average with value higher than the median implies a distribution skewed to the right (e.g. more results above the median), with values having a greater effect on the average calculations. For further details and an explanation on the use and application of statistical information contained in this report, see Appendix 1 at paragraphs 528–534.

25 These findings do not affect all the reviewed financial groups to the same extent; in general, the major financial groups took longer to identify, investigate, report and remediate significant breaches.

26 All AFS licensees, not just those who participated, should benefit from robust benchmarking of their performance and resources, to assess the effectiveness of their own breach reporting processes and make improvements where weaknesses are identified. We are seeking to influence the entire financial industry with our findings and better equip AFS licensees to monitor their own performance, internally, as well as against their peers.

27 Based on our findings, we have stated our expectations for industry and identified opportunities for improvement to strengthen the effectiveness of breach reporting processes: see Table 4. These should be considered as additional guidance to supplement Regulatory Guide 78 *Breach reporting by AFS licensees* (RG 78).

28 We have also set out actions we will take to improve breach reporting in Australia: see Table 5.

ASIC's expectations

29 Table 4 sets out our expectations for AFS licensees regarding the breach reporting obligation, informed by our findings in this report.

Table 4: ASIC's expectations for AFS licensees

Expectation	Description
1 Compliance with breach reporting obligation, including reporting to ASIC within 10 business days	All AFS licensees are legally required to have a process that effectively identifies breaches and then reports significant breaches to ASIC. The failure to report significant breaches to ASIC within 10 business days of becoming aware of them is a criminal offence. The identified instances of non-compliance with the 10 business days reporting requirement are unacceptable, especially when the legal requirement is to report 'as soon as practicable' but no later than 10 business days from awareness.
2 Greater capacity and speed in identifying and investigating incidents, and reporting significant breaches to ASIC	AFS licensees must look for opportunities to improve the operation of their breach reporting processes by: • investing in business and compliance systems that more readily allow AFS licensees to identify and investigate incidents that may be breaches; • maintaining systems that capture accurate, complete, and current information of the type required in a breach report (and breach register) and that are searchable, updatable and extractable; • ensuring investigations of incidents are resourced and conducted quickly, and their findings are accurate and escalated in a timely manner; • engaging with ASIC at the earliest possible opportunity when it is apparent that there is a significant breach—in particular, during lengthy investigations where further work is needed to determine *how* significant a breach is rather than whether it *is* significant (e.g. where investigations may still have a substantial amount of work to uncover the full extent of the breach); • reviewing and monitoring current interpretations of significance to avoid overly legalistic and inconsistent approaches to breach reporting. The breach's impact on consumers—such as the individual and total financial losses and how long they have been out of pocket—is an important consideration. The significance of a matter should not be unduly diluted by consideration of other factors, such the overall percentage of consumers affected; • better monitoring by senior management and benchmarking the operation and effectiveness of their current breach reporting practices; and • better management of delays in reporting significant breaches to ASIC, by increased senior management oversight and board reporting.

Expectation	Description
3 Demonstrate a sound breach management culture that makes breach reporting a priority	All AFS licensees should create and maintain a workplace where management of breaches, and timely breach reporting, is a priority. This means maintaining a workplace culture where: • staff are encouraged to be vigilant, raise and escalate incidents, and feel comfortable when doing so; and • escalation of incidents and management of breaches is a priority and is supported by senior managers and executive leaders. We expect senior management of licensees to consider and understand whether: • breaches, and incidents more broadly, are detected quickly; • robust compliance measures (systems and processes) are in place; and • the investigation of breaches is prioritised. We expect these issues to be assessed on an ongoing basis. We have included detailed 'Questions to ask' for each of these in Section E.
4 Demonstrate a sound breach management culture that makes consumer remediation a priority	All AFS licensees should create and maintain a workplace and culture where ensuring fair consumer outcomes following a breach is a priority—for example, where financial loss is involved, ensuring that consumers are remediated swiftly. Licensees must provide adequate resources for the processes for remediation of consumers affected by the breach, as well as process, system and policy changes without undue delay. We expect that these different processes will occur concurrently wherever possible to ensure that consumers are remediated as soon as possible. AFS licensees should aim to deliver comprehensive remediation to all affected consumers, to restore them to the position they would have held but for the significant breach. If licensees are not able to remediate all affected consumers, we expect that licensees will have in place processes to ensure that they do not profit from their mistakes.
5 Make the most of the lessons learned opportunities that each breach presents	AFS licensees should: • proactively and transparently share the findings of investigations to allow identification of similar issues within the licensee and the broader group (where relevant), and prevent similar issues from occurring in the future; and • consider the breach in the broader context of their breach reporting process, including the timeliness and effectiveness of their reporting to ASIC and rectification.

ASIC's actions

30 Table 5 sets out the actions we will take to improve breach reporting. See Section F for further details.

Table 5: ASIC's actions regarding breach reporting

Action	Description
1 **Close and continuous monitoring program**	Senior ASIC staff will commence an on-site monitoring role at the major financial groups and AMP from October 2018. ASIC will have dedicated on-site supervisory staff spending extended periods within these institutions to monitor their governance and compliance with laws, including how they are improving breach identification, reporting and rectification programs.
2 **Monitor the operation of breach reporting, including consumer outcomes**	We will continue to monitor the effectiveness of AFS licensees' breach reporting processes. We will also continue to require and monitor the remediation of consumers financially affected by significant breaches and intervene to ensure fair outcomes for consumers, where necessary.
3 **Develop the ASIC Regulatory Portal to lodge breach reports electronically**	We are developing the capacity for AFS licensees to lodge breach reports to ASIC through the ASIC Regulatory Portal. This will assist with proposed annual publishing of breach report data. It will also allow possible industry benchmarks relating to AFS licensees' breach reporting obligation.
4 **Enforcement**	ASIC is actively considering enforcement action for failures to report breaches on time, noting the problems in the existing law. These problems include that there are only currently criminal sanctions, ambiguity as to when the time allowed for reporting commences and the subjectivity of the 'significance' test. Failures to report can only be prosecuted on a criminal basis, with the associated high standard of proof. At the same time, the existing penalty is modest. A contravention of s912D has a maximum penalty of 250 penalty units ($52,500) for a body corporate.
5 **Support law reform**	We will continue to support the law reform recommended by the ASIC Enforcement Review, and which the Australian Government has accepted in-principle, to create stronger and clearer rules for reporting breaches to ASIC. For example, only around a quarter of breach reports are lodged within 30 days after the start of an AFS licensee's investigation. If this law reform was adopted, all breach reports (or suspected breach reports) would need to be lodged with ASIC within this timeframe. This will improve our ability to take appropriate enforcement action.
6 **Guidance and stakeholder engagement as part of law reform**	If the breach reporting obligation is extended to Australian credit licensees (e.g. mortgage brokers and providers of credit or consumer leases), and other proposed changes are enacted, we will produce updated regulatory guidance to help all licensees comply with any new requirements.

Excluded from scope

31 In this review, we did not re-assess or re-investigate the underlying breach by an AFS licensee. Nor did we include in the scope of our review whether the decision not to lodge a breach report with ASIC was appropriate, other than to highlight the inconsistency of the application of 'significance' in practice. We have previously considered each significant breach included in this review and determined the appropriate response—that is, ongoing surveillance, monitoring or enforcement action. We publish detailed statistics on significant breach reports received and our regulatory response in our annual report.

32 We did not include the following notifications to ASIC in the review:

(a) breach reports from auditors under s311, 601HG or 990K of the Corporations Act;

(b) suspicious activity reports from market participants under the relevant market integrity rules; and

(c) other types of notifications (e.g. those from responsible entities and credit licensees).

B Background to the review

Key points

Breach reporting is an important component of Australia's financial services regulatory structure, where AFS licensees act as the 'first line' of compliance. The regulatory structure acknowledges that, despite an expectation of compliance, breaches will occur.

If a significant breach by an AFS licensee has occurred, it is required to report the significant breach to ASIC within 10 business days of becoming aware of it.

We have for some time held concerns that AFS licensees are either not reporting breaches to ASIC or not reporting breaches in a timely and consistent manner, and have advocated for law reform to make the obligation clearer and more readily enforceable.

We continue to take a range of regulatory action against those AFS licensees that have not complied with their breach reporting obligation.

Role of breach reporting

Compliance measures

33 Breach reporting is an important component of Australia's financial services regulatory structure, where AFS licensees act as the 'first line' of compliance. The regulatory structure acknowledges that, despite an expectation of compliance, significant breaches will occur and AFS licensees then have an obligation to report these to ASIC. Timely breach reporting allows ASIC to identify emerging harms in the market and take the appropriate regulatory response.

34 AFS licensees are required to have adequate compliance measures in place as part of obtaining and maintaining their licence. Regulatory Guide 3 *AFS Licensing Kit: Part 3—Preparing your additional proofs* (RG 3) provides specific guidance on the full scope of such necessary compliance measures (see RG 3.19), of which breach reporting is a key element.

35 Further, Regulatory Guide 104 *Licensing: Meeting the general obligations* (RG 104) provides guidance on how we assess compliance with the general AFS licence obligations in s912A(1): see RG 104.21 and Table 2 of RG 104 for a list of questions to consider when designing and testing your compliance measures to ensure you comply with the general obligations.

36 All licensees are expected to have in place structures, systems and policies designed to ensure compliance with the breach reporting obligation in the

Corporations Act. The effectiveness of the compliance measures put in place to meet the breach reporting obligation, and the AFS licensee's culture, will affect its ability to:

(a) identify and escalate issues to be investigated;

(b) conduct timely investigations;

(c) undertake an accurate and honest assessment of whether the issue is a breach and whether it is significant;

(d) notify ASIC in a timely, accurate and honest report; and

(e) be fair, transparent and timely in communication with consumers who have been affected by the breach.

37 Breaches are real-life stress tests of an AFS licensee's compliance measures. How an AFS licensee responds is not only a reflection of the effectiveness of their compliance measures but also of their culture. An AFS licensee's response extends to how they fix the issue, resolve any impact on consumers (i.e. restore consumers to the position they would have held but for the breach), and implement steps to prevent recurrence.

> Note: This report focuses on breach reports made under s912D of the Corporations Act; however, there are other compulsory reports that can be more broadly categorised as 'breach reporting'.

38 Breach reporting should be a vital source of learning for AFS licensees to both reinforce and improve that 'first line' of compliance. Each breach, whether significant or not, highlights a weakness that must be understood, so that improvements can be made to prevent the recurrence of the breach in the future. Internal reporting on the root causes and the effects of the breach, as well as the current and intended responses, need to be escalated to senior management or higher.

39 AFS licensees each have a clear role in lifting industry standards as a whole, and part of this is timely identification of their own problems within the financial services industry. AFS licensees' ability to quickly identify emerging conduct and systemic issues relies heavily on their business and compliance systems, as well as their staff and senior management. Timely identification facilitates more efficient reporting of breaches to ASIC and allows AFS licensees to rectify breaches more swiftly.

40 Further, AFS licensees may have an opportunity to remediate consumers affected by a breach in a way that can restore some of the trust and reputational damage caused by the breach. These problems tend to cause consumers financial detriment and prolonged inconvenience. It is important to understand that AFS licensees' responsibility extends beyond industry standards to fulfilling consumer expectations.

> Note: In this report, we use the term 'systems' to mean information technology (IT) systems.

Key information for ASIC

41 Breach reports lodged by AFS licensees are also a key information source for ASIC. We consider all reports we receive. Effective and timely breach reporting enables ASIC to:

(a) identify misconduct and compliance issues within AFS licensees;

(b) take steps to remedy the effects of misconduct and to protect investors from further misconduct;

(c) take regulatory and law enforcement action where warranted (disrupting harmful behaviour);

(d) understand emerging and changing trends and harms within the financial services industry; and

(e) respond to trends and harms by:

(i) educating investors; and

(ii) providing guidance to AFS licensees.

42 Beyond compliance with the breach reporting obligation, we expect that AFS licensees will have a transparent, open and cooperative relationship with us.

43 Recent admissions at the Royal Commission into misconduct in the banking, superannuation and financial services industry (Royal Commission) that AFS licensees' conduct relating to breach reports, namely that they contained misleading information to ASIC or failing to lodge timely breach reports, had fallen below community standards and expectations, undermines trust between ASIC and the industry and consumers' trust in the industry.

44 Without trust, breach reporting is less effective. We would have to investigate and corroborate all the information in a breach report every time one was made. We would also have to devote substantial resources to investigate failures to lodge breach reports.

45 With trust, after receiving a report, we can focus on the appropriate action for the AFS licensee to take—such as remediating any consumers, rectifying systems and processes, and taking any appropriate regulatory action for the breach.

Regulatory framework for breach reporting

46 Section 912D(1B) of the Corporations Act requires an AFS licensee to notify ASIC of a significant breach or likely significant breach of their obligations under s912A (including their licence conditions), s912B (compensation arrangements), or financial services laws. Under this section, the AFS licensee must make the report in writing as soon as practicable, and in any

event within 10 business days of becoming aware of the breach or likely breach.

> Note 1: Before 2003, s912D required an AFS licensee to report all breaches of s912A and s912B as soon as practicable, and in any case within three days of becoming aware of the breach. This requirement proved too burdensome for both industry and ASIC, with the majority of matters reported being technical or minor.
>
> Note 2: Our guidance on s912D(1B) is contained in RG 78.

47 A 'likely breach', as defined in s912D(1A), requires AFS licensees to report breaches that have yet to occur. We interpret this as the licensee becoming aware that they will be unable to prevent the breach from occurring and, at the time of reporting to ASIC, this is still the case: see RG 78.9–RG 78.10. If the AFS licensee is able to prevent the breach within the 10-business day reporting timeframe, then no likely breach is reportable. Also, if the breach occurs before the report to ASIC, then the breach report should reflect this (i.e. reported as an actual, not likely, breach).

48 Section 912D(1)(b) sets out the factors that determine whether a breach, or likely breach, is 'significant' (significance test). These are:

(a) the number or frequency of similar previous breaches;

(b) the impact of the breach or likely breach on the AFS licensee's ability to provide the financial services covered by the licence;

(c) the extent to which the breach or likely breach indicates that the AFS licensee's arrangements to ensure compliance with those obligations is inadequate; and

(d) the actual or potential loss to clients or the AFS licensee itself.

> Note: RG 78 provides guidance on consideration of the factors set out in s912D—see Table 2 of RG 78.

49 The maximum penalty for an AFS licensee failing to notify ASIC of a significant or likely breach within 10 business days of becoming aware of the breach or likely breach is currently:

(a) for an individual, $10,500 (50 penalty units), imprisonment for one year, or both; and

(b) for a body corporate, $52,500 (250 penalty units).

> Note: The value of the Commonwealth penalty unit increased from $180 to $210 on 1 July 2017.

50 The only 'bright line' requirement of the section is the 10-business day reporting requirement. If an AFS licensee intentionally delays reporting after becoming aware of a significant breach or likely breach for their own interests, or if there is a pattern of repeated delays, then stronger regulatory action is more appropriate.

Issues in the current regulatory framework

51 Ambiguity around the concept of 'significance', and the legislation being silent on the timeliness of *investigation* before 'becoming aware', is largely responsible for the current perceptions that the breach reporting regime is inadequate.

52 In early 2015, we obtained advice from senior counsel about what would be required to prove a contravention of the breach reporting obligation. We provided details of that advice in a public statement to Royal Commission.

> Note: See *Witness statement of Peter Kell*, Exhibit 2.1, prepared for the Royal Commission, 16 April 2018.

53 Senior counsel advised us of the impediments to prosecuting an AFS licensee for failing to comply with the breach reporting obligation:

(a) The significance test is subjective. It involves matters of judgement, and so gives the AFS licensee a very wide discretion when assessing significance. Prosecution for contravention of the section would be highly problematic except in extremely clear factual scenarios.

(b) Section 912D(1B) requires the AFS licensee to be aware that a breach is significant—that is, the requirement is not triggered by the AFS licensee becoming aware that a breach *may be* significant, is *probably* significant, or is *suspected to be* significant.

(c) To establish a contravention of the section, it would not be sufficient for ASIC to establish that, at a certain point in time, the AFS licensee was aware of the facts and circumstances that created the breach and, in turn, the facts and circumstances that created the significance of the breach. Rather, we would need to establish that the AFS licensee was aware that there was a breach and, in turn, that the breach was significant.

(d) The time limit set out in s912D(1B) does not commence until the responsible officer becomes aware of the breach and that the breach was significant.

> Note: In this report responsible officers are also referred to as 'key decision makers'.

ASIC's concerns about current breach reporting practices

54 For some time we have raised concerns about AFS licensees' approach to compliance with the breach reporting obligation.

> Note: See *Why breach reporting is important*, speech by ASIC Deputy Chairman, Peter Kell, Risk Management Association Australia Chief Risk Officers Forum, 16 September 2014.

55 These concerns include that AFS licensees:

(a) are not reporting breaches to ASIC in a consistent timely manner;

(b) may extend the timeframe for internal investigation and reporting processes to delay informing ASIC of significant breaches;

(c) interpret 'significance' differently, leading to an inconsistent approach to breach reporting and level of breach reporting; and

(d) provide ASIC with breach reports that often do not contain enough information to assess and act on the report.

56 In some cases, there is less than constructive engagement with ASIC, particularly at levels of senior management below the most senior in large AFS licensees. As ASIC's then-Chairman, Greg Medcraft, observed in August 2017:

> I'm afraid that we routinely encounter a culture of seeking to delay and frustrate our surveillance, investigation and enforcement work.
>
> Note: See *Opening statement*, statement by then ASIC Chairman, Greg Medcraft, Parliamentary Joint Committee on Corporations and Financial Services (PJC), Canberra, 11 August 2017.

57 Often this lack of constructive engagement is around procedural matters. For instance, we routinely experience delays in AFS licensees responding to notices to compel the production of documents, including ASIC inquiries following the receipt of a breach report. This indicates to us that the licensee has failed to give the matter appropriate priority and resourcing.

58 We have flagged our concerns with industry in different forums—for example, presentations, industry association meetings and one-on-one meetings with AFS licensees—and with the Australian Government in hearings for PJC and Senate Estimates and various inquiries over the last decade. In particular, see most recently the *ASIC Enforcement Review taskforce report*, December 2017.

Enforcement action for non-compliance

59 The ambiguity and subjectivity of the existing law has limited circumstances in which we can take enforcement action for non-compliance with the breach reporting obligation in s912D(1B). To date, we have only once successfully pursued enforcement action for non-compliance with s912D(1B): see our action against Top Quartile Management Ltd for failing to report to ASIC breaches of their legal obligation—*ASIC Annual Report 2006–07*, p. 23.

60 Despite the difficulties of establishing the elements of the offence (see paragraph 53) where appropriate we will continue to look to enforce the current requirements. However, law reform is required to increase ASIC's ability to

take regulatory action. The ASIC Enforcement Review has recommended, and the Government has accepted in-principle, reform to introduce stronger and clearer rules for breach reporting: see paragraphs 63–67.

61 Compliance with breach reporting is not a standalone obligation. Breach reporting forms part of the general licensing obligations under s912A(1), which requires AFS licensees to, among other things, comply with financial services laws.

62 To date, we have focused on enforcing the regulatory requirements of breach reporting, in conjunction with the broader requirements, through:

(a) administrative action against AFS licensees for, in part, failing to comply with their breach reporting obligation—for example, see Media Release (16-045MR) *ASIC suspends AFS licence for failing to lodge financial statements* (24 February 2016);

(b) the required remediation set out in court enforceable undertakings—for example, see Media Release (13-240MR) *ASIC accepts enforceable undertaking from Wealthsure Pty Ltd, Wealthsure Financial Services Pty Ltd and their former CEO* (2 September 2013); and

(c) voluntary reviews and improvements to systems resulting from surveillances or projects—for example, see Report 528 *Responsible entities' compliance with obligations: Findings from 2016 proactive surveillance program* (REP 528) at paragraph 40.

Recommended law reform for the breach reporting obligation

63 The Australian Government set up the ASIC Enforcement Review in 2016, which consulted on possible changes to the breach reporting obligation to create stronger and clearer rules when reporting breaches to ASIC. After a preliminary analysis, the ASIC Enforcement Review released *Position and Consultation Paper 1: Self-reporting of contraventions by financial services and credit licensees* on 12 April 2017.

64 In December 2017, the ASIC Enforcement Review reported to the Australian Government and made the following recommendations for the breach reporting regime:

(a) the 'significance test' should be retained but clarified to ensure that the significance of breaches is determined objectively (Recommendation 1);

(b) the Government should introduce a self-reporting regime for credit licensees equivalent to the regime for AFS licensees (Recommendation 2);

(c) the obligation for AFS licensees to report should expressly apply to misconduct by an employee or representative (Recommendation 3);

(d) significant breaches (and suspected breach investigations that are ongoing) must be reported within 30 days (Recommendation 4);

(e) ASIC should prescribe the required content of breach reports and they should be lodged electronically (Recommendation 5);

(f) criminal penalties should be increased for failure to report as and when required (Recommendation 6);

(g) a civil penalty should be introduced in addition to the criminal offence for failure to report as and when required (Recommendation 7);

(h) the reporting requirements should encourage a cooperative approach where AFS licensees report breaches, suspected or potential breaches, or employee or representative misconduct at the earliest opportunity (Recommendation 8);

(i) the reporting requirements for responsible entities of managed investment schemes should be streamlined, by replacing the requirements in s601FC(1)(l) with an expanded obligation in s912D (Recommendation 9); and

(j) ASIC must annually publish breach report data for AFS licensees (Recommendation 10).

Note: See *ASIC Enforcement Review taskforce report*, December 2017.

65 In April 2018, the Australian Government's response to the *ASIC Enforcement Review taskforce report* was to agree in principle with these recommendations. However, the Government noted that the Royal Commission would consider internal systems of financial entities to identify misconduct.

66 The Australian Government deferred implementation of these recommendations to enable it to take into account any findings arising out of the Royal Commission.

67 ASIC supports changes to breach reporting obligation for stronger and clearer rules about the obligation of AFS licensees to report breaches.

C Breach reporting process

Key points

This section sets out the key stages of the breach reporting process and identifies opportunities for improvement:

- key stage 1–-identification of incident;
- key stage 2—identification to investigation; and
- key stage 3—investigation to breach report.

Delays in the breach reporting process are a serious and ongoing problem. Primarily, delays are caused by AFS licensees taking an average of 1,517 days (median: 925 days) to identify a possible breach (key stage 1). But we are also concerned that reporting significant breaches to ASIC are further delayed due to lengthy investigations—the reviewed financial groups took an average of 128 days (median: 69 days) from commencing their investigations to lodging a breach report with ASIC (key stage 3).

Delays in breach reporting increase the risk of consumer loss or detriment. Delays also undermine our capacity to take timely and appropriate enforcement or other regulatory action, as well as reducing our confidence in the ability of AFS licensees to resolve breaches and implement effective measures to prevent recurrence.

Reporting stages

68 Table 6 sets out the key stages of the reporting process and where we have discussed them further in this section.

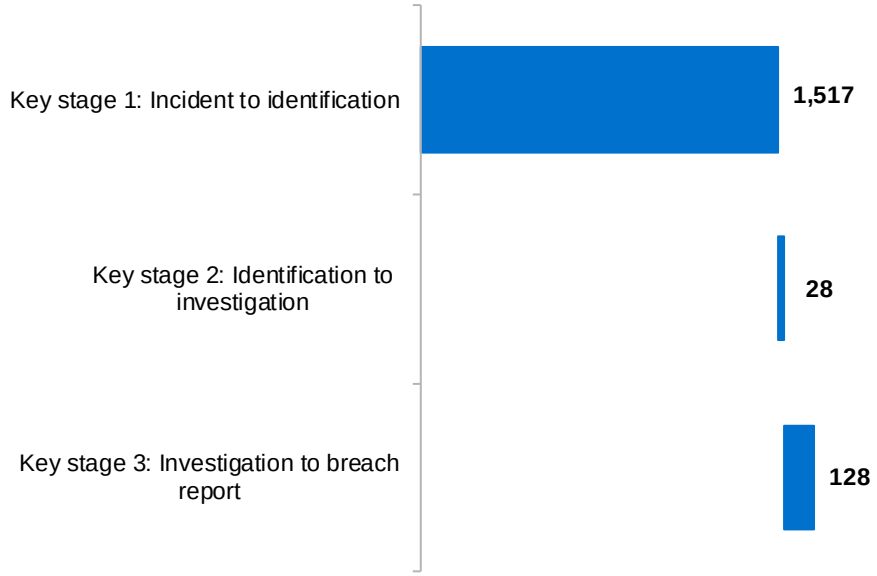
Table 6: Key stages of the reporting process

Key stage	Description	Further discussion
1 Identification of incident	The length of time between the first instance of the significant breach to identification of the incident.	Paragraphs 83–131
2 Identification to investigation	The length of time between identification of the incident and the start of the investigation into whether a significant breach has occurred.	Paragraphs 132–153
3 Investigation to breach report	The length of time between the start of the investigation into whether a significant breach has occurred and the date the significant breach report is lodged with ASIC.	Paragraphs 154–288

69 Figure 1 sets out the average calendar days for each reporting stage for all significant breaches the reviewed financial groups reported to ASIC between 2014 and 2017.

Note: The key stages of a significant breach are non-linear. This figure depicts the average duration in days for each of those key stages and should be considered only as indicative.

Figure 1: Average timeline of the reporting stages of a significant breach



Note 1: This figure is based on 686, 705, and 707 significant breaches, for key stages 1–3 respectively (out of 715) that had available data. Average calculations have included both positive and negative metrics.

Note 2: See Table 30 in Appendix 2 for the data shown in this figure (accessible version).

70 As Figure 1 shows:

(a) delays in significant breach reporting are primarily caused by AFS licensees failing to identify a possible breach;

(b) investigations usually begin swiftly, but delays can occur; and

(c) delays in reporting are also caused by the length of investigations.

71 The timeframes for each key stage in Figure 1 are displayed in a sequential or linear fashion. Mostly a stage commences following the completion of the previous stage (linear progression). We found that in around 90% of instances the reviewed financial groups reported a significant breach to ASIC after the end of their investigation.

72 But these stages do not always operate in linear progression. For example, an AFS licensee may identify a likely *future* significant breach and report to ASIC before the breach occurs. Another common instance of non-linear progression is where an investigation is still ongoing, but the licensee has been able to determine that a significant breach has occurred, based on known findings, and lodges a significant breach report to ASIC. The

investigation may then continue to quantify the total extent and impact of the breach and consider how to fix the breach.

Case study 1: Lengthy stages in the breach reporting process

An AFS licensee reported one significant breach that had occurred over approximately four and a half years, from the first instance to the last instance of the breach.

The breach related to the licensee failing to honour product quotes provided to consumers, which were supposed to be valid for a specified period of time. The licensee first identified an incident of this breach almost one and a half years after it started. Despite the incident being identified, it continued to occur over the next three years.

After the incident was identified, it took the licensee a further two years to record it as a breach in its breach register and start an investigation. Then there was an additional four months before the licensee reported the breach to ASIC as a significant breach. During this four months, the licensee sought and obtained legal advice on the breach.

The licensee had not taken the necessary steps to ensure that further breaches did not occur until just before reporting the breach.

73 The interdependence of the reporting stages means that delays at one stage can cause a ripple effect that increase delays at the other stages and intensify harm. In some instances, it can cause additional breaches to occur, unless appropriate measures are taken in a timely fashion.

Breach reporting policies and procedures

74 To have a full understanding of how key stages 1–3 of a significant breach are intended to operate, we examined the reviewed financial groups' policies and procedures for breach reporting (produced under notice).

75 The reviewed financial groups' AFS licensees have well-documented processes that, if implemented, appeared adequate to enable compliance with the breach reporting obligation. Once a breach was identified it was managed in a highly centralised process within the reviewed financial groups. This meant that while the financial services, products, packages, and root causes may change, the process for assessment and reporting was largely consistent. While there was some variation to AFS licensees' approach within a reviewed financial group, the policies were generally standardised.

76 All the reviewed financial groups' documented breach reporting processes contained the following common steps:

(a) identifying and recording incidents;

(b) assessing whether an incident is a breach;

(c) assessing whether a breach is significant; and

(d) if the breach is assessed as significant, a requirement that the relevant AFS licensee report it to ASIC within 10 business days of becoming aware of the significant breach.

77 Industry faces a challenge to capture, filter and analyse incidents to correctly determine whether they are significant breaches, non-significant breaches, or not breaches at all. It is paramount that they do so in a timely, accurate and effective manner.

78 We consider that policies and procedures are the foundation of effective compliance measures. Senior management must provide support and oversight, in conjunction with staff training, to ensure policies and procedures operate effectively and are complied with. Systems must also be appropriately resourced and targeted.

79 We consider that AFS licensees are best placed to identify instances of non-compliance in a timely manner when all these elements are established.

80 Many reviewed financial groups re-examined their processes, at least once in the last five years. A number of these re-examinations coincided with or occurred shortly after the release of ASIC comments on the importance of breach reporting. We consider this demonstrates a responsiveness to the clear messages coming from the regulator.

81 We have also been advised by some reviewed financial groups, since the end of the review, that their relevant policies and procedures have been updated more recently. As a result, these updates may have already addressed some of our observations and opportunities for improvement identified in this report.

82 In this section, we discuss the relevant policies and procedures for each key stage and AFS licensees' compliance with some aspects of them.

Key stage 1: Identification of incident

The length of time between the first instance of the significant breach to identification of the incident.

We found the delay in identifying breaches to be a serious problem. The average time from a significant breach starting to it being identified for investigation is 1,517 days—that is, just over four years (median: 925 days).

The time taken to identify a significant breach is the biggest factor that contributes to ASIC receiving breach reports about events or conduct that occurred some time ago.

The reviewed financial groups need to invest, and continue to invest, in systems that enable quicker identification of significant breaches.

83 Before an AFS licensee can begin to investigate a significant breach, it must identify that a potential significant breach has occurred. At this stage, AFS licensees generally refer to these potential significant breaches as 'incidents'.

84 An incident means a matter that the AFS licensee is investigating to determine whether the licensee has failed to comply with legislation, industry code, or its internal policies, procedures or arrangements, or whether there has been a system failure. Some examples of incidents include:

(a) inappropriate advice from representatives;

(b) unit pricing and fee errors;

(c) representatives operating outside the scope of AFS licence authorisations;

(d) deficient disclosure; and

(e) fraud in the supply of financial services by a representative.

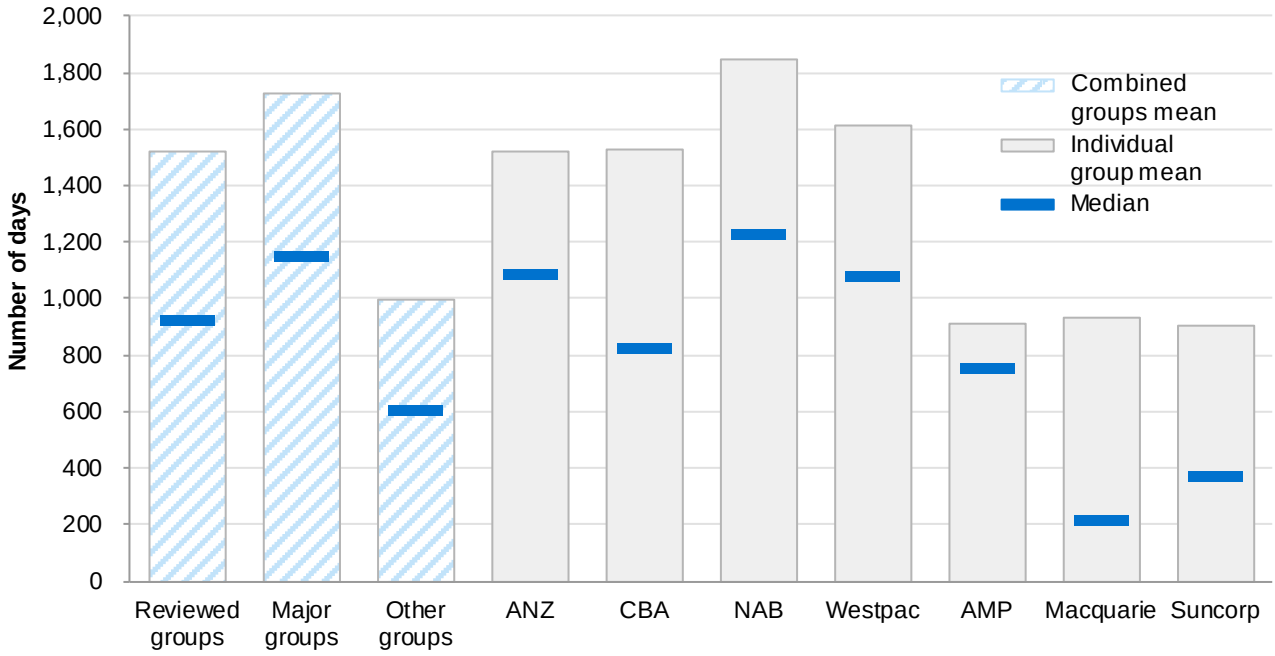
85 A complaint may also be considered an incident, but our review indicated that complaints were often part of a separate policy and managed through a separate process. However, we did find some examples where an AFS licensee's policy and procedure incorporated dealing with complaints as part of the management of incidents.

86 We found that relevant business units' staff identified most incidents that were later determined to be significant breaches (46% of incidents), while compliance and internal audit reviews together identified 20% and consumer complaints identified 10%.

87 We found the length of time taken to identify the significant breach as an incident is the biggest factor that contributes to ASIC receiving significant breach reports about events or conduct that happened many years ago.

88 Figure 2 sets out the average and median days from the first instance of the significant breach to the identification of it as an incident.

Figure 2: Average time taken for key stage 1, by reviewed financial groups



Note 1: This figure is based on 686 significant breaches (out of 715) that had available data. The standard deviation for all the reviewed financial groups is 1,590 calendar days. It does not separately display individual groups that had available data for 10 or fewer significant breaches.

Note 2: See Table 31 in Appendix 2 for the data shown in this figure (accessible version).

89 Based on the reviewed financial groups' current average, some significant breaches that start today may not be identified as an incident by an AFS licensee before 2022. This projection assumes no improvements in AFS licensees' ability to identify breaches.

90 Table 7 sets out the distribution of when significant breaches were identified as incidents.

Table 7: Distribution of significant breaches by time taken to identify incident

Year	Number of significant breaches
Before first instance	12
Year 1 (0–365 days)	188
Year 2 (366–730 days)	81
Year 3 (731–1095 days)	98
Year 4 (1096–1460 days)	51

Year	Number of significant breaches
After year 4 (more than 1460 days)	256
Total	**686**

Note: This table is based on 686 breaches (out of 715) that had available data.

91 Breach reports should be reported as 'likely' if they are yet to occur. Of the 12 significant breaches that were identified before first instance, only one was reported to ASIC as a likely significant breach: for information on likely breaches, see paragraph 47.

92 We are concerned that at least 256 of the 715 significant breaches reviewed went undetected for more than four years.

93 Many of these breaches are not one-off events but continuing failures. The late detection of significant breaches has a domino effect, with older breaches generally being more difficult to investigate—including identifying the root causes, the products, packages and systems potentially affected, and quantifying the impact on any affected consumers. Further, the investigation and rectification may be more resource intensive and expensive for AFS licensees, consumers may be entitled to greater remediation, and ASIC may consider a need for a stronger regulatory response to the breach. Based on the data, the major financial groups particularly need to improve their ability to identify incidents earlier.

94 All AFS licensees need to consider how best to monitor existing practices to identify incidents and to do so in a much timelier fashion. They should also consider committing further resourcing to this task and where best to allocate both existing and new resources. AFS licensees are required to have adequate training, resources and systems—including adequate and effective compliance measures and risk management systems to ensure compliance with their license obligations: see s912A(1).

> Note: For guidance on when we assess AFS licensees compliance with general obligations in s912A(1), see RG 104.

95 We are also concerned that in 29 instances, the reviewed financial groups were unable to identify and advise when the breach started. This leaves the possibility that the full extent of the breach, and total number of consumers affected, cannot be determined—despite, in some instances, lengthy investigations.

Case study 2: Investigating old breaches

An AFS licensee could not advise when one significant breach started, despite having conducted investigations for almost two years and identifying historical concerns with fee disclosure on some types of credit and debit cards.

The availability of data meant that the licensee could only identify instances that had occurred in the previous seven years (which totalled around $7 million in overcharged fees). As a result, the remediation was limited to the identified $7 million overcharged. Further investigation of unavailable data may have revealed a greater impact.

Domino effect: Number of significant breaches and consumers

96 We are concerned that this lapse in time may have a profound effect on the volume of significant breaches that occur. In 98 instances, AFS licensees identified the length of time that the breach remained undetected as a factor in determining that a breach was significant: see paragraphs 183–189.

97 We expect that more timely identification of breaches will reduce the duration of breaches and number of significant breaches. Once identified, a fix can be implemented, likely leading to:

(a) fewer consumers affected; and

(b) less financial loss to those consumers that are affected.

98 In Table 8 we summarise the financial loss incurred by consumers based on the duration of significant breaches reported to ASIC by reviewed financial groups between 2014 and 2017. We further explore the financial loss incurred by consumers in Section D.

Table 8: Effect of duration of significant breaches on consumer financial loss

Duration of breach	Number of breaches with financial loss	Number of consumers affected	Total loss for consumers	Average loss per breach	Average loss per consumer
0–4 years	134	2,243,029	$165,623,117	$1,235,993	$73.84
More than 4 years	134	2,188,749	$305,238,962	$2,277,903	$139.46
Total	**279**	**4,959,214**	**$497,241,980**	**$1,782,229**	**$100.27**

Note: This table is based on 279 significant breaches (out of 715) with applicable data. A further 11 significant breaches incurred financial loss to consumers, but the AFS licensees were unable to provide all dates required to calculate the duration of those significant breaches. These 11 significant breaches affected 527,436 consumers, with a total loss of $26,379,901, an average loss per breach of $2,398,173, and an average loss per consumer of $50.02.

The average loss per breach is calculated using the total loss for consumers and dividing it by the number of breaches with financial loss. The average loss per consumer is calculated using the total loss for consumers and dividing it by the number of consumers affected.

99 In total, we found 279 significant breaches incurred financial loss to consumers. Almost 5 million consumers were financially affected by those breaches, with a total financial loss of approximately $497 million. This equates to an average loss per significant breach of around $1.8 million, and around $100 per consumer.

100 Despite a similar total number of consumers affected and the same number of significant breaches with financial loss, the consumer impact is noticeably greater in instances where the breach went undetected by AFS licensees for four or more years.

101 The total financial loss to consumers in breaches of this duration is just over $300 million—close to double the financial impact of significant breaches identified in the first four years (just short of $166 million).

102 In addition, for those significant breaches identified after four or more years, the average loss per significant breach is around $2.2 million and the average loss per consumer is around $140—also close to double the financial impact when compared to the respective losses for significant breaches identified in the first four years (around $1.2 million and just short of $75, respectively).

Opportunities for improvement

Recognising emerging systemic issues: Red flags

103 We found instances where AFS licensees failed to quickly recognise indicators of a breach (e.g. consumer complaints and other systemic issues) that should have been a 'red flag' that the incident, if not already recognised as an incident, needed to be investigated thoroughly. Examples of red flags include consumer complaints, whistleblowers, consumer remediation, and consequence management. Further, findings from third parties, such as external dispute resolution (EDR) schemes or code compliance committees, may also be considered red flags.

104 We found that a whistleblower identified only one of the 715 significant breaches reported by the reviewed financial groups between 2014 and 2017. We would be concerned if this number was markedly higher. If staff are able to raise concerns internally, there should be very few breach reports made by whistleblowers.

105 We found that 67 significant breaches were identified by way of complaint, while only three were identified by way of EDR schemes. The investigation into nine of the 67 significant breaches identified by way of complaint only commenced after receiving 10 or more complaints. For three of these breaches, over 100 complaints were received before the AFS licensee began an investigation. We are pleased that we identified many instances (58) where investigations were begun after nine or fewer complaints and the majority of these breaches only had one or two complaints.

106 In some instances, the AFS licensee conducted an investigation after receiving just a single consumer complaint, rather than multiple complaints. This was pleasing and should be modelled where appropriate by all licensees.

Case study 3: Investigating one consumer complaint

An AFS licensee received a single complaint from a consumer about poor advice. After confirming that the complaint was valid, the licensee was proactive in making inquiries about whether the issue was isolated or systemic. The result of the investigation was that the issue was systemic, and the licensee reported a significant breach to ASIC.

107 Where ASIC or another unrelated third party (excluding external auditors) identifies the breach, this indicates that the AFS licensee's three lines of defence have failed. First, the breach was allowed to occur, then the licensee failed to identify it before it was raised by the unrelated third party.

108 AFS licensees' attention and response to consumer complaints about matters that appear to be systemic can uncover an underlying significant breach and limit its adverse impact. Such complaints may often be channelled through a licensee's internal dispute resolution (IDR) process.

Case study 4: Consumer complaints and potential red flags

An AFS licensee identified that nearly 200 consumer complaints received within one year through the IDR process were about home loan offset arrangements within the broker channel.

The licensee conducted an investigation and identified approximately 2,000 active accounts with offset account linkage errors, resulting in a number of these consumers not receiving the benefits of an offset account and paying too much interest on their home loan.

109 This case study is also an example of where system enhancements were implemented during the breach rectification (although systems deficiency was not a root cause) to improve the overall consumer experience and show consumers details of their linked offset account and the amount of interest saved on their home loan via the offset arrangement.

Case study 5: Consumer complaints and potential red flags

An AFS licensee reported a significant breach, relating to account opening errors that occurred over an eight-year period. This systemic issue affected over 100,000 consumers who were unable to access the full benefits of their account.

The licensee had started to receive complaints four years before making the breach report to ASIC. An initial investigation only identified part of the root causes and complaints continued. A second investigation revealed more and led to the breach report to ASIC; however, by this stage the licensee had received over 120 complaints.

Recognising emerging systemic issues: Compliance systems

110 AFS licensees need to continue to develop their data analytics abilities, along with the quality of compliance data, so that they can more quickly identify emerging systemic issues.

> Note: In this report, we refer to 'compliance systems' as generally any systems that record and monitor incidents for the purposes of managing risk.

111 All reviewed financial groups had a system that was used to record, manage, and escalate incidents, which was supported with corresponding policies and procedures for staff to follow.

112 Some reviewed financial groups used an online form that captured details of the incident and automatically populated the AFS licensee's breach register: see paragraphs 250–257.

113 We consider that, when systems are appropriately resourced, used and audited, they should better identify instances of non-compliance in a timely manner.

114 In our view, there is a greater risk that systemic issues and similar previous breaches will go unnoticed in circumstances where AFS licensees use multiple systems to raise, review and record breaches (no matter how classified) that will then be subject to ongoing interrogation, searching, and consideration per incident raised.

115 We are concerned that some of the reviewed financial groups' development of these capacities has until recently been neglected.

116 This issue not only affects AFS licensees' ability to identify systemic issues, but also affects their ability to manage risks—including investigating an incident, reporting a significant breach, and managing the rectification and remediation of significant breaches.

Case study 6: Compliance systems

An AFS licensee's external audit during the review period found it was not possible to conduct analysis of risk indicators such as customer complaints, operational issues, and financial data (e.g. customers' refunds) to look for systemic compliance issues. The audit found that the present incident data was inadequate, incomplete and inaccurate and as such would inhibit conducting such an analysis.

In 2018, despite years attempting to improve the system, the licensee still had great difficulty searching their compliance system and, therefore, delivering reports of misconduct.

117 The reviewed financial groups' current efforts to reduce the level of inadequate, incomplete and inaccurate incident data will likely see an improvement over time in their ability to be proactive and swiftly identify

emerging systemic issues. This will not be a quick transformation for some. The ability to identify existing systemic issues will be hampered until such time that their systems accurately capture the necessary information or data necessary for identification.

Recognising emerging systemic issues: Product systems

118 The age, complexity and diversity of products and business unit systems inhibit the identification of incidents that, after investigation, are determined to be breaches.

Case study 7: Product systems

An AFS licensee reported a significant breach, relating to automatic funds transfers.

Direct debits for a service in approximately 2,000 accounts were not correctly cancelled on the system and, as a result, approximately $3 million in fees were incorrectly collected.

These fees could be charged to accounts operated on seven different systems within the licensee.

The identification, investigation and remediation were made more complex by the different systems that also had at times different data formats.

Encouraging staff to report incidents

119 Staff within business units identified 46% of significant breaches (331 out of 715 significant breaches) in this review.

120 All reviewed financial groups' policies and procedures made staff and management responsible for identifying and reporting incidents. Policies and procedures varied, but AFS licensees usually allowed up to five business days for staff who identified the incident, or the business unit to which that staff belonged, to record the incident in the relevant system.

121 All reviewed financial groups made identifiable efforts during the relevant period, with some making efforts before the review, to improve staff awareness of breach reporting and the accessibility of the channels for staff to raise and report an incident. The reviewed financial groups are aware that this is an area for ongoing improvement.

Case study 8: Staff reporting incidents

A reviewed financial group surveyed the perceptions of its staff on risk management. They found 70% of staff were comfortable speaking out about risks in 2016, an increase from 53% for the previous year.

122 Reviewed financial groups were able to point to current practices that were designed to promote compliance, including, but not limited to:

(a) regular compliance statements;

(b) a percentage of the representative's bonus being dependant on compliance, often with a 'gateway' feature that made some or all of the bonus unavailable if a certain level of compliance was not achieved; and

(c) statements from chief executive officers (CEOs) or other key figures about the importance of compliance.

123 These practices were focused on the staff's own compliance. We found a limited use of recognition and reward for individuals who raised incidents. Only nine of the 331 significant breaches identified by staff resulted in any formal recognition or reward for the identifying staff member. The reviewed financial groups usually saw such actions as staff meeting the requirement to report incidents once identified. AFS licensees should consider whether greater and more transparent use of recognition and reward would encourage staff to raise incidents and make them more comfortable doing so.

124 We identified a range of procedures, some more developed than others, to enable AFS licensees to share progressive details and findings throughout an investigation into the breach. This extended to sharing the root causes and other learnings with staff within the business unit that identified the significant breach.

125 Greater transparency during the process, both to the individual identifying the matter and the organisation more broadly, can demonstrate the importance of raising matters and that the organisation has taken action that is consistent with their stated values and their legal requirements.

126 It is impossible to know how many incidents could have been identified earlier if staff were more willing to raise concerns about risks. However, until there is a culture and embedded practice of raising concerns about risks within all AFS licensees, the likelihood remains that significant breaches will be identified later than they should be: see further discussion in Section E.

Compliance and audit

127 The importance of audit and assurance in encouraging compliance and identifying non-compliance is well established in the reviewed financial groups, with compliance and audit functions identifying 20% of the significant breaches in this review. The level of resourcing for these functions impacts the AFS licensee's ability to identify matters.

128 We were disappointed to observe a number of significant breaches where it appeared that AFS licensees had failed to be proactive in thoroughly

investigating the incident. In extreme examples, the AFS licensee suspected there was a breach but failed to adequately resource the audit work that may have identified the full extent of it earlier.

Case study 9: Adequate resourcing

An AFS licensee reported a significant breach relating to reconciliation discrepancies. These discrepancies occurred for approximately eight years before the licensee first resourced a project to identify, analyse and rectify the full extent of the problem. However, this review was curtailed and absorbed into the business as usual work.

Two years later the problem remained unresolved. A second project was resourced; but, despite there being a substantial amount of work left to be done, the project was again curtailed and absorbed into the business as usual work.

There were strong indicators that the problem remained; however, it was a further two years before the licensee quantified the extent of the problem and formed the view a significant breach was reportable. This was 12 years after reconciliation discrepancies started.

129 The effectiveness of audit and assurance depends on how limited resources are deployed and, once deployed, what questions are asked.

Case study 10: Adequate controls

An AFS licensee reported a significant breach by a financial adviser. During six years of employment, the adviser maintained a 'low' risk rating, despite failing to follow the internal and regulatory requirements. This was unidentified for a long period, as the control within the licensee was not effective in identifying and/or preventing non-compliance with business process and policies.

The licensee was aware of this weakness in the controls before the misconduct of the adviser was identified. However, the controls were only updated after the adviser had left and the extent of their misconduct started to emerge.

Proactive approach to incident identification

130 We have dealt with instances where AFS licensees failed to adequately review and/or monitor systems to ensure that they worked as intended as part of sound business practice. Licensees should have clear internal ownership of this practice.

131 AFS licensees regularly reviewing their compliance measures to ensure that they are implemented and effective can help in identifying and dealing with potential issues earlier. A review of compliance measures becomes more imperative where there is a change.

Case study 11: Failure to review compliance measures

An AFS licensee reported a significant breach relating to a failure to properly refund fees and interest incurred on successfully disputed transactions.

The licensee considered the significant breach likely dated back to 2007, but only had available data back to 2009.

The licensee's investigation, conducted between 2016 and 2017, revealed that they had an opportunity to identify the breach earlier (in 2014) when the process was transferred between business units. However, the new business owner did not review the previous compliance measure, which would have identified that in 20% of cases the licensee had failed to properly refund fees and interest on successfully dispute transactions.

Key stage 2: Identification to investigation

The length of time between identification of the incident and the start of the investigation into whether a significant breach has occurred.

Generally, investigations are resourced and commenced swiftly after incidents are identified. Of the 715 significant breaches reported to ASIC, 544 investigations started within 10 days of the incident being identified. However, we were particularly concerned that in 98 instances the investigation started more than 40 days after the incident was identified.

Across the reviewed financial groups, the average time for key stage 2 is 28 days (median: 0 days).

Delays in commencing an investigation may, in part, occur due to a failure to record incidents in a timely fashion—despite the AFS licensees' own internal procedures.

132 Once an incident has been identified, it needs to be escalated if an investigation is to occur. The escalation is not instantaneous. AFS licensees commonly require the incident to be recorded on the relevant system, which may include details of the incident, for the incident to progress to the relevant area (i.e. compliance) for an initial assessment and investigation.

133 The time taken to escalate is a key stage, because delays here are a risk that need to be managed and ideally avoided.

Time taken to record an incident

134 The reviewed financial groups had policies that required swift recording of incidents, commonly within five business days of the incident being identified. However, we found there were many instances where AFS licensees frequently took three times longer to record the identified incident.

135 Delays within this key stage can unnecessarily affect the start of the investigation and have both incremental and detrimental effects on the timing of reporting and rectification of significant breaches.

136 The reviewed financial groups took an average of 22 days (median: 3 days) to record an incident in the relevant system after identification. The median is consistent with the general policy of recording an incident within five business days. However, the average would suggest that the stated expectation of prompt recording of incidents is not always occurring in practice.

137 Based on the distribution, we found that 451 significant breaches had been recorded in accordance with this common timeframe set by AFS licensees, while in 252 instances AFS licensees recorded incidents more than five business days after identification.

138 Where AFS licensees create policy and set internal requirements, but fail to enforce them, this indicates a level of acceptance for internal non-compliance.

Time taken to start an investigation

139 Across the reviewed financial groups, the average time for key stage 2 is 28 days (median: 0 days).

> Note: The standard deviation for key stage 2 is 129 days, which shows that the distribution has outliers. It means that, in some instances, the investigation started much later or earlier than 28 days after the breach was identified.

140 The data shows that at least 50% of investigations into the reported significant breaches started immediately after the incident was identified. The distribution is best illustrated at Table 9, which shows that the reviewed financial groups generally resourced and commenced an investigation within 10 days of identifying the incident.

141 We encourage this process. Where it is not possible to immediately investigate an incident, we encourage AFS licensees to ensure investigations are resourced as swiftly as possible.

Table 9: Number of significant breaches by days for key stage 2

Days from identification to investigation	Number of significant breaches
Less than 11 days	544
11–20 days	28
21–30 days	22
31–40 days	13

Days from identification to investigation	Number of significant breaches
More than 40 days	98
Total	**705**

Note: This table is based on 705 significant breaches (out of 715) with applicable data.

142 For the most part, investigations are resourced swiftly. We found that 544 investigations started within 10 days of the incident being identified; however, 98 investigations started more than 40 days later. This accounts for the difference between the average and median days.

143 There are also inherent risks in practices that do not adequately monitor such reporting and escalation. AFS licensees may be unable to identify systemic issues as they arise and, as discussed in key stage 1 at paragraphs 96–102, prolonged and unidentified issues can manifest, resulting in breaches of greater significance both for AFS licensees and any affected consumers.

Opportunities for improvement

Timely recording of incidents

144 All the reviewed financial groups had a system that was used to record, manage, and escalate incidents. The system is usually group-wide, rather than segregated at the AFS licensee level, but some systems were divided according to AFS licensees within the reviewed financial groups.

145 As we observed at paragraph 136, the reviewed financial groups took an average of 22 days (median: 3 days) to record an identified incident in the relevant system. This observation closely aligns with our observation that the reviewed financial groups took an average of 28 days (median: 0 days) for key stage 2.

146 The timeliness in AFS licensees recording an incident, and the possible failure to comply with internal standards (e.g. to record the incident within five business days), may partly explain why the start of some investigations may be delayed.

147 A tolerance for the failure to comply with timeframes set in internal policy may be having a more profound impact than AFS licensees would otherwise anticipate. In our view, such tolerance does not reflect a sound breach management culture.

148 We were pleased to find one instance where an AFS licensee's policy and procedure required an explanation if there was a delay of more than two days in recording the incident after it was identified.

Appropriate recording of incidents

149 An element of a sound breach management culture is having systems in place that allow information about breaches, and incidents more broadly, to be recorded accurately, tracked and kept up to date: see further discussion in Section E.

150 In our review, we observed that incident information was:

(a) often recorded in a fragmented fashion over many databases;

(b) often not searchable—key information could not be easily extracted as required; and

(c) sometimes missing key data (e.g. the data RG 78 recommends AFS licensees record was not included in the system).

151 Further, the current systems often inhibit the identification and management of breaches, both significant and otherwise. They also affect the AFS licensees' ability to quickly respond to our requests for information on breaches.

152 Where a sound breach management culture exists, we would expect to see that:

(a) once a matter has been identified as a breach, systems are in place to ensure staff are able to record details of that breach, including how it was identified, and track how the breach is being addressed including its ongoing progress;

(b) staff using the system can easily extract data about the breach and report on different aspects in real time; and

(c) the quality of information being recorded on breaches is subject to regular audits.

153 The quality of information that is recorded directly affects the accuracy and completeness of breach registers and breach reports. We recommend AFS licensees consider whether their existing compliance systems and surrounding practices could be improved to better record and track incidents (including complaints) and enable an accurate real-time view of incidents (including those later determined to be significant breaches).

Key stage 3: Investigation to breach report

The length of time between the start of the investigation into whether a significant breach has occurred and the date the significant breach report is lodged with ASIC.

Approximately one in seven significant breaches (110) were reported to ASIC more than 10 business days after the AFS licensee became aware of the breach. Most non-compliance was between one and three days late.

In too many instances it takes too long to report a matter to ASIC once an investigation has begun. We found that across the reviewed financial groups, the average time for key stage 3 was 128 days (median: 69 days). We are particularly concerned that one in four investigations take longer than 168 days to report to ASIC.

154 Investigations are the examination of incidents—usually by the compliance function, with support from the relevant business unit(s) and, if necessary, legal advice—to determine whether the incident is both a breach and significant. An investigation can be simple or complex and require varying levels of resources and inquiries to reach a finding.

155 AFS licensees rely on the findings, either preliminary or final, and recommendations of these investigations to allow their key decision makers to determine if a breach is reportable.

> Note: In this report, we refer to the individual or group that considers and determines whether there is a significant breach for the purpose of the breach reporting obligation as the 'key decision maker' or 'key decision-making group' (as applicable).

156 Only after an AFS licensee's key decision makers determine that an incident is a significant breach does the licensee consider it has become aware and must lodge a report with ASIC within 10 business days.

157 We found that, across the reviewed financial groups, it took AFS licensees an average of 128 days (median: 69 days) for key stage 3: see Figure 3 for a breakdown across the reviewed financial groups.

158 We found it took the major financial groups an average of 150 days (median: 95 days) to investigate and lodge a breach report to ASIC. The major financial groups' average was double that of other financial groups that took an average of 73 days (median: 34 days).

159 We want to understand why there is such a difference between the major financial groups and other financial groups.

Figure 3: Average number of days for key stage 3, by reviewed financial groups

Note 1: This figure is based on 707 significant breaches (out of 715) that had available data. The standard deviation for all the reviewed financial groups is 185 calendar days. It does not separately display individual groups that had available data for 10 or fewer significant breaches.

Note 2: See Table 32 in Appendix 2 for the data shown in this figure (accessible version)

160 Based on the above current averages, some significant breaches that start today may not be reported to ASIC before 2023. This projection assumes no improvements in AFS licensees' the ability to identify and investigate breaches.

161 We acknowledge that investigations of potential significant breaches will invariably require time to obtain and analyse the available information before an AFS licensee is in a position to determine whether there is a reportable significant breach. Nevertheless, we want to be notified of matters earlier than is currently the case. Further, the reviewed financial groups should have a strong desire to improve the efficiency in running investigations.

162 That said, we were pleased to find that 58 significant breaches were reported to ASIC before the end of the AFS licensee's investigation into the breach.

163 This means the licensee was satisfied, based on the information on-hand, that the breach was significant and did not wait until the investigation was complete to report the matter to ASIC. This is consistent with our guidance and we encourage this to continue where possible.

164 The limited number of reports prior to the end of an investigation may be driven by a legalistic approach that requires the group to have knowledge of the full extent of the breach before it is willing to determine that a significant breach has occurred.

165 AFS licensees need to critically monitor their investigations, so that they can be responsive and act when timeframes begin to slip.

166 The overall timeframes are influenced by several possible steps in key stage 3. We have set out these steps and made further observations on them at paragraphs 167–257.

Investigation of incident

167 The reviewed financial groups' policies and procedures generally made the compliance area responsible for investigations of incidents and required assistance from the relevant business unit. Where there was oversight of the investigation, it was usually the responsibility of the risk and compliance functions. The procedures included an initial assessment of whether the incident could be a potential breach of the law. Some AFS licensees set timeframes for the initial assessment to be completed (e.g. five business days). If the assessment found no breach was possible, then a fuller investigation was not undertaken. The basis for the assessment is then recorded.

168 However, we also identified an alternate approach where the significance of an incident was first considered before proceeding to consider whether a breach has occurred. A benefit of this approach may be the prioritisation of incidents; however, if there is no further assessment of the incident to determine whether a 'non-significant' breach has occurred, this may create a risk that systemic issues are not identified and addressed.

169 To avoid this risk, AFS licensees need to eventually assess whether the incident is a breach and take any necessary steps to address it. This includes recording the outcome of the assessment to allow identification of emerging systemic issues.

170 If, after the initial assessment, the incident remains a potential significant breach or is determined to be a breach but has not been determined as significant, the AFS licensee continued their investigation. It was common that the full extent of an incident required further investigation to be understood. In practice, this may be a continuation of the same investigation or escalated to the relevant team for further investigation. We found that polices had an implicit and sometimes an explicit expectation that if the incident was found to be a breach, the escalation would occur immediately.

Investigation of breach

171 A central purpose of all investigations is determining whether an incident is a breach and, if so, determining whether it is significant.

172 Investigations of potential significant breaches will invariably require time to obtain and analyse the available information before an AFS licensee is able to determine whether it is a significant breach.

173 We observed that most of the policies and procedures did not provide any timeframes for investigating incidents, although some indicated that the investigation should be conducted as a priority and expeditiously: see paragraph 132. One reviewed financial group's policy set out the principle that its AFS licensees must investigate each incident without delay. However, this principle did not appear to translate into the policies and procedures of those licensees or business units.

174 The length of the investigation could depend on numerous factors, including:

(a) the age of the potential breach;

(b) the period it occurred over;

(c) the number of consumers, products and systems affected;

(d) the records available; and

(e) the nature of the potential breach.

175 While it may not be practical to set a clear timeframe for when an investigation should be completed, nor is there a statutory period, it is possible to set expectations about how long is reasonable before additional reporting and oversight is required. We consider that this gap may have contributed to prolonged investigations. The lack of clear policies and procedures on the length of investigations may have also contributed to our observation that it was rare for prolonged investigations to be challenged.

176 Despite the lack of stated timeframes, we did find some policies and procedures containing the principle that the investigation was a priority and should be conducted quickly.

177 The ability to determine whether a breach has occurred will depend on the facts and specifics of the regulatory requirement. In addition, AFS licensees often seek legal advice—internally, externally or both—and this can extend the length of investigation. This may also include seeking legal advice about the significance of the potential breach.

Potential impact of legal advice

178 RG 78.29 sets out that an AFS licensee should inform ASIC of significant breaches as soon as practicable and, if legal advice is not needed to determine a breach or its significance, should not wait until the breach (or likely breach) has been considered by the licensee's internal or external legal advisers.

179 Table 10 sets out the number of breaches that the AFS licensees did and did not seek legal advice on.

Table 10: Number of breaches with and without legal advice

Significant breach type	Number of breaches
Breaches with legal advice	531
Breaches without legal advice	184
Total number of breaches	**715**

Note: This table is based on all 715 breaches.

180 We found the major financial groups sought legal advice on approximately 80% of their significant breaches, while the other financial groups sought legal advice on approximately 60% of their significant breaches.

181 Table 11 suggests a correlation between AFS licensees seeking legal advice and the length of time it takes to report to ASIC. It took an average of 35 days longer to breach report if AFS licensees sought legal advice (median: 42 days longer).

Table 11: Number of breaches with and without legal advice, by days for key stage 3

Significant breach type	Average number of days	Median number of days
Breaches with legal advice	137	83
Breaches without legal advice	102	41

Note: This table is based on 707 significant breaches (out of 715) that had available data.

182 AFS licensees are best placed to determine the need for legal advice, but they should be aware that seeking legal advice may be one factor that adversely affects the timeliness of the breach report. In this review, we did not test whether the legal advice was appropriate.

183 Reviewed financial groups currently have policies that external advice is sought on a case-by-case basis. We consider this to be in line with ASIC guidance. The high percentage of significant breaches that involved seeking legal advice could be an indication of an unnecessarily legalistic approach.

Investigation of significance

184 In this review, we examined all factors that led AFS licensees to conclude that each breach was significant, including the factors in the significance test. As previously noted, these are:

(a) the number or frequency of similar previous breaches;

(b) the impact of the breach or likely breach on the AFS licensee's ability to provide the financial services covered by the licence;

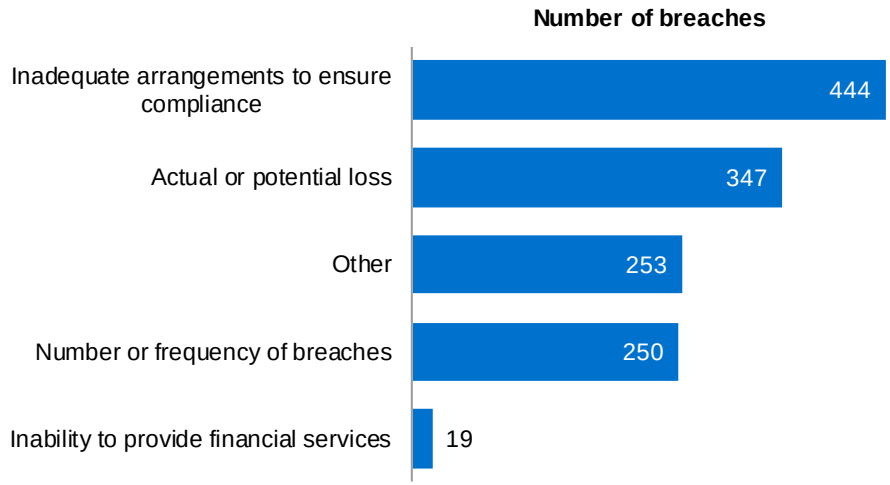
(c) the extent to which the breach or likely breach indicates that the AFS licensee's arrangements to ensure compliance with those obligations is inadequate;

(d) the actual or potential loss to clients or the AFS licensee itself; and

(e) any other matters the regulations prescribe.

185 As part of our review, we allowed the reviewed financial groups to select more than one significance test factor, if applicable. This was because multiple factors may have led an AFS licensee to conclude the breach is significant.

Figure 4: Frequency of significance test factors in determining whether a breach is significant



Note 1: This figure is based on all 715 significant breaches.

Note 2: See Table 33 in Appendix 2 for the data shown in this figure (accessible version)

186 The most frequently selected significance test factor was 'inadequate arrangements to ensure compliance' (444), followed by 'actual or potential loss' (347). The third most common legislative factor was 'other' (253).

187 We acknowledge that the 'other' factors considered by AFS licensees in assessing significance are likely to be specific to their business, but should not distract from the intent of the significance test. For example, one reviewed financial groups considered the number of brands affected by the breach in its determination of significance.

188 Of the 253 significant breaches with an 'other' determining factor, AFS licensees declared, as a factor in their consideration of significance:

(a) the length of time the breach went undetected for 98 breaches; and

(b) the number of consumers or members that the breach affected for 84 breaches.

189 The high proportion of the 'other' category suggests there is scope for additional prescriptive factors in determining significance to reduce ambiguity for AFS licensees and improve consistency in reporting. Based on the data, it may be appropriate for potential law reform to consider these two 'other' factors in s912D(1)(b).

190 AFS licensees have a healthy desire to be aware of the size and scope of the breach to determine whether a breach is significant. AFS licensees place emphasis on investigating the impact of the breach in terms of the number of consumers affected and the extent of consumer financial loss.

191 However, delaying reporting until further investigation is completed is not needed to confirm that a breach is significant when known issues are extensive and impact multiple processes and products.

Case study 12: Delays caused by determination of significance

An AFS licensee identified a systemic issue that had previously been undetected for 10 years.

Based on the adequacy of their supervisory arrangements for their systems and the likelihood of consumer losses, the AFS licensee's compliance area had escalated the matter, during the investigation, to the key decisionmakers with a recommendation to report the matter to the regulator.

The key decision makers did not accept the recommendation, requesting the number of consumers affected and the financial impact of those losses before making a determination of significance.

The report was lodged six months later with no apparent progress on identification of consumer impact, other than to base the decision to report on the original recommendation and previous experience.

Case study 13: Delays caused by determination of significance

An AFS licensee produced a progress report created during the course of its investigation into whether the breach was significant.

It noted that the root causes of the breach were still being determined, but included:

> poor detective controls (lack of exception reporting), multiple manual processes, multiple hand off points, having grandfathered packages, complicated product design and staff oversight/error.

The report also noted the licensee was 'currently sizing up the number of impacted customers and the dollar value of any remediation'—preliminary estimates indicated that affected consumers made up 20% of all packages distributed, with around $5 million overcharged.

> Despite the extent of the root causes, the diverse range of affected products, the number of potential affected consumers, and the size of dollar estimates, the report provided a status update that the compliance function was assessing whether the event would be reportable.

Subjectivity of the significance test

192 We found the subjectivity of the significance test affects the consistency and number of significant breach reports. The reviewed financial groups who appeared to have a low bar for significance reported a higher number of significant breaches to ASIC. This is consistent with a more transparent and less legalistic approach to breach reporting.

193 This is also consistent with our experience and supports our arguments in our submissions to the ASIC Enforcement Review that the test for significance needs to be more objective.

> Note: See ASIC, *Self-reporting of contraventions by financial services and credit licensees: Submission by the Australian Securities and Investments Commission* (PDF 1.1 MB), May 2017, Section A.

194 The data supports this observation—the major financial group that reported the most significant breaches, NAB, had a relatively lower median total consumer financial loss for its significant breaches: see Table 12. In contrast, the major financial group that reported the least significant breaches, Westpac, had the highest median total consumer financial loss.

Table 12: Subjectivity of the significance test—Major financial groups

Category	CBA	Westpac	NAB	ANZ
Number of significant breaches with financial loss to consumers	34	19	121	40
Median total consumer financial loss	$709,827.91	$1,407,010.84	$206,538.00	$991,040.21

195 We consider a comparison between the major financial groups on this point is reasonable, based on their similar size and profiles. However, it is important to note that reporting levels are also affected by the reviewed financial groups' compliance with requirements. We note that a low number of recorded breaches can be because a group is generally compliant, or because its AFS licensees either have not identified breaches or have been unwilling to report them as such once identified. Conversely, a high number of recorded breaches relative to its peers can indicate that the group implemented a thorough breach identification, recording and, ultimately, rectification process, or it had a higher level of noncompliance.

196 The significance test, as currently drafted, is not objective. It requires AFS licensees to make a judgement about the effect of the breach on them or their clients. The result of this subjectivity is that, although all licensees have an

obligation to report, the differing scale, nature and complexity of their respective businesses and balance sheets (see RG 78.12) can mean that larger firms tend to report fewer breaches or less often—depending on the precise interplay of each of the factors, of which consumer financial loss is only one, in the particular circumstances.

Note: See *ASIC Enforcement Review taskforce report*, December 2017, pp. 4–5.

Case study 14: Error rate

In evaluating significance, one AFS licensee used an 'error rate' calculation, effectively working out what proportion of accounts had been affected by the breach. This calculation was included in the final report that was considered by the key decision makers when determining the breach's significance and reportability.

In this instance, close to 3,000 out of 400,000 current accounts were affected by the breach. The error rate, or proportion of accounts affected, was less than 1%.

The licensee's key decision makers appeared to give greater weight to other factors in its assessment (i.e. the dollar impact, ineffective processes to manage product features, and other historical issues regarding the product).

However, this highlights the subjectivity of the significance test—the licensee's key decision makers could have been swayed by any one or a combination of the following metrics:

- less than 1% error rate;
- close to 3,000 accounts affected by the breach; and
- up to 400,000 accounts potentially affected by the breach.

197 Since the AFS licensee assesses significance from its own perspective, its perception of whether a breach is significant can differ from that of an external assessor, including ASIC.

198 We found AFS licensees had internal risk matrices to help staff determine significance; however, additional and more specific examples, benchmarking and thresholds may help ensure staff make consistent determinations. For example, one reviewed financial group had set a significance threshold of $1 million in financial loss where the breach must be reported as a significant breach. AFS licensees within the reviewed financial group were still able to determine breaches under this threshold as significant.

199 The current legal settings allow for an undefined period of investigation and are only specific about the timing of reporting once awareness has been achieved. Therefore, we support Recommendation 4 of the ASIC Enforcement Review, which proposes that significant breaches (and suspected breach investigations that are ongoing) must be reported within 30 days.

200 We found that the significance test contributes to delays in reporting breaches to ASIC. The review identified instances where key decision makers had been unable or unwilling, based on known information, to determine significance until an investigation produced more certainty around the extent of impact (i.e. total consumers affected and total losses).

Case study 15: Adopting a structured approach to assessing 'significance'

An AFS licensee adopted a simple methodology in their final report to help key decision makers determine whether a breach was significant. They included a tabular checklist of the various financial services laws and industry codes that the licensee was required to comply with. It also includes the significance test specified in s912D(1)(b). This document is completed by the licensee's business unit, compliance function or audit function and it has the advantage of requiring a structured approach to thinking about *what* may have been breached and the *impacts* that breach has.

201 While a structured approach and the use of a checklist can help an AFS licensee achieve compliance, our view is that regulatory compliance is not achieved solely by a checklist approach to the law:

> Policies and procedures, the ones you write and review, only provide a framework for compliance. They cannot ensure compliance. It is a positive business culture that converts these arrangements into true regulatory compliance.
>
> Note: See *Improving business through compliance: A regulator's perspective*, speech by ASIC Commissioner, Cathie Armour, General Counsel Summit, Sydney, 4 May 2016.

Reporting a significant breach to ASIC

202 As already mentioned, s912D(1B) requires the AFS licensee to lodge a report to ASIC as soon as practicable and, in any case, within 10 business days after becoming aware of the breach or likely breach.

203 In the review, AFS licensees explained their understanding of when awareness occurs for the purposes of the 10-business day reporting requirement. AFS licensees considered that awareness was not triggered by those responsible for investigating the incident, but instead only occurs once the key decision makers have considered the investigations' findings.

> Note: Due to the legal requirement, we measured timeframes for reporting by business days. Delays displayed in business days are shorter than the total number of calendar days, as reflected in other sections of this report.

204 The findings of investigations are commonly required to be escalated to key decision makers in the form of a written statement that contains the findings and/or recommendations resulting from the AFS licensee's investigation.

> Note: In this report, we refer to these written findings as the AFS licensee's 'final report'.

205 Typically, the key decision makers or key decision-making group is drawn from compliance, operational risk, legal, and/or the business unit affected by the breach. Sometimes it comprises a single individual—for example, the CEO or the managing director of the business or product line. In any case, the key decision makers largely rely on the significance test to make their decision on the final report.

206 AFS licensees may provide either an interim report (if the investigation is ongoing) or a final report (if the investigation has concluded) to the key decision makers, who then need time to consider the report.

207 Only after the key decision makers had determined that there was a reportable significant breach did the AFS licensees consider they had become aware of the breach and triggered the reporting obligation.

208 Most significant breaches were swiftly reported to ASIC after the end of an AFS licensees' investigation. We found reviewed financial groups took an average of two business days (median: 10 business days) to report to ASIC.

209 Table 13 shows the distribution of AFS licensees' lodgement of breach reports, relative to the end of an investigation.

Table 13: Reporting to ASIC, by business days

Timing of breach report to ASIC	Number of breaches
During the investigation	58
0–10 business days after the investigation	284
11–20 business days after the investigation	228
More than 20 business days after the investigation	73

Note 1: This table is based on 643 significant breaches (out of 715) with applicable data.

Note 2: Business days calculations does not currently include state-based holidays.

Reporting during an investigation

210 We found that 58 significant breaches were reported to ASIC during the AFS licensees' investigation into whether a significant breach had occurred.

211 This is in line with previous ASIC guidance that AFS licensees should not wait until after the following events have happened to satisfy itself that the breach or likely breach is significant:

(a) the licensee's board of directors or legal advisers has considered that breach or likely breach;

(b) the licensee has taken steps to rectify the breach. An AFS licensee should consider what it may need to do to rectify a breach but should not wait until then to report to ASIC. Efforts to rectify a breach, even if well intentioned,

could take such a long time that they can compromise our ability to investigate and take action once the incident is finally reported; and

(c) in the case of a likely breach, the breach has in fact occurred.

Note: See RG 78.29 and *Why breach reporting is important*, speech by ASIC Deputy Chairman, Peter Kell, Risk Management Association Australia Chief Risk Officers Forum, 16 September 2014.

212 AFS licensees should ensure they are monitoring their investigations to be able to escalate and consider the significance of a breach at the earliest opportunity to do so.

213 Even after reporting to ASIC, where investigations are prolonged, AFS licensees need to ensure the investigation is efficient and not lose sight of the objective to fix the breach in a timely manner. This extends to any possible rectification for consumers (i.e. remediation).

Reporting after an investigation

214 Generally, AFS licensees swiftly report breaches to ASIC once an investigation has ended. The average length of this timeframe was two business days (median: 10 business days). At this time, AFS licensees should have all the information they need to determine whether a significant breach has occurred and is reportable.

215 In at least 284 instances, AFS licensees were able to escalate the findings of an investigation to key decision makers for determination, and report to ASIC, all within 10 business days: see Table 13.

216 AFS licensees made 301 significant breach reports to ASIC more than 10 business days after the end of the licensee's investigation.

217 We expect that industry will have agile and responsive internal breach escalation and decision-making mechanisms to achieve better and more consistent compliance with the 10-business day reporting requirement.

218 We found that delays occurred either due to time taken to:

(a) escalate information to key decision makers (to form awareness, as explained and described by AFS licensees); or

(b) report to ASIC after forming awareness.

219 Table 14 shows the distribution of AFS licensees' lodgement of breach reports, relative to the licensees' awareness.

Table 14: Significant breaches reported to ASIC after awareness

Timing of breach report to ASIC	Number of breaches
0–10 business days after awareness	170

Timing of breach report to ASIC	Number of breaches
More than 10 business days after awareness	110
No record of awareness provided	21

Note 1: This table is based on 301 significant breaches (out of 715) with applicable data.

Note 2: Business days calculations does not currently include state-based holidays.

Time taken to escalate information to key decision makers

220 In 170 significant breaches we found breach reports to ASIC were delayed by the additional time taken to escalate the investigation's findings (e.g. final report) to key decision makers. In these instances, it took an average of seven business days (median: three business days) to escalate to key decision makers.

221 In five instances it took more than 100 days to escalate information to key decision makers from the end of the AFS licensee's investigation.

222 We recognise that a short period may be necessary to provide the findings of an investigation, and recommendations, to key decision makers; however, lengthy delays should not be tolerated.

223 We were pleased to find, in at least 71 instances, that AFS licensees were able to escalate the investigation's findings to key decision makers on the same day as the end of the investigation.

224 Monitoring and benchmarking are necessary to appropriately manage this aspect of the process. AFS licensees should monitor the length of time it takes for key decision makers to receive the information necessary to make their determination as part of assessing their overall speed in reporting to ASIC.

Case study 16: Key decision makers who determine significance

An AFS licensee had a three-step process that delayed awareness until the chief-executive level before reporting a breach to ASIC. After the compliance area submits an interim or final report:

- the matter is considered at a meeting of the licensee's breach committee, which makes a recommendation;
- the recommendation is put to an email vote via a 'circular resolution'. Each committee member is required to vote on whether they agree or disagree with the recommendation; and
- if the vote passes, an email is sent to the licensee's CEO seeking confirmation that they are comfortable to confirm the recommendation.

225 Whatever process AFS licensees adopt, they must ensure that breaches are escalated promptly to key decision makers. Unreasonable delays in

escalating to key decision makers are unacceptable as they unnecessarily delay forming awareness by the licensee and, in turn, reporting to ASIC.

Time taken to report to ASIC after awareness

226 All the reviewed financial groups' policies reflected the need to report to ASIC within 10 business days of forming awareness.

227 Based on the reviewed financial groups' explanation of when awareness occurs, and previously referred to legal advice (see paragraph 53), we sought the minutes or communications to show awareness of only those significant breaches reported to ASIC more than 10 business days after the end of AFS licensees' investigations.

228 We found one in seven (110) significant breaches reported to ASIC did not appear to comply with the requirement to provide the breach report within 10 business days of the AFS licensee becoming aware of the significant breach.

229 The majority of these (84) were attributable to NAB. A failure to report to ASIC within 10 business days from awareness is a criminal offence: see s1311(1).

230 Between 2014 and 2017, only four of these 110 significant breaches were subject to an additional breach report from the AFS licensee based on failing to report to ASIC within the required 10 business days. As set out in RG 78.29, a failure to meet this requirement is also a significant breach.

231 In five instances, the breach was reported to ASIC more than 40 days after the AFS licensee became aware of the significant breach.

232 However, the number of late reports identified, in addition to over 100 reports received on the tenth business day, is symptomatic of processes focused on the default period of 'within 10 business days', rather than 'as soon as practicable'.

Unable to produce a record

233 There were 21 instances where AFS licensees could not produce records of key decision makers (no record of awareness provided). All were from 2014 and 2015, often from before an update to the reviewed financial groups' processes.

234 The failure to produce these records is indicative of some of the poorer record keeping and lack of management of the process that existed during the relevant period. However, we do take some comfort from the ability of the reviewed financial groups to produce more recent records.

235 One major financial group advised that in some cases—for example, where the decision to report was made verbally and not subsequently documented—there is no record to produce. This is consistent with some of that major financial groups' documentation that included email records referring to previous discussions:

> As per my verbal confirmation last week […] I confirm I agree with the advice that the incident is reportable.

236 The major financial group does not appear to have an internal requirement to record decisions on reportability, at least not until after the fact. Such approach means, when required to, AFS licensees may have difficulty demonstrating compliance with their reporting obligation, as well as their general licence obligations under s912A(1).

Findings of no significant breach

237 An AFS licensee may conclude that a significant breach has not occurred. This determination may be made when the licensee initially assesses the incident or may require a full investigation.

238 Those incidents that AFS licensees have determined not to have breached any compliance requirement can be assessed purely from a risk and consumer experience perspective.

239 Those incidents that AFS licensees have determined to be a breach of regulatory requirements, but not significant, are then rectified with processes consistent with key stages 4–7: see Section D.

240 This review collected data on the number of incidents that were assessed by AFS licensees and determined as either:

(a) a breach, but not a significant breach; or

(b) not significant but with no final determination as to whether a breach had occurred.

241 The combined total of these two types of determinations was 9,625 (compared to 715 incidents found to be significant breaches between 2014 and 2017).

242 Of these 9,625 incidents, some AFS licensees chose to submit voluntary reports to ASIC. Voluntary reports are often referred to by AFS licensees as 'good governance notifications' and are explicitly identified as non-reportable. Nonetheless, AFS licensees considered it appropriate to alert ASIC to the substance of the report despite finding that no significant breach had occurred at that point in time.

243 These voluntary reports can provide ASIC with many of the same intelligence benefits as a formal breach report. This is more likely to be the case when the information contained in the voluntary report is equivalent to

that expected in the breach report. Voluntary reports can also be evidence of AFS licensees' willingness to have an open and transparent engagement with ASIC. Historically, ASIC has not received many voluntary reports from AFS licensees.

> Note: ASIC received 93 voluntary reports during the 2017 calendar year for all AFS licensees—this data is not limited to those licensees within this review.

244 However, we identified the subjectivity of the significance test led to an inconsistent approach by AFS licensees to voluntary reports. This may also suggest that it affected some determinations, unreported to ASIC, by licensees about whether a significant breach had occurred.

Case study 17: Voluntary report of a systemic issue

An AFS licensee provided a voluntary report to ASIC that they had failed to appropriately advise 2,500 consumers to changes in their term deposit accounts. The resulting remediation is estimated to require $1.4 million. However, despite these numbers the licensee did not consider the breach significant, partly because the number of consumers affected only made up 0.2% of consumers in the product.

Case study 18: Voluntary report of fees for no service

An AFS licensee provided a voluntary report to ASIC that nearly 300 consumers had been charged fees for services they didn't receive, requiring approximately $180,000 in remediation.

The rationale for the matter not being significant included that:

- the breaches had no impact on the licensee's ability to provide financial services covered by their licence; and
- there was only a small number of consumers and amount of money involved.

245 Other AFS licensees have reported incidents similar to these case studies as significant breaches. The objective significance test proposed by the ASIC Enforcement Review will address this discrepancy.

246 Voluntary reports are not an alternative to complying with the breach reporting obligation. If a matter is determined to be a significant breach, if a previous voluntary report has been submitted, a breach report must still be lodged. We were pleased to find 74 voluntary reports that were subsequently reported to ASIC as significant breaches.

247 AFS licensees may reassess initial findings and later determine a breach to be significant and reportable due to:

(a) new information being identified;

(b) consumer remediation being larger than predicted; and

(c) the outcome of legal proceedings.

248 However, 20 of the 74 voluntary reports were received after the AFS licensee had concluded its investigation. After engagement with ASIC about these voluntary reports, the AFS licensees submitted breach reports with no apparent additional information available that may have influenced the decision to lodge a voluntary report as opposed to a significant breach report.

249 It is important to remember that even if an AFS licensee assesses a breach as not being significant from the licensee's perspective, the detriment (financial or otherwise) caused to consumers may be very real, independent of how that licensee classifies the breach.

Content of breach report and breach register

250 Generally, the reviewed financial groups adopted a policy of updating their breach registers after lodging a breach report with ASIC.

251 We observed numerous instances where key pieces of information were not included, as we would expect, in the breach report. There was no adequate explanation for their absence. This is explicable when investigations are continuing, but unacceptable when the information is available.

252 AFS licensees should ensure this information is available. If the information is unavailable at the time of lodging, they should explain what steps are being undertaken to obtain the information and include an estimate of when that additional information will be provided.

> Note: Proposed law reform means ASIC may have the means to prescribe the content required in a breach report.

253 All the reviewed financial groups maintain a breach register, as recommended in RG 78, even though there is no obligation on AFS licensees to do so. However, the extent of information contained in those breach registers varied considerably between the reviewed financial groups, and between AFS licensees within the groups.

254 We observed the following suboptimal practices in the breach registers of the reviewed financial groups, which could impede identification of systemic issues:

(a) separate registers for different business units on the same AFS licence;

(b) separate registers for each year;

(c) no master register for all the AFS licensees within a reviewed financial group;

(d) registers that only recorded significant breaches; and

(e) not updating the information in the breach register beyond the date of the breach report to ASIC. As a result, breach registers did not have complete, accurate or, often, any information on the actions undertaken

> by AFS licensees beyond lodging the breach report to ASIC—for example, there was often no information on rectification measures, including consumer remediation.

255 As a side effect, some reviewed financial groups found responding to ASIC's requests for data, in the context of this review, to be challenging and resource intensive.

256 A breach register should be used to record actions in identifying, reporting and resolving breaches. In our view, based on the evidence obtained, existing breach registers are not being fully realised. They have the potential to form part of a searchable database to identify systemic issues or emerging risks. Any tool designed for this purpose, standalone or otherwise, should ensure the information is able to be automatically or readily extractable, and allow users to update the information as required.

257 All breach reports, and breach registers, should attempt to contain the information that is recommended by ASIC's regulatory guidance: see Table 5 in RG 78.

Opportunities for improvement

Monitoring and benchmarking

258 Effective breach reporting processes should be current and establish a clear set of rules or expectations that staff can adhere to. This is consistent with broader obligations outlined in RG 104. RG 104.26 states:

> You also need to monitor and report on your compliance, including reporting relevant breaches to ASIC under s912D. We expect that you will keep records of your monitoring and reporting, including records of reports on compliance and breach notifications.

259 AFS licensees would benefit from regularly monitoring, benchmarking and internally reporting on:

(a) the number of incidents assessed and their outcomes;

(b) any trends; and

(c) timeliness, including for ongoing investigations and remediation.

260 The reviewed financial groups were not holistically monitoring their processes. As such, they were largely unaware of the findings we detailed for them and subsequently contained in this report.

261 The collation of data, in the context of this review, has created the ability to benchmark reviewed financial groups against external performance, where previously they may have only been measuring against their own performance.

262 Further, as part of adequate monitoring, AFS licensees should ensure a regular review is conducted of their breach reporting processes. Besides some one-off reviews, often external, we identified little evidence that reviewed financial groups regularly monitored the operation of the breach reporting process. Their focus was invariably on the underlying breach that was being assessed as part of the process. The timing of such reviews will differ depending on the licensee. The outcomes of these reviews should be escalated by senior management to the board to ensure that they are aware of the licensee's overall performance.

263 Throughout an investigation, it was common for 'progress reports' to be prepared by AFS licensees to provide updates to senior management. We found some progress reports to be more detailed than others.

Case study 19: Preparing progress reports of investigations

An AFS licensee categorises the key actions recommended in their progress reports into two broad categories: 'action taken' and 'action to be taken'.

The group also specifies 'target' and 'actual' completion dates for each action item and records the completion rate (i.e. percentage) of all action items as at the date of the progress report.

264 We found some progress reports that included the staff or management responsible for the completion of the action item as an 'owner'. We were pleased to observe this level of accountability. Effective use of well-developed and well-detailed progress reports will help AFS licensees better manage their investigations and improve their efficiency.

Managing delays

265 We have received breach reports concerning conduct that occurred some years earlier, after lengthy investigations to conclude that a breach was significant.

266 As noted, one in four investigations took longer than 168 days before reporting to ASIC. In the extreme, we identified four investigations that exceeded 1,000 days before reporting to ASIC.

267 Delays in any well-designed and documented process can occur. However, it is important that AFS licensees have appropriate and efficient processes for reporting, and monitoring those processes, to ensure delays are managed and escalated where necessary.

268 It is also important that AFS licensees challenge and raise concerns about lengthy investigations, rather than adopting an accepting attitude. Even if such challenge does not result in faster response times, the licensee would have assurance that the investigation is not being unduly delayed. Further,

the board and executives should be accountable for tracking and reporting response timeframes.

269 In addition, if third parties—for example, consumers or former employees—hold information needed for the investigation to proceed, then appropriate efforts should be made to obtain that information. If key information is not obtained, and that prevents a clear determination of an investigation, then that outcome should be recorded.

270 We also found that some of the reviewed financial groups need to better monitor the final stages of reporting to ASIC, including monitoring the length of time taken to escalate information to key decision makers and compliance with the reporting requirement to ASIC after forming awareness.

271 We would be concerned by any investigations that were unnecessarily prolonged as a means 'of mitigating or pre-empting enforcement outcomes by seeking to avoid having to negotiate an approach with ASIC while under the spectre of enforcement action.'

> Note: See ASIC Enforcement Review, *Position and Consultation Paper 1: Self-reporting of contraventions by financial services and credit licensees*, April 2017, at paragraph 46.

272 We recommend a process that escalates oversight of investigations once an investigation has been ongoing for a set period. That oversight should enable:

(a) an understanding of the investigation to date;

(b) reasons for any current delays, if applicable;

(c) appropriate management of the investigation moving forward; and

(d) consideration as to significance of the breach.

Processes and systems

273 We found that 36% of significant breaches (or 257 out of 715) were, at least in part, caused by systems issues, and 65% (or 466 out of 715) were, at least in part, caused by process issues.

> Note: Causes are not mutually exclusive; a breach may have multiple root causes.

274 In conjunction with the data, we are concerned by the inability of many of the reviewed financial groups' systems to provide automatic and consistent information about how often a breach had affected a consumer.

275 We observed that, to access the information required for an investigation, all too often AFS licensees needed to manually calculate the extent of the breach. Further, for the purposes of determining significance and conducting remediation, licensees often needed to perform intensive and time-

consuming operations—for example, entire account reconstructions per affected consumer for the duration of the significant breach.

276 Another example that we identified were investigations into breaches relating to financial advice, which also involved a high number of manual reviews. This is due to AFS licensees having to make a qualitative assessment of the advice that was provided or reconcile the documented advice with allegations of alternate verbal advice.

277 Unsurprisingly, the number of systems, products and consumers is a relevant factor in the reviewed financial groups' ability to conduct a timely investigation. It also affects the quality and completeness of the information received in the breach reports.

278 As technology and systems improve there is an opportunity to make these processes as automated as possible. This requires AFS licensees to consider what information they would need if a problem occurs. Previous breaches and the information that would have helped with rectification and remediation would be a reasonable starting point for the reviewed financial groups. This is one practical example where previous breaches should be used as a learning opportunity.

Record keeping

279 As noted, maintaining records, particularly of key decision-making such as the significance and reportability of a breach, is important to ensure AFS licensees can demonstrate compliance with their reporting obligation.

280 Further, accurate and comprehensive record keeping, within compliance systems, will help AFS licensees to comply with this requirement.

Learning from a significant breach

281 We found AFS licensees were generally good at identifying the root cause of a significant breach and explaining the root cause to the business unit directly affected. This is an important element of the licensee's ability to respond swiftly, fix the root cause, and reduce or remove the risk of further or similar breaches.

282 Our review found some reviewed financial groups were less consistent in considering and sharing the broader learnings from their investigation with other business units within the group.

283 Sharing information more broadly is important because it allows other parts of the business, or other AFS licensees within the group, to use that information to identify or prevent similar breaches occurring in their business.

284 This is further explored in Section E.

Proactive approach to breach reporting

285 We observed that the process of identifying breaches and breach reporting is generally reactive.

286 For industry to meet the challenge to capture, filter and analyse incidents, breach reporting processes should be both reactive and proactive in dealing with risks. If the process is only reactive, matters will only be identified once they have clearly emerged or reputational consequences begin to develop.

287 A proactive approach will better enable AFS licensees to identify risks in people, processes and systems to avoid breaches in the first instance. It may also enable AFS licensees to identify breaches before they become significant. Being proactive may help reduce the overall number of breaches and significant breaches that occur.

288 In this review, we have tracked the lifecycle of significant breaches reported by reviewed financial groups between 2014 and 2017, effectively from beginning to end. The use of similar tracking by AFS licensees will greatly assist the proactive efforts to meet their obligations, reduce risk, and achieve better outcomes for consumers. A fair, consistent and transparent process can also foster a sound learning environment that values compliance.

D Breach rectification process

Key points

This section sets out the key stages of the breach rectification process and opportunities for improvement:

- key stage 4—first communication with consumers;
- key stage 5—first payments to consumers;
- key stage 6—first process and/or system change; and
- key stage 7—first consequence management for staff and management.

We note that these stages may not apply to each significant breach.

Significant breaches can undermine trust and confidence in the financial system and may result in significant consumer losses.

AFS licensees did not always have robust remediation processes in place to ensure consumers affected by significant breaches were remediated in an efficient and timely way.

Rectification stages

289 Table 15 sets out the key stages of the rectification process, which may not be applicable to each significant breach, and where we have discussed them further in this section.

Table 15: Key stages of the rectification process

Key stage	Description	Further discussion
4 Communication with consumers	The length of time between the end of the investigation into whether a significant breach has occurred and the first communication with affected consumers.	Paragraphs 304–329
5 Payments to consumers	The length of time between the end of the investigation into whether a significant breach has occurred, the first payment to affected consumers, and the last payment to affected consumers.	Paragraphs 331–383
6 Process and/or system change	The length of time between the end of the investigation into whether a significant breach has occurred and the first process change, as well as first system change.	Paragraphs 384–409
7 Accountability	The length of time between the end of the investigation into whether a significant breach has occurred and the first application of consequence management for staff, as well as for management.	Paragraphs 410–451

290 We have calculated AFS licensees' responsiveness using the time it took them for each key stage, starting from the end of their investigation into the significant breach. While a licensee might make further findings after this time, generally it will have already gathered relevant information about the cause, impact, and intended rectification process for the significant breach. At this point, if not sooner, the licensee should be able to commence rectification or implement steps to begin rectification.

> Note: One major financial group, ANZ, advised that, in some instances, investigations may have continued beyond the relevant dates provided as the end of their investigation into the significant breach, to identify the full extent of consumers affected and their loss. As a result, if ANZ had been able to provide this data, some of the figures for key stages 4–7 may have been reduced.

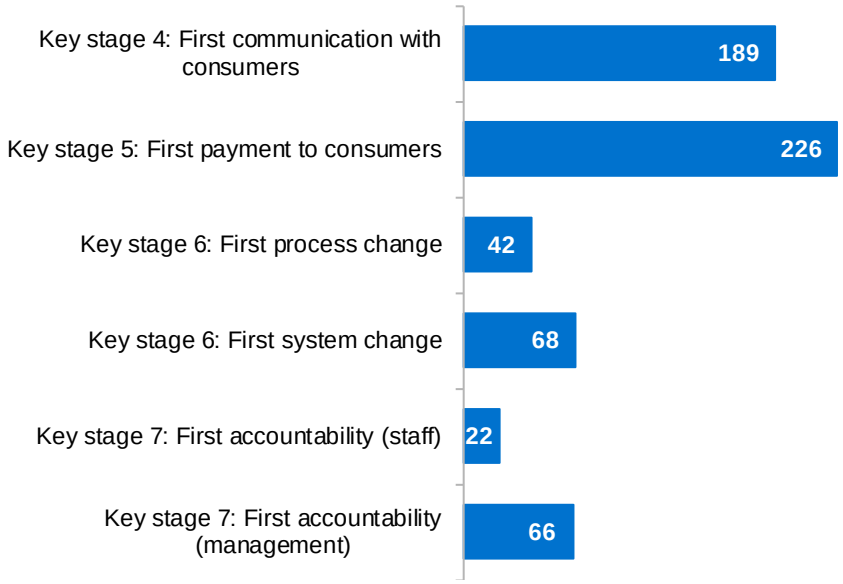
291 Based on our review, the investigations conducted by AFS licensees usually identified the steps required to implement rectification of the significant breach. Generally, this involved identifying the extent of impact of the breach, including the pool of consumers affected and the financial impact.

292 Where breach reports were lodged before an investigation was completed, AFS licensees continued to investigate further to identify the full extent of the rectification and remediation required.

293 In discussing the rectification stages in this section, we examine AFS licensees' responsiveness. Depending on the significant breach, a licensee may not need to undertake every rectification stage. For example, a significant breach without consumer financial loss will not require the licensee to make payments to consumers.

294 Figure 5 shows how quickly AFS licensees can start to implement the required rectification of a significant breach, from the end of their investigation. The breakdown between major financial groups and other financial groups is explored in the relevant key stage section of this report.

Figure 5: Average time taken for each rectification stage of a significant breach



Note 1: This figure is based on available data. For more information on each stage, see the relevant figures in our discussion of the key stages in this section. Average calculations have included both positive and negative metrics.

Note 2: See Table 34 in Appendix 2 for the data shown in this figure (accessible version).

295 We have excluded instances where any of the rectification stages were undertaken by the AFS licensee before the start of its investigation into the significant breach. Since the first action occurred before the investigation, we considered it was unrelated to the investigation, the findings of the investigation, and the licensee's responsiveness to these findings.

296 Further, the circumstances in which an AFS licensee determines that it needs to either communicate with a consumer, make payments to a consumer, implement a form of rectification (such as a process or system change), or carry out some form of consequence management, should be a red flag for the licensee to at least consider whether the incident (or however classified) warrants an investigation.

Breach rectification policies and procedures

297 Breach rectification is an important part of the breach management process. Breach reporting is not limited to a description of the issue and how it happened but encompasses how the AFS licensee intends to fix it. When we examined the reviewed financial groups' rectification processes and remediation policies, we considered them in the context of their responsiveness to resolving a significant breach.

298 From the moment a breach or potential breach is identified, AFS licensees must move swiftly to remedy the breach. This may include short-term temporary measures and permanent fixes to prevent a recurrence of the

breach. Some AFS licensees capture these collective measures in a formal rectification plan.

299 All breaches need to be rectified. Breaches found to be non-significant in isolation may result in systemic issues in the future if left unresolved or are ineffectively rectified (i.e. expecting a short-term measure to be sustainable).

300 Timely and effective rectification of breaches is crucial to ensuring that harms to consumers are minimised and remediated. The remediation process itself should ensure all affected consumers are restored to the position they would have held but for the breach.

301 In some instances, it may be appropriate for AFS licensees to complete a full investigation into the breach before commencing rectification. For example, an investigation may reveal a need to take complex and extensive steps to upgrade systems that affect broader areas of the business. However, AFS licensees should also consider a tiered approach to rectification, where appropriate, to start as soon as possible.

302 Generally, significant breaches that incurred financial losses to consumers involved outward-looking rectification measures, including:

(a) communicating with affected consumers; and

(b) providing remediation to affected consumers.

Note: This is not always the case. We found instances where financially affected consumers were not subject to such communication and some subsets of consumers were not subject to remediation.

303 Depending on the root cause or causes of the breach, inward-looking rectification measures may have also been necessary, including:

(a) changes to compliance measures, such as processes;

(b) changes to systems;

(c) changes to financial products offered, including changes to product features or disclosure documents, or withdrawal of a product or products within a package;

(d) communicating with staff;

(e) staff training, including training to reinforce regulatory requirements and internal policies and procedures; and

(f) staff consequence management.

Note: Such inward-looking rectification measures may be applicable to both the AFS licensee and more broadly the reviewed financial group.

Key stage 4: Communication with consumers

The length of time between the end of the investigation into whether a significant breach has occurred and the first communication with affected consumers.

In too many instances it takes too long to communicate with consumers affected by a significant breach. The reviewed financial groups took an average of 189 days (median: 143 days) from the end of their investigation to the first communication with consumers affected by the breach.

Excessive delays in communicating with consumers after an investigation are unacceptable.

AFS licensees should consider all reasonable methods of communication, and use multiple methods where appropriate, to establish contact with consumers affected by a significant breach.

304 The focus of our review of this key stage is how quickly AFS licensees were able to respond to the significant breach and communicate with affected consumers, relative to the end of the licensee's investigation.

305 Consumers may not have been directly financially impacted by the significant breach (e.g. where the breach involved a failure to provide disclosure documents); however, it still may be necessary to communicate with them to notify them of the breach and rectify the breach.

Time taken to communicate with consumers

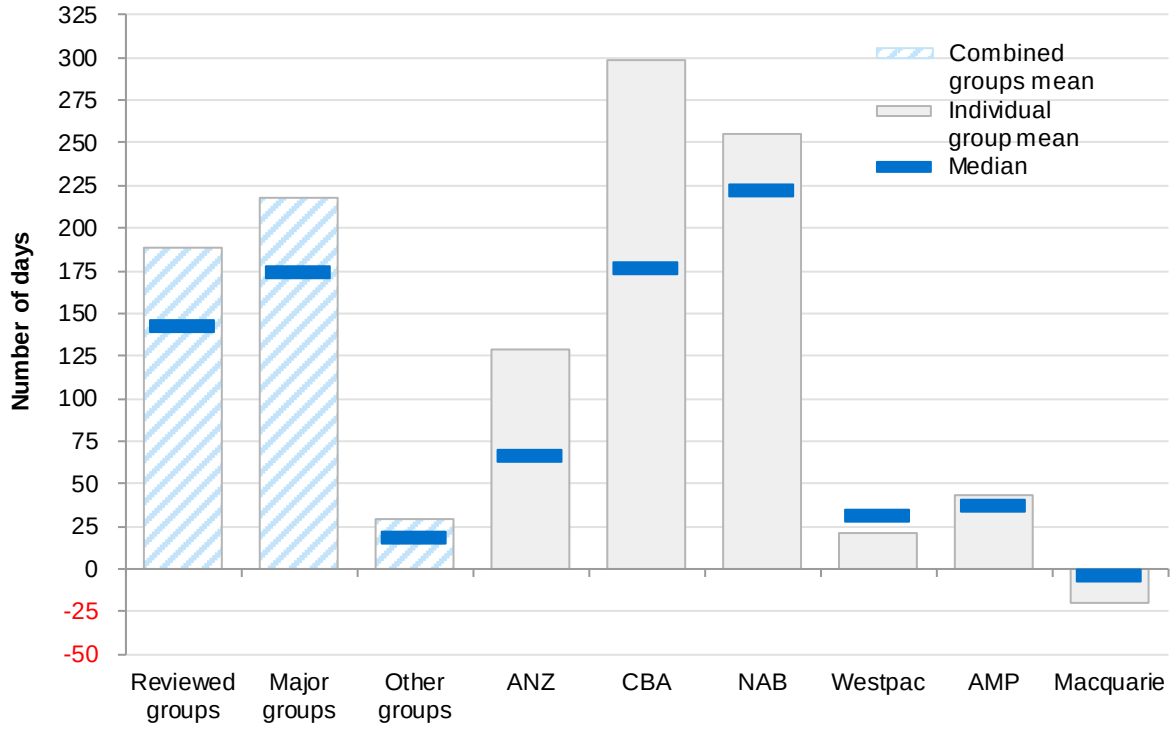
306 Based on the data, communication with consumers affected by a significant breach appears to be given a lower priority by AFS licensees than implementing a process or system change.

307 AFS licensees communicated, in some form, with consumers affected by 364 of the 715 significant breaches.

> Note: 'Communication' may be made by letter, telephone, text message, email, personal meeting, an AFS licensee's generic online message or public statement, updated disclosure, or product-related account statement or periodic statement.

308 Figure 6 sets out the average number of days between the end of the investigation and the first communication to consumers (key stage 4).

Figure 6: Average number of days for key stage 4, by reviewed financial groups



Note 1: This figure is based on 321 significant breaches (out of 364 that involved communication with consumers) that had applicable data. It does not separately display individual groups that had available data for 10 or fewer significant breaches.

Note 2: See Table 35 for the data shown in this figure (accessible version).

309 The major financial groups took an average of 218 days (median: 175 days), however, Westpac's data indicates performance consistent with the other financial groups. The other financial groups took an average of just 29 days (median: 19 days) to first communicate with affected consumers.

310 In 43 instances, the first communication with consumers affected by a significant breach occurred before AFS licensees had started their investigation. While it is important to quickly communicate with consumers about their individual circumstances, AFS licensees should be alert to the possibility that these types of communications may indicate a red flag and the need to investigate. AFS licensees should not delay the start of an investigation into whether an incident is a significant breach while they are taking steps to rectify the incident. Otherwise it is possible that systemic risks are missed while dealing with apparently isolated incidents.

311 The data demonstrates the variation in AFS licensees' responsiveness and possible scope for improvement.

> Note: Our review did not conduct a case-by-case analysis of each significant breach and the content of those communications.

312 The data also demonstrates that some AFS licensees start communicating with consumers before the end of their investigation. In 65 instances, the first communication with consumers affected by a significant breach

occurred during the AFS licensee's investigation. We were pleased with this finding and encourage this practice. In 256 instances, the first communication occurred after the AFS licensee's investigation. The data highlights the possibility for other AFS licensees to improve in this area.

313 Excessive delays in communicating with consumers after an investigation are unacceptable. After an investigation, an AFS licensee should be able to engage in transparent and clear communication with consumers about the full extent of the breach as it relates to those consumers. The licensee should have determined, with some level of certainty, a preferred method and content of such communication (at least in draft form, if not approved).

Case study 20: Delays in communicating with consumers

An AFS licensee took about three years to inform affected consumers that their financial adviser had been terminated for serious compliance failures.

The reasons for this delay appeared to be a lack of clear ownership of the rectification process, including an initial error in identifying the appropriate licensee to manage the remediation (consumer communication and payments).

The breakdown in internal process also involved delay in communicating with consumers; a draft letter was not finalised for several months.

314 Prompt and accurate communication with consumers about the occurrence of a significant breach and the measures that the AFS licensee is taking to remediate it is crucial to allay consumers' concerns. It also demonstrates a licensee's consumer-focused approach to breach rectification.

Opportunities for improvement

Engagement with the regulator

315 Of the 364 significant breaches that AFS licensees communicated with consumers about, licensees engaged with ASIC on draft communication for 79 breaches.

316 Based on the average time taken for key stage 4, it would appear there is ample opportunity to engage with the regulator in a way that does not unduly delay communication with consumers.

317 We recognise this level of engagement is not always necessary. However, where it is, it allows ASIC to have regulatory oversight of communication with consumers.

Method of communication

318 Engaging with ASIC on intended communication with consumers, and the methods to be used, will also ensure the regulator is more comfortable with the proposed approach.

319 We observed a range of methods of communication with consumers affected by a significant breach, including by way of letter (394), telephone (127), and email (118). These were the most common methods used.

320 AFS licensees are not restricted to a single method of communication. We found in 242 instances, AFS licensees used multiple methods, and in at least three instances AFS licensees attempted seven methods of communication.

321 On a case-by-case basis AFS licensees should consider using multiple methods to engage and inform consumers affected by breaches, particularly if the first attempt proves to be unsuccessful.

322 In our experience, this can assist in establishing contact with ex-customers and may help to return funds to consumers entitled to financial remediation because of a breach: see paragraphs 353–374.

Accurate messaging

323 In our view, the interaction between ASIC and an AFS licensee can lead to more complete and accurate messaging to affected consumers. This may also lead to a more efficient rectification process because of more accurate messaging the first time.

324 We observed a number of significant breaches where the clarity of the messaging benefited from engagement with ASIC.

Effective communication

325 Effective, timely and targeted communication is key to ensuring that consumers understand the need and reasons for the remediation and how it will affect them.

> Note: See Regulatory Guide 256 *Client review and remediation conducted by licensees* (RG 256) for further information.

326 Transparent and clear communications are integral to maintaining or restoring consumers' trust and confidence after experiencing some form of detriment due to a significant breach.

327 Generally, to be effective, communications with affected consumers should:

(a) acknowledge the breach;

(b) explain the issue or problem that caused the breach. If the issue or problem is complex, the explanation can be brief to not cause confusion;

(c) apologise for the breach;

(d) describe the actions the AFS licensee is taking or intending to take to rectify the issue or problem that caused the breach;

(e) describe any action consumers need to take to avoid further harm or inconvenience;

(f) detail any related key dates or timeframes within which the AFS licensee anticipates rectification will be complete; and

(g) provide contact details for consumers to seek further information if required.

328 If consumers have suffered financial loss, the AFS licensee should also:

(a) detail the amount of remediation and explain any calculations, including a breakdown of funds that include interest payments; and

(b) notify consumers about any choices available regarding those funds, and possible methods to receive such payments.

329 In instances where consumers are subject to tiered remediation, the AFS licensee should consider providing updates as the remediation progresses and advising of any adjustments to the anticipated timeframe.

Case study 21: Communicating effectively with impacted consumers

An AFS licensee used the clear subheadings in a one-page letter to consumers who were financially impacted by a breach outlining:

- Why they were communicating with the consumer (i.e. the AFS licensee owed them money)—This section provided a brief introduction to the breach and offers the consumer an apology.
- What had happened—This section provided clear and effective information on the breach.
- Other effects—This section stated the tax implications of the financial remediation.
- How and when they would be compensated—This section provided the AFS licensee's contact details and next steps.

The licensee also produced a document directed at remediation staff. This two-page document was intended to brief staff on the breach, and document various tips and frequently asked questions in response to anticipated consumer queries.

330 AFS licensees should ensure that information provided to staff is transparent, accurate and consistent with that provided to consumers.

Key stage 5: Payments to consumers

The length of time between the end of the investigation into whether a significant breach has occurred, the first payment to affected consumers, and the last payment to affected consumers.

In too many instances, the time taken to commence remediation is unacceptably long. The reviewed financial groups took an average of 226 days (median: 201 days) from the end of their investigation into the breach to the first payment to consumers affected by the breach.

We also found, in at least 21 instances, AFS licensees were not able to return all funds to consumers that were financially affected by a significant breach. In those instances, the reviewed financial groups retained those funds.

331 The focus of our review of this key stage is how quickly AFS licensees were able to respond to the significant breach and remediate affected consumers, relative to the end of the AFS licensee's investigation. We also focus on how quickly licensees were able to complete payments to consumers (i.e. first to last payments) and how long consumers may have been out of pocket.

Time taken to pay consumers

332 AFS licensees must ensure they restore consumers that are financially impacted by a breach to the position they would have held but for the breach occurring.

333 An AFS licensee that is focused on the best interests of their consumers and doing the right thing by their consumers should prioritise timely remediation—that is, putting the consumer right.

Time taken to start payments

334 Of the 715 significant breaches, 279 incurred financial loss to consumers. At the time of providing responses to ASIC, AFS licensees had started financial remediation to consumers affected by 260 of these significant breaches.

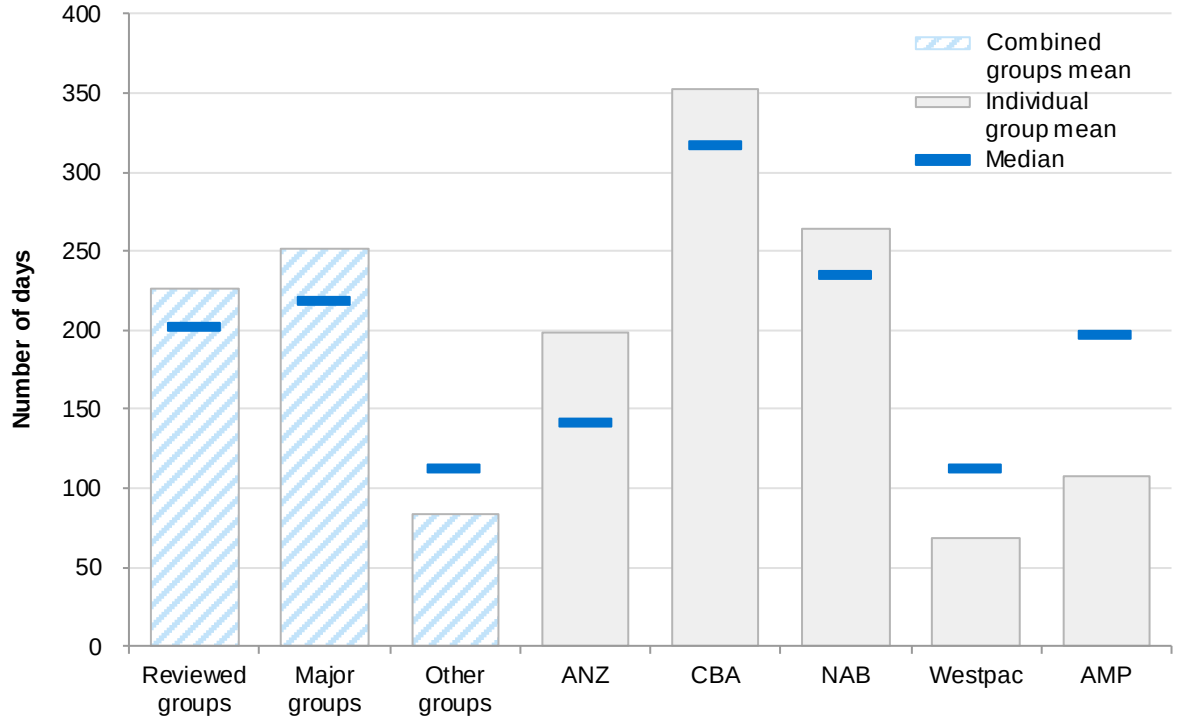
335 We expect that AFS licensees will attempt to remediate all financial losses in a timely manner.

336 It is not unusual for AFS licensees to conduct a full investigation to quantify all consumers and all payments required before starting to make payments. However, this approach commonly leads to delays in starting investigations. We found 204 instances where this occurred. However, we found 31 instances where AFS licensees started making payments before the end of their investigation.

> Note: The findings in this report are based on data provided by the reviewed financial groups during our review. Some data was updated in early 2018; however, the remediation to consumers may not have started or, if started, not yet finished at the time of the collection of the data.

337 Figure 7 sets out the average number of days between the end of the investigation and the first payment to consumers (key stage 5).

Figure 7: Average number of days for key stage 5, by the reviewed financial groups



Note 1: This figure is based on 235 significant breaches (out of 260 that involved financial remediation) that had applicable data. The standard deviation for all the reviewed financial groups is 247 calendar days. It does not separately display individual groups that had available data for 10 or fewer significant breaches.

Note 2: See Table 36 for the data shown in this figure (accessible version).

338 The major financial groups took an average of 251 days (median: 217 days) to make the first payment to consumers affected by a significant breach after the end of their investigation. However, Westpac's data indicates performance consistent with the other financial groups. The other financial groups took an average of 84 days (median: 111 days) to make the first payment to affected consumers.

339 We note, again, that AFS licensees should be in a position, by the end of their investigation, to swiftly start and then efficiently manage the remediation process. In doing so, AFS licensees should appropriately resource and prioritise the remediation of consumers.

340 In 20 instances, the first payment to consumers affected by a significant breach occurred before AFS licensees had started their investigation. In a further five instances, licensees were not able to provide useable data.

341 Both measurements (average and median) are greater than the corresponding periods for communicating with affected consumers. It is, however, common for communications to coincide with payments—AFS licensees tend to

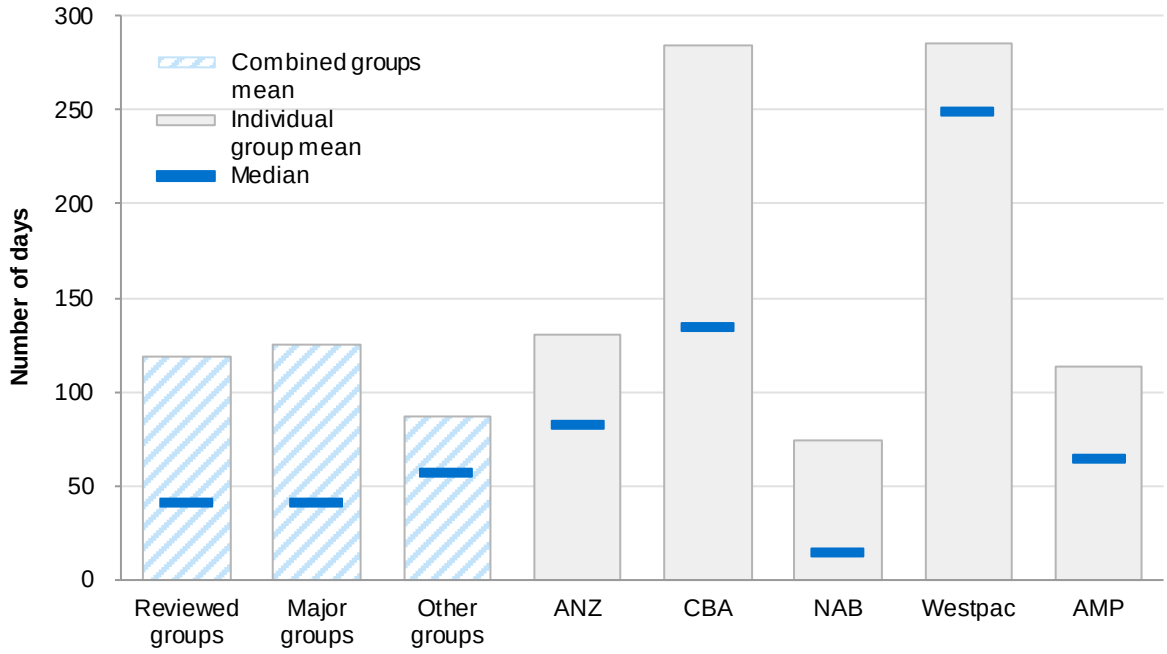
engage consumers when they are ready to conduct remediation, and there is added incentive (part convenience, part financial) for licensees to contact a consumer only once in the process.

342 The statistical measure of delay in remediation is consistent with some of ASIC's experiences with remediation. This is one of the reasons why we sought a directions power in our submissions to the ASIC Enforcement Review. We want more ability to ensure that remediation processes are appropriate and timely, and a directions power would assist with that.

Time taken to complete payments

343 For the purposes of calculating the length of remediation, we relied on reviewed financial groups' ability to provide dates for first and last payment to consumers financially affected by a significant breach: see Figure 8.

Figure 8: Average number of days between first and last payment to consumers affected, by the reviewed financial groups



Note 1: This figure is based on 218 significant breaches (out of 260 significant breaches subject to financial remediation) that had available data. The standard deviation for all the reviewed financial groups is 206 calendar days. It does not separately display individual groups that had available data for 10 or fewer significant breaches.

Note 2: See Table 37 for the data shown in this figure (accessible version).

344 Despite better internal reporting and monitoring of timeframes, AFS licensees generally seemed to accept delays in the remediation process.

345 We acknowledge that there may be valid and unavoidable reasons why a financial remediation process is prolonged. In fact, we would encourage AFS licensees to use their best endeavours and exhaust all possible means to locate and contact affected consumers, which can extend the period.

346 Further, it may be appropriate to conduct a tiered remediation if the impact on segments of consumers varies greatly and it would be best to target a large pool of affected consumers as a priority. It may also be sensible, in large-scale complex remediation, to conduct a 'pilot run' as a test case (open to consumer feedback) for a limited subset of consumers before completing the full remediation to all affected consumers.

347 All reviewed financial groups reported internally on the progress of remediation. However, some of this information was stored on alternate systems and not easily produced or reconciled to the significant breach.

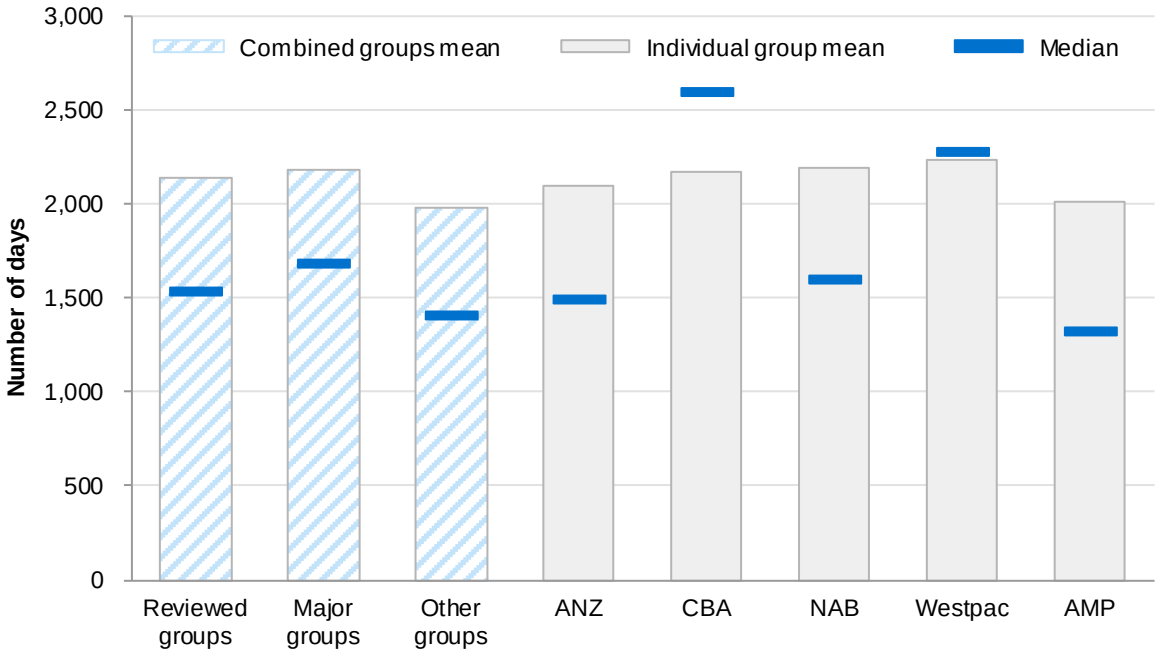
348 We did observe some monitoring of the remediation process that included a level of oversight with a clear objective to achieve the remediation as quickly as practicable. This included requiring senior approval to extend the required length of the process and further included instances of rejection of initially long estimates of additional time required.

Time consumers may be out of pocket

349 Particularly driven by current averages of time taken for key stage 1 (incident to identification), key stage 3 (investigation to breach report) and key stage 5 (investigation to payments), at least some consumers that experience losses due to a significant breach that starts today may be out of pocket until 2024: see Figure 9. This projection assumes no improvements in AFS licensees' ability to identify, investigate, and remediate breaches.

> Note: Not all consumers financially impacted will be out of pocket for the full length of time from the first instance of the incident to the first payment to consumers affected by the significant breach. Depending on the circumstances, consumers may have been impacted at varying times. Losses may have been incurred at any time from the first instance of the breach to the remediation. Full remediation may have occurred at any time from the first payment to consumers to the last payment to consumers.

Figure 9: Average number of days between the first instance of a significant breach and the first payment to consumers, by the reviewed financial groups



Note 1: This figure is based on 243 significant breaches (out of 260 that involved financial remediation) that had available data. The standard deviation for all the reviewed financial groups is 1,662 calendar days. It does not separately display individual groups that had available data for 10 or fewer significant breaches.

Note 2: See Table 38 in Appendix 2 for the data shown in this figure (accessible version).

350 While delays in remediation can, in part, be compensated by adding appropriate interest payments to the amount of remediation, any unnecessary delay is damaging for consumers. If they are aware of the issues, delay only adds to the stress for a consumer. Where they are not aware of the process, delay can make it more difficult to locate and remediate all those affected.

351 The longer the lapse of time before remediation begins, the greater the likelihood that existing customers will become ex-customers and the information on hand becomes outdated. This concern is exacerbated due to the average time it takes AFS licensees to identify and investigate a breach.

352 Excessive delays not only inconvenience affected consumers, but can also reduce their level of trust and confidence (which is already eroded by the significant breach itself).

Consumers may be out of pocket

353 We found that not only are some consumers out of pocket for too long but, in some instances, consumers are permanently disadvantaged by the impact of the significant breach.

354 Despite AFS licensees generally disbursing unreturned funds in a way that ensured that the licensees did not make a profit from the significant breach, we identified at least 21 instances where the licensee was not able to return

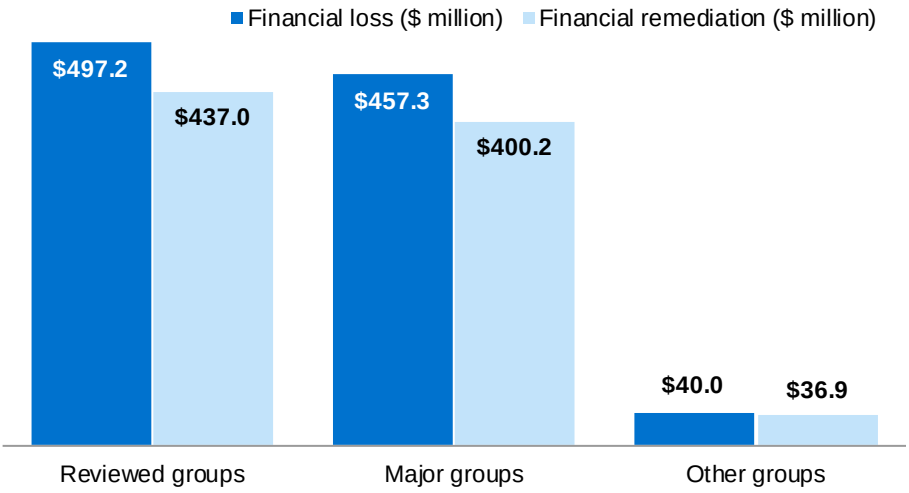
all funds to consumers financially affected by the significant breach. In those instances, the licensees or the reviewed financial groups retained those funds. Licensees have since updated their policies to ensure that funds are disbursed appropriately.

Financial loss and remediation

355 As noted, of the 715 significant breaches, 279 incurred financial loss to consumers and 260 have been subject to at least some financial remediation.

356 Figure 10 sets out the total financial loss and remediation reported as part of our review.

Figure 10: Total financial loss and remediation, by the reviewed financial groups



Note 1: This figure is based on the 279 significant breaches that stated a financial loss was incurred and the 254 significant breaches that stated that a financial remediation had occurred.

Note 2: See Table 39 in Appendix 2 for the data shown in this figure (accessible version).

357 Of the 279 significant breaches that incurred financial loss to consumers, the total financial loss is approximately $497 million. This equates to an average loss of around $1.8 million per significant breach.

358 Of the 260 significant breaches that involved financial remediation to consumers, so far the total financial remediation is approximately $437 million. This equates to an average remediation of around $1.7 million per significant breach.

359 It is no surprise, based on market share and the volume of significant breaches reported, that the major financial groups accounted for most of the financial loss and financial remediation to consumers.

360 All affected consumers should be returned to their original position, as if the breach never occurred. This requires that financial remediation should at least be equal to financial loss.

361 However, we acknowledge that there may be practical difficulties in reimbursing all adversely affected consumers. In part, this highlights the importance of a fair and efficient breach reporting process.

362 AFS licensees should be able to contact any current customer or deposit funds directly into a relevant account, where one exists. Practical difficulties may arise where the customer is no longer current and, despite making reasonable attempts, the AFS licensee is unable to locate and contact the ex-customer. The difficulties in making payments, and the likelihood of this occurring as time goes by, was noted by at least one of the reviewed financial groups:

> Paying back customers is challenging when they may no longer bank with us, have closed the impacted products, may be in collections or deceased, have changed their name or cannot be contacted.

363 There may be times where the provision of nominal amounts is outweighed by the inconvenience that may be caused to ex-customers, and AFS licensees have adopted a tiered remediation. Such an approach commonly involves setting a threshold for payments and ensuring that any residual funds below such threshold are disbursed to members or a charitable organisation: see RG 256 for further information.

364 If consumers seek remediation payments after the AFS licensee has disbursed those funds, they should receive such payments regardless of additional costs that may be incurred by the licensee.

Retained residual funds

365 In at least 21 instances where a significant breach caused financial loss to consumers, the reviewed financial groups retained some funds that could not otherwise be returned to consumers.

366 In those 21 instances, despite having losses totalling approximately $114 million, AFS licensees were able to return all but approximately $1.3 million (which they retained). These 21 instances of retained residual funds were spread across six reviewed financial groups and included 12 individual licensees.

367 We do not think that this practice of retaining residual funds is aligned with principles of ethical business conduct, nor with community expectations.

368 Residual funds (the difference between financial loss and remediation) can occur, for example, where an AFS licensee no longer holds current information about a consumer and is unable to locate and contact that person (or, potentially, a trustee or beneficiary).

369 The longer the period lapsed from the event or conduct that is the subject of the breach, the greater the risk that a current customer becomes an ex-customer and/or circumstances change.

370 Ordinarily, residual funds are not retained, but are instead disbursed by AFS licensees—payments are commonly made to unclaimed money accounts, charities or, where appropriate, other unitholders in the fund.

371 Although financially affected consumers are otherwise entitled to these funds, it may be reasonable to disburse them for other appropriate purposes if the AFS licensee has made best endeavours to remediate those consumers.

372 AFS licensees must ensure they do not make a windfall gain because of a breach. As a starting point, we expect that all financially affected consumers will be restored to the position they would have held but for the breach.

373 Clearly, any delays in both starting and finishing a consumer remediation process will add to the possibility of residual funds and financially affected consumers being out of pocket. As noted, there is a clear capacity for reviewed financial groups to improve the efficiency of consumer remediation.

374 We observed at least one instance where an AFS licensee limited the extent of data they interrogated for the purposes of scoping the remediation process. This may have resulted in the licensee failing to identify further losses and further consumers impacted by the significant breach. As a result, it is possible that the licensee has unwillingly retained funds that would otherwise have been returned to affected consumers. Equally, it is possible that the amount of retained funds identified in this review is only part of the actual amount of funds retained by reviewed financial groups.

Case study 22: Scope of remediation

An AFS licensee was only able to investigate data going back seven years. The licensee identified affected consumers and quantified losses to those consumers.

However, as these calculations were limited to that period, it is possible that those identified consumers experienced a greater financial impact, and it is possible that other consumers were affected by the breach but were not identified for the purposes of remediation.

The ability to conduct a more comprehensive investigation may have revealed, or confirmed, the full extent of the breach.

Opportunities for improvement

Consumer-centric approach

375 AFS licensees should not delay starting remediation to consumers if they have sufficient confidence that the value of remediation is accurate.

376 An AFS licensee—or, more broadly, a reviewed financial group—that is focused on the best interests of consumers, and doing the right thing by them, should prioritise timely remediation—that is, restoring consumers to the position they would have held but for the significant breach, and doing so as swiftly as possible.

377 While AFS licensees also need to ensure that the cause of the breach is addressed, they should be able to balance priorities and resource concurrent streams of remediation and rectification.

Case study 23: Changing focus of consumer remediation

An AFS licensee noted a shift in focus for consumer remediation.

In January 2018, the licensee shared learnings within a business unit affected by a significant breach. The document includes information about recent remediation projects, the root causes of breaches, and the importance of consumer remediation.

The document noted that in the past there was less focus on consumer remediation:

> it was seen as a distraction, at the expense of earning revenue, and therefore not always given the highest priority

The document also noted that the increased focus comes from many factors including a gradual internal cultural shift, an increased focus on customer experience, and doing the right thing:

> Whenever we fail to meet our obligations to our customers, we need to put it right.

Financial remediation policy

378 At the time of our review, most but not all the reviewed financial groups had a clear written policy for dealing with financial remediation, including how to deal with funds that cannot be returned to affected consumers. Some reviewed financial groups had distinct policies across AFS licensees within the reviewed financial group.

379 Those AFS licensees that did not have a financial remediation policy at the time of our review gave assurance that such a policy would be created. Where this is the case, AFS licensees must ensure such policies are communicated and related training is delivered to staff.

380 AFS licensees should have, or review to ensure they have, policies that are consistent with RG 256.

Oversight of remediation projects

381 AFS licensees should ensure that they have appropriate oversight and reporting of the rectification and remediation projects.

382 If an AFS licensee or, more broadly, the reviewed financial group has encountered multiple large-scale significant breaches, it may be necessary to engage in simultaneous rectification and remediation projects.

383 We observed that at least one reviewed financial group created a platform for greater visibility of all ongoing remediation projects to better monitor those activities and ensure it could dedicate resources appropriately.

Case study 24: Oversight of investigations

One reviewed financial group provided visibility to executive-level staff on all current consumer remediation projects. Large-scale breach remediation work streams are commonly stand-alone projects.

Such oversight was facilitated by providing documents that included timelines and key milestones, traffic-light status coding, associated risks and challenges for each project, and action to be taken.

The portfolio view allows for comparison of projects and consideration of current and future resources that will be required to complete each project.

Key stage 6: Process and/or system change

The length of time between the end of the investigation into whether a significant breach has occurred and the first process and/or system change.

Generally, AFS licensees undertook timely process and system changes in direct response to the specific significant breach.

AFS licensees must provide adequate resources to rectify the root causes of the significant breach, where required, without undue delay.

It is important that licensees consider any necessary process or system changes where this is attributable to the root cause of the significant breach. Where no changes are made despite attributing the root cause to a process or system, licensees should record the rationale for their decision.

384 The focus of our review of this key stage is how quickly AFS licensees were able to respond to the significant breach and implement a process and or system change, relative to the end of the licensee's investigation.

Time taken to change a process and or system

385 Changes to processes and systems are given priority by AFS licensees once a risk is identified.

386 To reduce the risk of recurrence of a significant breach, AFS licensees made at least one form of:

(a) process change in response to 415 breaches; and

(b) system change in response to 204 breaches.

Note: Out of 715 significant breaches. Licensees may have made both process and system changes in response to a breach.

387 As noted previously, for the purposes of our calculations, we excluded instances where the first change occurred before the start of the AFS licensee's investigation, as we considered it was unrelated to the change to address the root cause of the significant breach. This is consistent with our calculations below regarding consequence management.

388 We found 334 instances where the first process change occurred after AFS licensees had started their investigation. The reviewed financial groups took an average of 42 days (median: 25 days) to implement the first process change.

389 We found 171 instances where the first system change occurred after AFS licensees had started their investigation. The reviewed financial groups took an average of 68 days (median: 33 days) to implement the first system change.

When change occurs

390 A process or system change may occur at any time: before, during, or after the AFS licensee's investigation into the breach. In any case, AFS licensees need to act as quickly as practicable to stop the identified breach from continuing.

Table 16: Timing of first process and system change in response to a significant breach

Timing	Number of breaches with process change	Number of breaches with system change
Before the start of the investigation	81	33
During the investigation	125	61
After the end of the investigation	209	110

Note: This table is based on available data. For more information, see the relevant figures in this key stage.

Change before the start of investigation

391 We were encouraged to find that AFS licensees review their processes and systems on a periodic basis, motivated by a desire to improve them (as opposed to responding to known weaknesses).

392 We observed that these proactive changes, at times, inadvertently addressed previous weaknesses that existed but had not yet been recognised as root causes of significant breaches.

393 We also noted that these changes lead to, in some instances, the identification of the reported significant breach.

Change after the start of investigation

394 Generally, changes to processes and systems occur after the end of AFS licensees' investigations. This is largely because, at this stage, licensees are aware of weaknesses and are in the position to implement fixes.

395 We were pleased to find the following instances of the first changes occurring during an investigation:

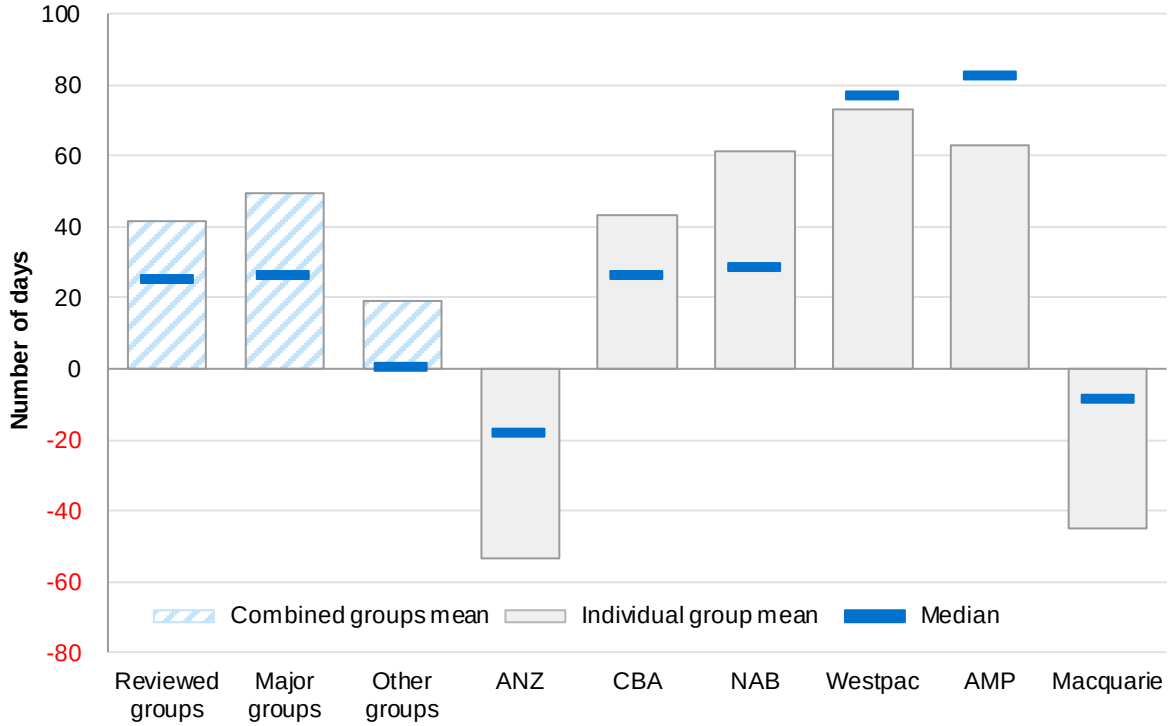
(a) 125 instances of the first process change; and

(b) 61 instances of the first system change.

396 This aligns with previous ASIC guidance that licensees should not wait until an investigation is complete, or key decision makers have considered the significance of a breach, to begin implementing fixes to stop the breach.

397 Figure 11 and Figure 12 set out the average and median time taken to make the first process and the first system changes, respectively (key stage 6).

Figure 11: Average number of days for key stage 6 (process change), by the reviewed financial groups

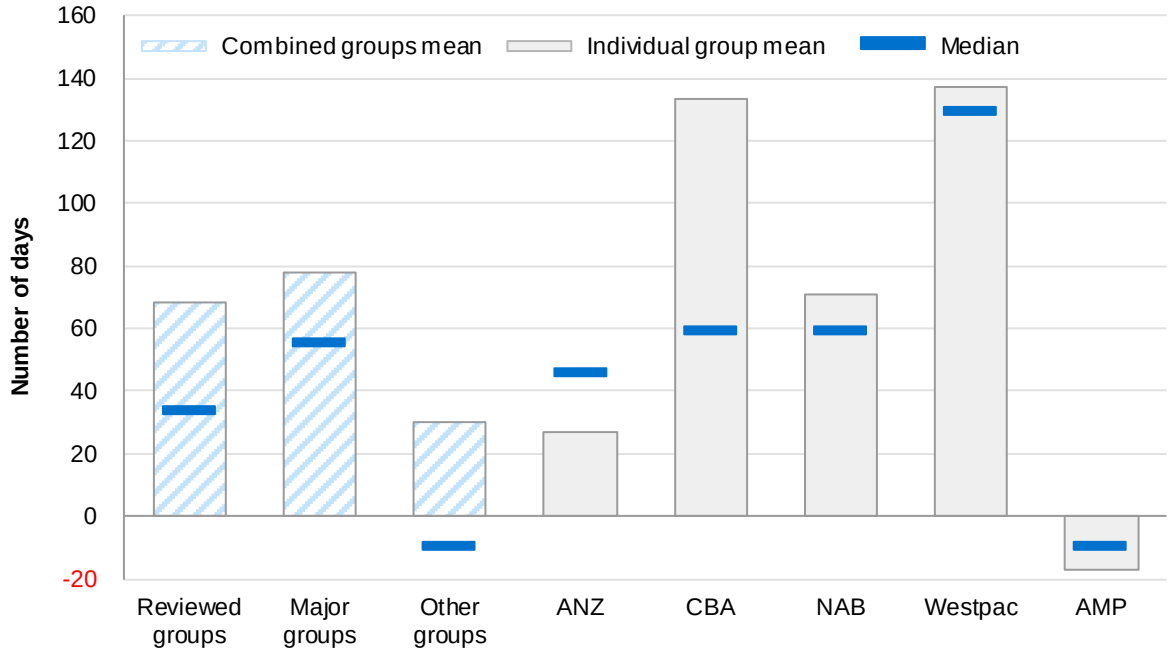


Note 1: This figure is based on 334 significant breaches (out of 415 that resulted in a process change) that had applicable data. The standard deviation for all the reviewed financial groups is 224 calendar days. It does not separately display individual groups that had available data for 10 or fewer significant breaches.

Note 2: See Table 40 in Appendix 2 for the data shown in this figure (accessible version).

398 All reviewed financial groups were swift to start to make process changes. One major financial group, ANZ, was generally more responsive than its peers, starting process change on average 53 days (median: 19 days) before the end of its investigation.

Figure 12: Average number of days for key stage 6 (system change), by the reviewed financial groups



Note 1: This figure is based on 171 significant breaches (out of 204 that resulted in a system change) that had useable data. The standard deviation for all the reviewed financial groups is 220 calendar days. It does not separately display individual groups that had available data for 10 or fewer significant breaches.

Note 2: See Table 41 in Appendix 2 for the data shown in this figure (accessible version).

399 Generally, we found it took longer for the reviewed financial groups to implement a system change than a process change.

400 Based on our experience, we consider that system changes take longer to implement because they are susceptible to AFS licensees' (or the reviewed financial groups') IT demands. This aligns with our findings.

Opportunities for improvement

Appropriate change

401 In limited instances, we observed no changes to a process or system despite the AFS licensee attributing a root cause of the significant breach to that deficiency: see Table 17.

Table 17: Number of significant breaches with and without change, by root cause

Root cause	Change made	No change made	Total number of significant breaches
Process deficiency	415	51	466
System deficiency	204	53	257

Note: This table based on 466 significant breaches where a process deficiency was listed as a root cause and 257 significant breaches where a system deficiency was listed as a root cause.

402 There can be more than one root cause—for example, a process and system deficiency may have both contributed to a significant breach occurring. We have observed instances where a change to a process or a system resolves the weakness without needing to change the other.

403 If this is not the case, it would be difficult to comprehend why the AFS licensee failed to implement a change after identifying a deficiency as a root cause of the significant breach.

404 It is important that, where no changes are made despite attributing the root cause to a process or system, that the rationale is recorded (i.e. what other steps were taken to remove or reduce the risk of recurrence of the significant breach).

Sharing learnings and reinforcing expected behaviours

405 We observed that reviewed financial groups update training once a process or system has changed. This is both appropriate and necessary to ensure future compliance with the new process or system. However, generally we did not observe that staff were made aware of why the process or system has been changed.

406 As part of this review, we did not measure training completion rates for specific training for the process or system change. However, we did measure the completion rates for training on breach reporting processes more generally. These were consistently high across reviewed financial groups.

407 If AFS licensees apply similar tracking and rigour to ensure staff are trained for other policies and procedures, then they are well placed to comply with new processes or systems when implemented.

408 Where there is no change to a product or system, specific training may be an effective way to communicate expected behaviours of staff to comply with internal procedures.

Monitoring and reporting

409 Consistent with our opportunities for improvement (see paragraph 259), AFS licensees should ensure that they have appropriate oversight and reporting of the rectification and remediation projects.

Key stage 7: Accountability

The length of time between the end of the investigation into whether a significant breach has occurred and the first application of consequence management for staff and/or management.

Accountability for mistakes made within a professional role provides a learning opportunity for the staff and management responsible, the AFS licensee, and even the broader group. Accountability is largely actioned through consequence management; although commonly framed as a 'blame' narrative, it is better viewed as:

- a learning opportunity; and
- importantly, a tool for licensees to stop a breach continuing or reoccurring by taking swift action.

Consequence management is also necessary to address misconduct, holding staff and management to account for their actions.

The time taken to first apply consequence management is inconsistent between staff and management. The reviewed financial groups took an average of 66 days (median: 23 days) to begin consequence management for *management*, and an average of 22 days (median: 23 days) to begin consequence management for *staff*, after the end of a licensee's investigation.

In only around one third of instances where an AFS licensee attributed a root cause for the significant breach to staff did the licensee record the application of consequence management to staff.

410 The focus of our investigation of this key stage is how quickly AFS licensees were able to respond to the significant breach and implement consequence management, relative to the end of the licensee's investigation.

Time taken to implement accountability

411 Our review found that consequence management is not likely to occur as a result of a significant breach.

412 According to AFS licensees, there were 296 instances where they attributed a root cause of a significant breach to staff and/or management, and only 100 instances of consequence management being applied to staff and/or management responsible for the root cause of the significant breach:

(a) 50 instances applicable to staff only;

(b) 8 instances applicable to management only; and

(c) 42 instances applicable to both.

Note: The application of consequence management to 'management' refers to it being applied to either managers, supervisors, or executives of staff responsible for the root cause of the significant breach: (collectively 'management').

413 The reviewed financial groups took an average of 22 days (median: 23 days) to begin consequence management for *staff* after the end of a licensee's investigation. In comparison, the reviewed financial groups took an average of 66 days (median: 23 days) to begin consequence management for *management* after the end of a licensee's investigation.

414 The application of consequence management is generally not transparent. The review found few instances where the AFS licensee advised unrelated staff about the application of consequence management and therefore limited the learning opportunity it presents.

What is consequence management?

415 Consequence management is the application of real and meaningful consequences for staff—and management responsible for oversight (at any higher level)—who have not followed the rules.

416 Significant breaches attributable to staff or management can result from:

(a) errors—that is, an isolated genuine mistake;

(b) negligence—that is, failure to take proper care; and

(c) intentional misconduct.

417 For those significant breaches attributable to staff, the appropriate consequence management will depend on both the cause of the breach (i.e. whether the cause of the breach can be attributed to the actions of an individual) as well as its impact and may range from warnings to more severe consequence management (such as termination).

418 We have listed a number of consequence management actions below, generally ranging in severity from low to high:

(a) warnings;

(b) additional training;

(c) closer supervision;

(d) adverse performance rating;

(e) loss of bonus in part;

(f) loss of bonus in full;

(g) change in role; and

(h) termination.

Note: This list is not exhaustive.

419 In our review, we did not test the appropriateness of the application of consequence management, merely whether it was applied and when it was applied.

420 Of the 100 instances of consequence management for those responsible for the root cause of the significant breach, the two most commonly identified types of consequence management applied by the reviewed financial groups was a reduction in bonus (47 instances) and adverse performance rating (44 instances).

Note 1: The most common type of consequence management AFS licensees advised was 'other' (105 instances).

Note 2: AFS licensees were able to advise of multiple types of consequence management per significant breach.

421 In 22 instances, staff (20) and management (2) were held accountable by reviewed financial groups and were subject to termination of employment as a result of being responsible for the root cause of the significant breach.

422 Consequence management can be also important for establishing and maintaining the AFS licensee's values and culture. For errors, we generally consider that the appropriate consequence is more likely to be at the low end of the spectrum, emphasising the learning opportunity for the individual.

423 This aligns with international research that shows that, in firms with an effective error management culture, errors are accepted as part of professional life and are discussed, addressed and learned from. There has been a growing awareness of the benefits of establishing and embedding error management practices that foster a transparent and learning environment: see Dutch Authority for the Financial Markets (AFM), *Learning from errors: Towards an error management culture—Insights based on a study in the capital markets*, October 2017.

424 For negligence and intentional misconduct, we generally consider that more severe consequence management is necessary. The possible effect on staff willingness to raise incidents needs to be balanced with the need to discourage breaches of any risk management procedures by staff through adequate consequence management: see Regulatory Guide 259 *Risk management systems of responsible entities* (RG 259) at RG 259.49.

425 Practically, AFS licensees need a sophisticated approach that deals with each case on its merits. When reviewing a breach, licensees should consider whether the cause was an error, negligence or misconduct.

426 For errors, firms need to be supportive and provide positive consequence management (e.g. individuals who identify errors should be encouraged and given positive feedback). Where staff demonstrate negligent behaviour or misconduct, a zero-tolerance approach is appropriate.

427 The key to achieving this balance, in addition to the appropriate and proportionate application of consequence management, is the concept of 'accountability'. This concept was also a stated value of the reviewed financial groups.

428 ASIC agrees with APRA's finding as follows:

> Accountability will not resolve issues in these areas but, when embedded, clear accountability will strengthen their effectiveness.
>
> Accountability is built on frameworks that provide for clarity of ownership for responsibilities and obligations, and proportionate consequences when adverse risk management, compliance and customer outcomes occur.
>
> Note: See APRA, *Prudential inquiry into the Commonwealth Bank of Australia—Final report*, May 2018, p. 57.

When consequence management occurs

429 Consequence management, like process and system change, can occur at any time—before, during, or after the AFS licensee's investigation into the breach: see Table 18. However, a swift response by the licensee is paramount to ensure the root cause of the significant breach is addressed.

Table 18: Timing of key stage 7 for staff and management

Consequence management	Before the investigation	During the investigation	After the investigation
For staff	17	32	43
For management	2	12	36

Note: This table based on 80 significant breaches (out of 100 that resulted in consequence management) that had applicable data.

Consequence management before the start of investigation

430 Consequence management that occurs before the start of an investigation should be unrelated to a reported significant breach. As such, we have excluded these from the calculations of responsiveness of the application of accountability.

431 However, the need for consequence management—in particular, more severe consequence management—could be an opportunity for an AFS licensee to proactively examine whether other rules (unrelated to the matter attracting the consequence management) have been complied with.

Consequence management after the start of investigation

Consequence management for staff

432 As noted at paragraph 412, 92 significant breaches resulted in consequence management for staff responsible for the root cause of the significant breach.

433 Of these instances, at least 75 resulted in consequence management occurring after the start of the investigation, of which:

(a) 32 occurred during the AFS licensee's investigation; and

(b) 43 occurred after the end of the licensee's investigation.

Consequence management for managers

434 As noted at paragraph 412, 50 significant breaches involved consequence management for management responsible for the root cause of the significant breach.

435 Of these instances, at least 48 involved consequence management occurring after the start of the investigation, of which:

(a) 12 occurred during the AFS licensee's investigation; and

(b) 36 occurred after the end of the licensee's investigation.

Where no consequence management occurs

436 We found 296 instances where AFS licensees attributed a root cause for the significant breach to staff. Around one third (92) of these instances recorded the application of consequence management to staff.

437 The high proportion of significant breaches with no consequence management is partly explainable, but not excusable, by the length of time taken to identify breaches.

438 With identification for four years or greater, it is often difficult to determine who was responsible for the root cause of the breach. Even when the reviewed financial groups identified staff or management that may have been suitable for consequence management, those individuals had often departed before consequences could be applied.

439 We also found 34 instances where the AFS licensee advised that the staff identified as responsible for the root cause was no longer employed before consequence management could be applied.

440 We found that the reviewed financial groups were likely to attribute a root cause for the significant breach to either process or system failures (65% processes, 36% systems, respectively). We consider that when the process or system are blamed, it becomes easier to not hold staff or management accountable for those breaches. This is despite the fact that staff and management were ultimately responsible for the development and implementation of those processes and systems.

441 The lower number of consequence management applied to management (50) versus staff (92) is consistent with APRA's observation that CBA was more likely to focus on allocating blame to specific individuals responsible for specific tasks, without appropriate focus on overarching accountability of senior leaders: see APRA, *Prudential inquiry into the Commonwealth Bank of Australia—Final report*, May 2018, p. 61.

Opportunities for improvement

Timely application of consequence management

442 Timely application of consequence management will enable AFS licensees to hold staff and management accountable. Timeliness is also important to reducing the chances of further breaches occurring or the same breach continuing.

443 Delays in enacting consequence management may enable staff members to avoid consequences by resigning. We found 34 instances where staff or management had resigned before being able to be subject to consequence management.

444 The timely application of consequence management may limit the possibility of this occurring. However, this may be unavoidable in many instances—individuals under investigation will usually be aware of it and there is no practical way to prevent staff or management resigning before the investigation is complete.

Recognising the need to consider potential red flags

445 The application of consequence management should trigger a review (or possible re-examination) of whether a significant breach has occurred.

446 We found, in 28 instances, AFS licensees first applied consequence management during their investigation, but did not lodge a breach report to ASIC until after the end of their investigation. While the application of consequence management may not be conclusive evidence that a significant breach has occurred, it should be a red flag for the AFS licensee to consider whether sufficient information is available to report a significant breach.

447 We found 19 instances where consequence management was applied before the start of the AFS licensee's investigation (i.e. unrelated to the investigation of the significant breach). Licensees are best placed to consider whether a broader, more proactive, inquiry into other aspects of the staff or management's work is appropriate based on the nature of the unrelated breach.

Record keeping

448 Sound record keeping is necessary to ensure the application of consequence management is consistently and transparently applied.

449 Some reviewed financial groups advised that, in some instances, no records may be available since they reflect the low-end spectrum of consequence management (e.g. a warning). If records did exist these were likely to be stored on the individual's file as opposed to the compliance system that stores information on the significant breach.

450 The reviewed financial groups specifically raised a concern that it would be difficult to identify consequence management in all instances. Our view is that where it is difficult to identify such measures, it would be equally difficult to monitor and ensure those measures are effectively implemented.

451 In instances where no consequence management has been applied, the AFS licensee should record the rationale for not doing so.

E Breach management culture

Key points

In this review, we considered the extent to which a reviewed financial group's culture supports its ability to meet its breach reporting obligation (i.e. whether we see elements of a sound breach management culture).

Key elements of a sound breach management culture (and which we have considered in this review) are:

- the quick detection of breaches, and incidents more broadly;
- robust compliance measures (systems and processes) that allow appropriate information about breaches and incidents to be captured;
- the prioritisation of investigations into breaches;
- the monitoring of outcomes following a breach and prioritisation of remediation; and
- the sharing of learnings about the breach, to allow staff to learn from the breach and keep key decision makers apprised of developing systemic issues.

Summary of our observations

452 In this review, we gathered data about the key stages of breach management. In this section we draw together our observations about:

(a) the extent to which a reviewed financial group's culture supports its ability to meet the breach reporting obligation; and

(b) whether we see elements of a sound breach management culture.

453 A sound breach management culture will:

(a) prioritise and support the ability of an AFS licensee to meet its breach reporting obligation; and

(b) provide an environment where:

(i) staff can raise concerns about risks, including incidents (and are vigilant for these);

(ii) investigations, rectification and remediation are prioritised—and overseen and championed by senior management; and

(iii) transparent communication about breaches and incidents promotes identification, rectification and reporting.

454 In general, we observed that aspects of the culture of the AFS licensees under review did not support the ability of these entities to meet the breach reporting obligation. In many instances, the reviewed financial groups did not demonstrate a sound breach management culture.

455 We observed that some licensees under review did not give adequate priority to:

(a) how breaches are detected and managed within the organisation—a significant minority of staff were uncomfortable raising concerns about risks; and

(b) how customers are remediated following a breach—which does not align with statements made by many of the reviewed financial groups about treatment of customers, both publicly (e.g. values) and in internal documents (e.g. policies and procedures).

Note: In this section we use 'customers' rather than 'consumers', as this reflects language used by the reviewed financial groups (e.g. in their values and other documents).

456 In some cases, we also observed a limited and inconsistent level of oversight by senior management across the key stages of a significant breach.

457 We have included our observations below, and encourage AFS licensees to consider these issues, and how they may apply to their business.

458 Our observations about how the reviewed financial groups demonstrated elements of a sound breach management culture are summarised in Table 19. Note that these observations are thematic, and generally apply to the reviewed financial group as a whole.

Note: 1. Our framework for analysis of the culture issues considered in this review draws from research on error management culture in financial institutions by AFM (*Learning from errors: Towards an error management culture—Insights based on a study in the capital markets*, October 2017) and De Nederlandsche Bank (*Supervision of behaviour and culture: Foundations, practice and future developments* (PDF 3.5 MB), September 2015).

Note 2. Culture remains a key priority for ASIC. This review of culture was a pilot project for ASIC to help us further refine our approach to understanding culture, and incorporating culture into our regulatory work.

Table 19: Elements of a sound breach management culture: Data and our observations

Element	What the data shows	Our observations
Breaches are detected quickly	Breaches are not detected quickly: see key stage 1 at paragraphs 83–131. For the major financial groups, breaches took nearly four years to identify: see Figure 2.	In general, the reviewed financial groups had values, policies, and training for staff that encouraged them to be alert to and identify risks, and to raise their concerns in a timely manner. The data and case studies did not always show this to be the case in practice. We encourage the reviewed financial groups to consider possible reasons for this: see Table 20.

Element	What the data shows	Our observations
Compliance measures (systems and processes) allow appropriate information to be captured	Breach information was often recorded over many databases, and was not always searchable: see key stage 2 at paragraphs 127–153.	A sound breach management culture is built on good data, and being able to use it to 'connect the dots' about emerging problems: see paragraphs 477–482.
Investigation of breaches is prioritised	In many instances, investigations of breaches took too long: see key stage 3 at paragraphs 154–288.	We are concerned that some investigations by the reviewed financial groups, in particular the major financial groups, are not sufficiently prioritised. These investigations appeared to lack adequate resources and oversight by senior management, which may have contributed to their length: see paragraph 483–486.
Customer outcomes following a breach are monitored and remediation is a priority	The major financial groups all had values relating to prioritising customers and addressing problems quickly. This contrasted sharply with data about the time taken to communicate with and remediate customers: see key stage 4 (at paragraphs 304–330), key stage 5 (at paragraphs 331–383) and Figure 9.	Some of the major financial groups did not always prioritise remediating customers. There was a lack of alignment between stated values in relation to customers and outcomes for customers following a breach, and evidence that, at times, remediation was perceived as a 'distraction' from core business: see paragraphs 487–494.
Learning from incidents and breaches	Formal 'lessons learned' reports were produced for 38% of significant breaches (271). Only 4.8% (13 of 271) of such reports were formally shared outside the business unit affected by the breach.	In many instances, 'lessons learned' processes appeared not to take place or were ad hoc and not formalised: see paragraphs 495–500.

Sound breach management culture

459 An AFS licensee with a sound breach management culture will take an organisational approach. This means that breaches and other incidents are identified, analysed and evaluated at the organisational level, as opposed to an individual approach—for example, only in relation to a specific incident or employee.

> Note: See De Nederlandsche Bank, *Supervision of behaviour and culture: Foundations, practice and future developments* (PDF 3.5 MB), September 2015, p. 281.

460 What this means in practice is that AFS licensees understand:

(a) what incidents and breaches are occurring across the financial group;

(b) why each incident and breach occurs; and

(c) how this knowledge can be used across the *organisation* (as opposed to only a business unit or line) to reduce the likelihood of it (or a similar problem) recurring in the future.

461 Elements we would expect to see in AFS licensees that have a sound breach management culture, and which we have considered within the scope of this review include:

(a) the quick detection of breaches, and incidents more broadly;

(b) robust compliance measures (systems and processes) that allow appropriate information about breaches and incidents to be captured and used by the financial group;

(c) the prioritisation of investigations into breaches;

(d) the monitoring of customer outcomes following a breach and prioritisation of remediation;

(e) the sharing of learnings from and knowledge about the breach, and the related analysis, across the financial group, to allow staff to learn from the breach and keep senior management apprised of developing systemic issues.

462 In order to create and maintain a sound breach management culture, we expect AFS licensees to consider all the above issues in relation to their own businesses. This must be an ongoing process, not a one-off exercise. Throughout this section, we have included 'Questions to ask' to provide licensees with a starting point for this process.

463 Our findings show that in many instances the reviewed financial groups did not demonstrate these elements. A general observation is that the reviewed financial groups do not give adequate priority to the management of breaches (and customer outcomes following a breach) relative to other business priorities.

464 We acknowledge that AFS licensees have many, often competing, priorities within their businesses, and that there is often a tension between these different objectives. These tensions are a reality for any business, and need to be managed effectively.

465 We expect AFS licensees to:

(a) be aware of and manage tensions between competing business priorities; and

(b) focus on customer outcomes and effectively manage problems that arise (e.g. following breaches and other incidents), and take steps to ensure that these are appropriately prioritised.

Note: See M Power, S Ashby & T Palermo, *Risk culture in financial organisations: A research report*, Centre for Analysis and Risk Regulation, 2013, p. 22.

Breaches are detected quickly

466 An indicator that an organisation has a sound approach to managing incidents and breaches is that they are detected quickly.

> Note: See De Nederlandsche Bank, *Supervision of behaviour and culture: Foundations, practice and future developments* (PDF 3.5 MB), September 2015, p. 287.

467 Quick detection allows problems to be fixed sooner, limiting the impact to fewer customers. The older an incident or breach becomes, the harder it is to fix: more customers are impacted, key staff may leave the organisation, and the scale of the problem increases: see our discussion of key stage 1 at paragraphs 83–131.

468 The reviewed financial groups were, in general, not able to detect breaches and incidents quickly. The average time from a significant breach starting to it being identified for investigation is 1,517 days—that is, just over four years—(median: 925 days): see Figure 2.

469 In general, we found that:

(a) the reviewed financial groups had values, and high-level expectations for behaviour, relating to how breaches are managed. This included:

  (i) values such as 'integrity' and 'doing the right thing'; and

  (ii) statements about what behaviour is expected from staff, including that staff should:

    (A) be alert to and identify risks;

    (B) raise concerns about risks and mistakes quickly with managers; and

    (C) err on the side of caution, and raise issues even if they are not 100% sure it is a problem;

(b) the reviewed financial groups had policies and guidance for staff that encouraged them to raise concerns with managers and escalate issues if they did not feel they were being dealt with effectively; and

(c) most of the reviewed financial groups acknowledge that staff raising issues, and logging incidents quickly and with the correct information, is important for their risk management and breach reporting processes to work effectively. This was stated in training and other documents.

470 These statements are important, as it makes it clear to staff that identifying incidents is a priority for the organisation. In their written policies and other documents (e.g. the formal values frameworks and communications with staff about expected behaviour), the reviewed financial groups do appear to place a priority on these issues.

471 However, a 2017 study by AFM found that in relation to how errors and incidents are dealt with:

> Structure and culture are also well aligned when a clear policy is really implemented in practice throughout the organisation. For example, when the importance of consistently reporting errors is not only stated on paper, but is also actively promoted and valued by the senior management, middle management and employees among each other. In that case, the tone at the top is the same as on paper and people are actively involved in the policy.
>
> Note: See AFM, *Learning from errors: Towards an error management culture—Insights based on a study in the capital markets*, October 2017, p. 13.

472 Given that the reviewed financial groups generally did have values, policies and processes in place to encourage staff to report incidents, one interpretation of the data is that the reason breaches are not being identified quickly is because:

(a) policies and procedures are not being effectively implemented in practice; and/or

(b) staff are not proactive in looking for risks; and/or

(c) managers are not actively promoting the desired behaviour (e.g. through recognition and reward for staff that identify and raise incidents).

473 These statements are observations, not findings, as we do not have clear data about these issues.

474 Staff survey results that were provided as part of the review indicated that there is still a significant minority of staff who are uncomfortable raising concerns. However, more recent results showed an improvement in the number of staff comfortable raising concerns. We also consider it a positive sign that the reviewed financial groups are gathering this data.

475 Given the inability of the reviewed financial groups to detect incidents and breaches quickly, we encourage all AFS licensees to review how quickly incidents and breaches are detected in their organisation. If it takes a long time to detect incidents and breaches, we expect AFS licensees to do further work to:

(a) understand why this is the case;

(b) make changes to reduce the time it takes for incidents and breaches to be detected; and

(c) monitor, on an ongoing basis, whether incidents and breaches are (in general) being detected more quickly.

476 We encourage all AFS licensees to consider the questions set out in Table 20 in relation to how breaches are managed in their own business, and take action as necessary.

Table 20: Questions to ask—Detecting incidents and breaches quickly

Issue	Questions
Staff raising incidents and breaches	Are staff encouraged to raise problems, incidents or breaches within their teams as part of their day-to-day roles? How are staff supported to do this? Does the AFS licensee truly value staff who raise issues or problems, or is there a 'good news only' culture? If staff surveys point to weaknesses, how are the possible root causes of staff perceptions explored? What senior management oversight and accountability exists to drive this work forward as a priority?
Support from senior management for raising incidents and breaches	Are leaders accessible and open to staff expressing a different point of view or raising problems? Does senior management encourage staff to discuss problems, and escalate them as appropriate? Does senior management provide oversight to middle managers and ensure that staff support is occurring in practice?
Role of audit and compliance	If compliance or internal audit raises concerns about the way breaches are being managed, what is done to address these concerns? Who is accountable in the organisation (i.e. what level of management) for ensuring the concerns raised by compliance or internal audit are addressed?
Senior executive committee and board oversight	What oversight do senior executive committees and the board have of the way that breach management systems and processes are working in practice? What reports do they see (i.e. is appropriate and clear information given to executive committees and the board)? How does the board hold management accountable for this oversight?
Monitoring—'closing the loop'	How and how often are all the above issues monitored to ensure that the various checks and balances in place are functioning as intended? Who is responsible for ensuring this monitoring takes place? How are issues that are identified addressed and learnings shared? What data sources are used to monitor staff perceptions about the way that incidents and breaches are being managed?

Compliance measures capture appropriate information

477 A sound breach management culture is built on good data; therefore, an important element of a sound breach management culture are compliance measures (systems and processes) that ensure that key information about breaches and incidents is consistently captured.

478 This allows the information to be used for more strategic analysis (e.g. to detect emerging systemic issues). In large organisations, problems can slowly emerge over weeks, months or years. Systems and processes that capture incident data that can be used for analysis at the organisational level can detect problems (or possible future problems) that individual business units may miss.

479 AFM found that, in relation to the best practice for how incidents are managed, well-designed software is an important aspect and should allow staff to 'report errors quickly and easily in one user-friendly registration system': AFM, *Learning from errors: Towards an error management culture—Insights based on a study in the capital markets*, October 2017, p. 13.

480 In this review, we considered the extent to which compliance measures for breach reporting helped the reviewed financial groups meet their breach reporting obligation: see our discussion about recognising emerging systemic issues using compliances systems at paragraphs 110–117. Our data indicates that this was a potential area of weakness for many of the reviewed financial groups. Our findings included that:

(a) breach information was often recorded over many databases;

(b) breach information was not always recorded in a searchable fashion. In some cases, key information was not recorded; and

(c) in some cases, investigations involved a high number of manual compilations and there was no automatic process to determine the extent to which an individual customer had been affected by the breach.

481 Capturing information in a fragmented way makes it difficult for staff to 'connect the dots' about what is going on within the licensee and make meaningful changes to fix problems. Further, once compliance measures are in place, they need to be regularly reviewed to ensure that they are functioning as intended, and able to provide useful information to the business more broadly: see Case study 6.

482 We encourage all AFS licensees to consider the questions set out in Table 21 and take action as necessary.

Table 21: Questions to ask—Compliance measures

Issue	Questions
Compliance systems and processes	Are compliance systems and processes user friendly? Is staff feedback about compliance systems and processes sought and used to improve the systems and processes? Do systems and processes capture key information about breaches (and incidents more broadly) in such a way that it can be used effectively by the licensee (e.g. for strategic reporting purposes (senior management, the board, other internal reporting), reporting to regulators, detecting emerging systemic issues)? Are compliance and audit teams able to use data about breaches and incidents to inform advice they give to senior executive committees?
Monitoring—senior management oversight	Once operational, are compliance measures monitored to ensure that they are functioning as intended? Is appropriate and strategic data about breaches and incidents regulatory reported to senior executive committees? Is the quality of data being captured about breaches and incidents subject to a regular audit process?

Investigation of breaches is prioritised

483 We consider that financial groups with a sound breach management culture will prioritise the investigation of breaches. Giving priority to investigating breaches means that:

(a) the root cause can be identified promptly and corrected; and

(b) staff are not given 'mixed messages'—that is, values and training stating that compliance issues are important, while actual business practices show that addressing compliance issues is not always a priority.

484 The data we collected demonstrated that, in a quarter of breach reports we received, the reviewed financial groups took almost six months (168 days) to investigate an incident and lodge a breach report with ASIC (key stage 3). Further, the major financial groups took an average of 150 days for this key stage, while other financial groups took an average of 73 days. This data implies that the major financial groups may not be giving adequate priority or resourcing to the investigation of breaches.

485 In some cases, we also observed a limited and inconsistent level of oversight by senior management across the key stages of a significant breach: see paragraph 270. This is another indicator of the general low priority given to timely investigations of breaches. It is also likely to send a message to staff that the financial group does not prioritise timely investigations: see Case study 9.

486 We encourage all AFS licensees to consider the questions set out in Table 22 and take action as necessary.

Table 22: Questions to ask—Prioritising investigation of breaches

Issue	Question
Values and stated priorities	Many AFS licensees make public statements (e.g. on their websites) that they will prioritising fixing problems—do these statements align with what occurs in the licensee's business?
Governance and controls	Once an investigation is underway, is there appropriate oversight by senior management to ensure that investigation is progressing, is resourced and is generally being appropriately prioritised by the licensee?

Customer outcomes are monitored and remediation is a priority

487 In this review we considered:

(a) the reviewed financial groups' stated values regarding customers and what they say they will do if something goes wrong; and

(b) following a breach being investigated, how quickly the reviewed financial groups:

(i) communicate with affected customers (see key stage 4 at paragraphs 304–330); and

(ii) make payments to affected customers (see key stage 5 at paragraphs 331–383).

488 We discuss our observations about the alignment between the stated values and the outcomes for customers following a breach in this subsection.

489 Values are important because they signal the organisation's priorities to customers, staff and the broader community. The major financial groups all have:

(a) one or more values that focus on customer service or 'putting customers first'; and/or

(b) public statements that they will quickly 'put things right' for customers when problems occur.

490 Our data found that, once an investigation of a significant breach has been completed:

(a) the first communication with customers took an average of 189 days (over six months); and

(b) the first payments to customers took on average 226 days (over seven months).

491 The long timeframes for communication with and payment to customers indicates that customers are not being prioritised, relative to other priorities within the business. This lack of priority given to putting customers back in the position they would have been in, is not aligned with the values and statements made about 'putting customers interests first' and fixing problems when they arise.

492 In our review of documents more broadly, we saw evidence of remediation being perceived as:

(a) a distraction from core business, and an activity which was undertaken at the expense of earning revenue. As a result, remediation was not given the highest priority; and

(b) an activity that distracts management away from opportunities to meet consumer needs.

493 The perception that remediation is a 'distraction' does not align with the stated values of the reviewed financial groups regarding putting the interests of customers first, and fixing problems quickly. We were pleased to see an example of a reviewed financial group 'calling out' this perception and acknowledging that it was a perception that needed to change and would change going forward: see Case study 23.

494 We encourage AFS licensees to consider the questions set out in Table 23 and take action as necessary.

Table 23: Prioritising remediation of customers—Questions to ask

Issue	Questions
Stated values about priority of customers and what the AFS licensee will do if something goes wrong	Do the AFS licensee's stated values about primacy of customers (e.g. 'we put our customers first') and what it says it will do when something goes wrong (e.g. 'we will put things right') align with what occurs following a breach?
Internal perceptions of remediation	Does the AFS licensee perceive remediation following a breach as an integral part of doing business (i.e. taking responsibility for fixing mistakes) or is it perceived negatively (e.g. as a 'distraction')? What is the 'tone' from senior management about remediation processes? Does senior management provide appropriate resources to and oversight of remediation projects? What steps are taken to ensure that remediation is treated by the business as an important process for ensuring fair customer outcomes?
Governance and controls	What oversight of remediation processes is provided by compliance, audit, customer advocate and senior executive committees? What information is shared with compliance, audit, customer advocate and senior executive committees, and what metrics do they consider in relation to delays in the remediation process and remediation being narrowly scoped?

Learning from incidents and breaches

495 Learning from incidents and breaches is an attribute that all AFS licensees with a sound breach management culture should display. For example, AFM found that 'more is learned from incidents and breaches in organisations with [a sound] error management culture'—this in turn contributes to ethical conduct (staff are more likely to report their own errors and errors others made), a better-quality service to customers and better performance of the firm.

> Note: See AFM, *Learning from errors: Towards an error management culture—Insights based on a study in the capital markets*, October 2017, p. 4.

496 Our review showed that licensees may not be maximising the improvement opportunities that breaches present.

497 We found that 'lessons learned' reports about significant breaches were only documented in 38% of instances. However, in the case studies where the AFS licensee identified that a 'lessons learned' report existed, most documents reviewed were more accurately described as a summary of key information about the breach. These documents did not demonstrate a deep exploration of the root causes of the breach or how similar breaches could be prevented in the future.

498 We did see aspects of some reviewed financial groups' breach reporting process that attempted to identify and share broader lessons about not only the significant breach, but also the implications for the business and for its customers. We identified specific workshops, training, and lessons contained in a final report to key decision makers: see key stage 3 at paragraphs 281–284.

499 We saw little evidence of sharing 'lessons learned' reports across other business units or other AFS licensees within the reviewed financial group. Our data indicated that this only occurred in 4.8% of instances. This finding is concerning, as without a formal and consistent lessons learned process around breaches, licensees are unlikely to be able to take proactive steps to see whether the breach or incident has affected or could affect similar systems, compliance measures, products or services across the licensee or within the financial group. It also hinders a licensee from adopting any improvements relevant to other parts of the business.

500 We encourage AFS licensees to consider the questions set out in Table 24 and take action as necessary.

Table 24: Questions to ask—Learning from breaches

Issue	Questions
Learning from breaches and incidents	How does the AFS licensee ensure that the organisation learns from breaches and other incidents, with the goal of reducing future problems? Do business units seek to learn from breaches and incidents that occur? Are these learnings shared across the licensee? Are learnings used strategically (e.g. in the development of new products and services, reporting back to senior management, senior executive committees or to the board)? How does the licensee ensure that learnings are utilised for maximum benefit?
Training	Does compliance and risk training for staff use learnings from recent breaches or incidents as case studies or scenarios to demonstrate conduct risks, behavioural standards and decision-making consequences?

F ASIC's actions

Key points

We will continue to monitor the conduct of AFS licensees, including their remediation of consumers financially affected by significant breaches, and the effectiveness of their breach reporting processes. This work will form part of our close and continuous monitoring of the major financial groups and AMP, which is scheduled to begin in October 2018.

We will continue to support the law reform proposed by the ASIC Enforcement Review to enable clearer and more objective compliance with the breach reporting obligation. In the meantime, despite the subjectivity and ambiguities in the current legal requirements, ASIC will continue to take the appropriate regulatory action for non-compliance with the breach reporting obligation.

We are developing the ability for AFS licensees to lodge breach reports to ASIC through the ASIC Regulatory Portal.

ASIC's ongoing work

501 Breach reporting to ASIC is a statutory requirement and a cornerstone of our regulatory architecture.

502 Despite the subjectivity and ambiguities in the current legal requirements, we will take regulatory action for non-compliance with the breach reporting obligation such as:

(a) failure to report significant breaches to ASIC;

(b) late lodgement of a breach report (i.e. later than 10 business days of awareness);

(c) lying to ASIC about the nature of a breach; and

(d) failure to have adequate compliance measures to meet obligations.

Monitoring and surveillance

503 As part of our ongoing business as usual and surveillance programs, we will continue to monitor the effectiveness of breach reporting processes. We may consider a follow-up review, or broader reporting of benchmarks of AFS licensees' future performance.

504 We will also continue to monitor, and where necessary intervene in, the remediation to consumers that is required as a result of significant breaches. If AFS licensees are not able to remediate all customers, we expect that licensees will have in place processes to ensure that they do not profit from their significant breaches.

505 Senior ASIC staff will commence an on-site monitoring role at the major financial groups and AMP from October 2018. ASIC will have dedicated supervisory staff on-site for extended periods within these institutions to monitor their governance and compliance with laws, including a focus on the management of significant breach reports and their rectification programs.

506 The new ASIC Regulatory Portal will help ASIC undertake more complex data analysis that may either indicate or identify systemic issues in AFS licensees' breach reporting processes. For more information on the portal, see paragraphs 512–514.

Updating guidance

507 We will also update the relevant regulatory guides, in particular RG 78. The updated guidance, where appropriate, will incorporate the findings in this report and set out the prescribed format AFS licensees will need to use to submit a breach report to ASIC via the portal.

Law reform

508 Regarding timeliness and consistency in breach reporting, we note that the *ASIC Enforcement Review taskforce report* attempts to strike a balance between allowing a reasonable amount time for an AFS licensee to conduct an investigation and achieving a more timely report to ASIC. The report recommends at p. 9 that:

> … there should be an objective element to the trigger for reporting and that reporting requirements should extend to circumstances where a breach is being investigated by the licensee but the investigation has not concluded within the prescribed time limit. In addition, the time frame should be extended so that licensees, in the first instance, have 30 days for conducting investigations and the initial assessment whether a matter is reportable.
>
> This should be achieved by providing that when a licensee becomes aware of conduct or has information that reasonably suggests that a breach has occurred, may have occurred or may occur in the foreseeable future, the licensee must as soon as practicable—but in any event within 30 calendar days—lodge a report with ASIC…

509 Thus, the ASIC Enforcement Review Taskforce recommends that the 30-day reporting period should commence when the AFS licensee becomes aware of or has reason to suspect that a breach *has* occurred, *may have* occurred or *may* occur—rather than when the licensee determines that the relevant breach *has* occurred and *is* significant.

510 Currently, the average time to report to ASIC from the start of an investigation is 128 days among the reviewed financial groups. Only around a quarter of the significant breaches would have been reported to ASIC

within the proposed 30-day reporting period. This recommendation will reduce delays in reporting to ASIC.

511 The move to a more objective standard for significance will also reduce the complexity of assessing whether a breach is significant, including by allowing for more detailed guidance from the courts and ASIC. This will make breach reporting more consistent across AFS licensees.

ASIC Regulatory Portal

512 We are developing the capacity to allow AFS licensees to submit breach reports, and updates, through the new online ASIC Regulatory Portal as part of our overall efforts to improve licensees' regulatory interactions with ASIC.

513 Breach reports will be able to be submitted through the portal in 2019. Before this feature becomes available, the portal webpage will be updated to give AFS licensees the necessary information to use this function.

514 The portal's capacity may be further developed in the future to address any law reform, if implemented, to allow submitting suspicious breaches to ASIC and extending the breach reporting obligation to credit licensees.

Appendix 1: Overview of breach reporting review data

Breach reporting review data

515 We collected data on 715 significant breaches that the reviewed financial groups reported to ASIC between 2014 and 2017.

516 In some instances, the same breach affected multiple AFS licensees within the reviewed financial group. This corresponds to a total of 512 unique breaches. When the same unique breach affected more than one AFS licensee within the reviewed financial group, ASIC would usually receive one document outlining the same breach for each AFS licensee.

517 ASIC has also received one document where different breaches may have been 'bundled' into a single breach report by one or more AFS licensees. In many of the reports received by ASIC, expected information was not included in the breach report.

518 For these reasons, we sought data per significant breach, per AFS licensee, and our findings reflect this methodology.

519 For each significant breach, we collected quantitative data, including the key dates of the reviewed financial groups' end-to-end breach management process. This allowed for a timeline that captures the lifecycle of each significant breach.

520 The lifecycle begins when the incident first occurs, continues when the AFS licensee identifies an incident, records that incident in their system, conducts an investigation, assesses whether it is a significant breach, reports to ASIC, and finishes with any breach rectification, including consumer remediation.

521 In addition, we collected qualitative data from the reviewed financial groups on the incident management processes used to identify incidents that may prove to be:

(a) a significant breach;

(b) a breach, but assessed as not a significant breach; and

(c) not a breach.

522 Further, as part of the qualitative data collection from the reviewed financial groups, we reviewed policies, procedures, and registers for breach reporting practices: see paragraphs 74–82.

523 Across the reviewed financial groups, classification of incidents was inconsistent. The process to arrive at some level of categorisation also varied across the reviewed financial group.

524 Variance in classification and process meant that no comparable data was obtained on the breadth of incidents that the reviewed financial groups investigated.

525 Most of the reviewed financial groups assessed incidents in two stages. First, they determined if a breach had occurred; if they determined that a breach had occurred, they then conducted a second assessment of whether the breach was significant.

526 Some of the reviewed financial groups, however, assessed all incidents directly against the significance test. If they determined the incident was not significant, did not appear to conduct a secondary assessment as to whether any breach had occurred.

527 We also reviewed the content of select voluntary reports or good governance reports that some of the AFS licensees in the reviewed financial groups made to ASIC. These voluntary reports are about breaches or potential breaches that are assessed as being not significant but are nevertheless reported. We have referenced these voluntary reports to highlight the subjective nature of significance.

Use and application of statistical information

528 In this report we have used two statistical measures of central tendency for timelines and financial losses: medians and averages. A median is the value that is in the middle of a range of values, whereas the average is achieved by adding all the values in the range and then dividing by the number of values in the range.

529 Although they do not provide a full picture of the data analysed, they give indications of data distribution. Averages are affected by outliers in a more substantial way than medians. Given the data we collected, we could observe in many instances that the average tended to be considerably larger than the median. This indicates a distribution of data skewed to the right (large positive outliers, which pushes the average up).

530 In addition, we have also calculated the standard deviation, which is a measure of spread. Large values show that the distribution in some instances is highly spread out.

531 It is important to take into consideration those measures to get a better understanding of the data, as an average might be showing a result that is not confirmed by the median. For example, when we talk about the time elapsed between the identification of a significant breach and the start of the

investigation, the calculated average showed a value of 28 days. That means that an investigation started an average of 28 days after the breach was identified.

532 The standard deviation is 129 days, which shows that the distribution has outliers. It means that in some instances the investigation started much later or earlier than 28 days after the breach was identified. Contrastingly, the median showed a value of 0 days. That indicates that at least 50% of significant breaches had their investigation started immediately after or even before the breach was identified.

533 An investigation may be used to determine whether a breach is significant or not or to determine other aspects of a significant breach (e.g. the root cause, consequences, number of consumers affected, need for remediation and/or rectification). Therefore, investigations starting before the identification of a breach could mean that they were used to determine the significance of the breach.

534 While reading this report, be mindful of the limitations of the measures used to reflect the behaviour and/or pattern of the reviewed financial groups.

Financial services and products

535 Significant breaches can occur in relation to any of the financial services or financial products that form part of an AFS licensee's business offering.

536 We examined the financial services and products affected by the reviewed financial groups' significant breaches. One breach could affect multiple financial services and products.

537 Table 25 sets out the top financial services and products subject to significant breaches, as advised by AFS licensees.

Table 25: Top financial services and products affected

Financial services and products	Number of breaches	Percentage of total breaches
Superannuation	284	40%
Personal advice	191	27%
Managed investment schemes	116	16%
Life insurance	98	14%
General advice	53	7%
General insurance	43	6%

Note: Each line item in the above table is based on a specific subset of the 715 significant breaches that had applicable data. Licensee groups were able to select more than one option, if applicable.

Types of significant breaches

538 We required the reviewed financial groups to categorise the significant breaches they reported to ASIC. The main broad categories included:

(a) breaches of various conditions of an AFS licensee;

(b) deficient disclosure;

(c) incorrect fees and charges;

(d) misconduct, including staff misconduct;

(e) conflicts of interest; and

(f) non-compliance with managed investment scheme obligations.

539 The categories were not mutually exclusive and AFS licensees could select more than one category if appropriate.

540 Table 26 sets out the top categories the significant breaches relate to, as advised by AFS licensees. We found that the top three categories that AFS licensees selected related to their failure to comply with the financial services laws, deficiencies in disclosure and breaches involving licensees' fees and charges.

Table 26: Top categories of significant breaches

Categories of significant breaches	Number of breaches	Percentage of total breaches
Breach of licence conditions—Failure of licensee to comply with financial services laws	465	65%
Deficient disclosure Note: Includes deficiencies in Statements of Advice (SOAs), Product Disclosure Statements (PDSs), Financial Services Guides (FSGs), periodic statements, fee disclosure documents and marketing materials.	265	37%
Incorrect fees and charges	174	24%
Breach of licence conditions—Inadequate compliance systems	152	21%
Breach of licence conditions—Failure of licensee's representatives to comply with financial services laws	97	14%

Note: Each line item in the above table is based on a specific subset of the 715 significant breaches that had applicable data. Licensees were able to select more than option, if applicable.

Root causes

541 We also required the reviewed financial groups to identify what they believed to be the root cause(s) of the significant breaches reported to ASIC. One breach could have multiple root causes. The root causes identified included but were not limited to:

(a) process deficiencies;

(b) system deficiencies;

(c) lack of training;

(d) staff not adhering to policy and/or process;

(e) negligence and/or error; and

(f) fraud and/or misconduct.

542 The options presented were not mutually exclusive and AFS licensees could select more than one root cause if appropriate.

543 Since a failure to report a significant breach may itself be a significant breach, we also asked AFS licensees to identify if they had failed to comply with s912D(1)(b) or with other statutory reporting requirements.

544 Table 27 sets out the root causes of significant breaches, as advised by AFS licensees.

Table 27: Root causes of significant breaches

Root causes	Number of breaches	Percentage of total breaches
Process deficiency	466	65%
Systems deficiency	257	36%
Staff—Non-adherence to policy and/or process	151	21%
Staff—Lack of training	97	14%
Staff—Negligence and/or error	87	12%
Staff—Fraud and/or misconduct	30	4%
Staff—Unaware that error amounted to breach	37	5%
Staff—Failure to comply with s912D or other statutory reporting requirements to ASIC	26	4%

Root causes	Number of breaches	Percentage of total breaches
Other Note: Includes disclosure issues, fraud and/or misconduct by authorised representatives, product deficiency, adviser conduct issues, change in legislation. It also includes some instances where licensees have erroneously selected this option instead of a more appropriate available option, like process deficiency or system deficiency.	98	14%

Note: Each line item in the above table is based on a specific subset of the 715 significant breaches that had applicable data. Licensee groups were able to select more than option, if applicable.

545 The reviewed financial groups' responses indicated that, at an industry level, process deficiencies and system deficiencies were the top two root causes. The third highest root cause was staff not adhering to the AFS licensee's policies or processes, followed by a lack of staff training.

Types of consequence management

546 Table 28 sets out the types of consequence management AFS licensees used to respond to significant breaches.

Table 28: Types of consequence management

Type of consequence management	Number of breaches	Percentage of total breaches
Reduction in bonus	47	7%
Adverse performance rating	44	6%
Additional mandated training	26	4%
Exclusion from bonus	20	3%
Official warning	19	3%
Termination	22	3%
Additional mentoring and/or closer supervision	15	2%
Other	105	15%

Note: Licensee groups were able to select more than option, if applicable.

Channels of identification

547 We sought information from the reviewed financial groups on the channels through which they identified significant breaches.

Note: The review considered external auditors as a channel of identification.

548 Table 29 sets out the channels of identification for significant breaches, as advised by AFS licensees.

Table 29: Channels of identification for significant breaches

Channel	Number of breaches	Percentage of total breaches
The relevant business unit's staff	331	46%
Internal audit and/or compliance departments	164	23%
Consumer complaints	67	9%
Engagement with ASIC	15	2%
Other	183	26%

549 It appears that many significant breaches were identified when the AFS licensee reviewed or updated its processes, systems, or disclosure documents. This underscores the importance of AFS licensees regularly reviewing their internal procedures and documents to ensure that they continue to meet regulatory requirements: see RG 104.28–RG 104.29.

550 In a few instances, the significant breaches were identified while following up on a client or financial adviser's query, rather than a complaint. This highlights the need to have open lines of communication and the value in promptly investigating apparent anomalies.

Case studies

551 After analysis of the data, in conjunction with the information on ASIC's systems, we selected cases studies based on poorer performance against one or more our measurements of the stages of breach reporting processes.

552 Additionally, we looked for evidence of how the reviewed financial groups could demonstrate technical elements of a sound breach reporting culture.

Appendix 2: Accessible versions of figures

This appendix is for people with visual or other impairments. It provides the underlying information for the figures presented in this report.

Table 30: Average timeline of the reporting stages of a significant breach

Reporting stage	Number of days
Incident to identification	1,517
Identification to investigation	28
Investigation to breach report	128

Note: This table shows the data contained in Figure 1.

Table 31: Average time taken for key stage 1, by reviewed financial groups

Groups	Mean number of days	Median number of days
Reviewed financial groups	1,517	925
Major financial groups	1,726	1,148
Other financial groups	995	600
ANZ	1,517	1,088
CBA	1,526	820
NAB	1,849	1,228
Westpac	1,613	1,080
AMP	908	750
Macquarie	934	214
Suncorp	903	370

Note: This table shows the data contained in Figure 2.

Table 32: Average number of days for key stage 3, by reviewed financial groups

Groups	Mean number of days	Median number of days
Reviewed financial groups	128	69
Major financial groups	150	95
Other financial groups	73	34

Groups	Mean number of days	Median number of days
ANZ	213	132
CBA	104	35
NAB	139	93
Westpac	165	126
AMP	69	34
Macquarie	40	20
Suncorp	111	81

Note: This tables shows the data contained in Figure 3.

Table 33: Frequency of significance test factors in determining whether a breach is significant

Significance test factors	Number of breaches
Inadequate arrangements to ensure compliance	444
Actual or potential loss	347
Other	253
Number of frequency of breaches	250
Inability to provide financial services	19

Note: This table shows the data contained in Figure 4.

Table 34: Average time taken for each rectification stage of a significant breach

Rectification stage	Number of days
Key stage 4: Communication with consumers	189
Key stage 5: Payment to consumers	226
Key stage 6: Process change	42
Key stage 6: System change	68
Key stage 7: Accountability (staff)	22
Key stage 7: Accountability (management)	66

Note: This table shows the data contained in Figure 5.

Table 35: Average number of days for key stage 4, by reviewed financial groups

Groups	Mean number of days	Median number of days
Reviewed financial groups	189	143
Major financial groups	218	175
Other financial groups	29	19
ANZ	129	67
CBA	299	177
NAB	255	222
Westpac	21	31
AMP	43	38
Macquarie	-20	-4

Note: This table shows the data contained in Figure 6.

Table 36: Average number of days for key stage 5, by reviewed financial groups

Groups	Mean number of days	Median number of days
Reviewed financial groups	226	201
Major financial groups	251	217
Other financial groups	84	111
ANZ	198	140
CBA	352	316
NAB	265	234
Westpac	69	112
AMP	107	196

Note: This table shows the data contained in Figure 7.

Table 37: Average number of days between first and last payment to consumers affected, by reviewed financial groups

Groups	Mean number of days	Median number of days
Reviewed financial groups	119	41
Major financial groups	125	40

Groups	Mean number of days	Median number of days
Other financial groups	87	56
ANZ	131	82
CBA	284	134
NAB	74	14
Westpac	286	248
AMP	114	63

Note: This table shows the data contained in Figure 8.

Table 38: Average number of days between the first instance of a significant breach and the first payment to financially affected consumers, by reviewed financial groups

Groups	Mean number of days	Median number of days
Reviewed financial groups	2,145	1,525
Major financial groups	2,179	1,676
Other financial groups	1,977	1,398
ANZ	2,098	1,481
CBA	2,176	2,590
NAB	2,191	1,593
Westpac	2,232	2,270
AMP	2,011	1,318

Note: This table shows the data contained in Figure 9.

Table 39: Total financial loss and remediation, by the reviewed financial groups

Groups	Financial loss	Financial remediation
Reviewed financial groups	$497.2 million	$437.0 million
Major financial groups	$457.3 million	$400.2 million
Other financial groups	$40.0 million	$36.9 million

Note: This table shows the data contained in Figure 10.

Table 40: Average number of days for key stage 6 (process change), by the reviewed financial groups

Groups	Mean number of days	Median number of days
Reviewed financial groups	42	25
Major financial group	49	26
Other financial groups	19	0
ANZ	-53	-19
CBA	43	26
NAB	61	28
Westpac	73	77
AMP	63	82
Macquarie	-45	-9

Note: This table shows the data contained in Figure 11.

Table 41: Average number of days for key stage 6 (system change), by the reviewed financial groups

Groups	Mean number of days	Median number of days
Reviewed financial groups	68	33
Major financial groups	78	55
Other financial groups	30	-10
ANZ	27	46
CBA	134	59
NAB	71	59
Westpac	137	129
AMP	-17	-10

Note: This table shows the data contained in Figure 12.

Key terms

Term	Meaning in this document
AFM	Dutch Authority for the Financial Markets
AFS licence	An Australian financial services licence under s913B of the Corporations Act that authorises a person who carried on a financial services business to provide financial services Note: This is a definition contained in s761A.
AFS licensee	A person who holds an AFS licence under s913B of the Corporations Act
ANZ	Australia and New Zealand Banking Group Limited
AMP	AMP Limited
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
ASIC Enforcement Review	Treasury's review of ASIC's enforcement regime, which ran from 2016 to 2017
ASIC Regulatory Portal	The internet channel that allows authenticated regulated entities to interact securely with ASIC, which can be accessed at the portal landing page
Australian ADI	An Australian authorised deposit-taking institution—has the meaning given in s9 of the Corporations Act
breach rectification process	The process of rectifying a significant breach, which may involve some or all of the following key stages: • key stage 4—Communication with consumers; • key stage 5—Payments to consumers; • key stage 6—Process and/or system change; and • key stage 7—Accountability
breach report	Written report on significant breach that an AFS licensee lodges with ASIC under s912D(1B) of the Corporations Act
breach reporting obligation	The obligation contained in s912D of the Corporations Act
breach reporting process	The process of reporting a significant breach, which involves the following key stages: • key stage 1—Identification of incident; • key stage 2—Identification to investigation; and • key stage 3—Investigation to breach report.
CBA	Commonwealth Bank of Australia

Term	Meaning in this document
compliance measures	Processes, procedures or arrangements that an AFS licensee has in place to ensure, as far as reasonably practicable, compliance with their licensee obligations including the general obligations
consumer	A potential customer, a current customer or an ex-customer of the reviewed financial groups
Corporations Act	*Corporations Act 2001*, including regulations made for the purposes of that Act
credit licence	An Australian credit licence under s35 of the National Credit Act that authorises a licensee to engage in particular credit activities
credit licensee	A person who holds an Australian credit licence under s35 of the National Credit Act
financial groups	The financial services groups included in this report with an Australian ADI as one of its AFS licensees
financial service	Has the meaning given in Div 4 of Pt 7.1 of the Corporations Act
financial services laws	Has the meaning given in s761A of the Corporations Act
incident	A potential significant breach
key decision maker	A person within an AFS licensee who considers and determines whether a breach is significant for the purpose of the breach reporting obligation
key decision-making group	A group of people within an AFS licensee who determine whether a breach is significant for the purpose of the breach reporting obligation
licensee obligations	The obligations of an AFS licensee as set out in s912A and 912B of the Corporations Act and the requirement to be of good fame and character as included in s913B of the Corporations Act
licensing provisions	The Australian financial services licensing regime under Pts 7.6–7.8 of the Corporations Act, including regulations made for the purposes of those parts
major financial groups	The four large Australian ADIs selected for the breach reporting review
Macquarie	Macquarie Group Limited
NAB	National Australia Bank Group of Companies comprising National Australia Bank Limited and its controlled entities (including NAB's Banking and Wealth Licensees)

Term	Meaning in this document
other financial groups	The eight medium-to-small Australian ADIs (including one credit union and two mutual banks) selected for the breach reporting review
PJC	Parliamentary Joint Committee on Corporations and Financial Services
REP 528 (for example)	An ASIC report (in this example numbered 528)
representative	Means: • an authorised representative of the AFS licensee; • an employee or director of the licensee; • an employee or director of a related body corporate of the licensee; or • any other person acting on behalf of the licensee Note: This is a definition contained in s910A of the Corporations Act.
reviewed financial groups	The 12 Australian ADIs selected for the breach reporting review
RG 78 (for example)	An ASIC regulatory guide (in this example numbered 78)
Royal Commission	Royal Commission into misconduct in the banking, superannuation and financial services industry
s912D (for example)	A section of the Corporations Act (in this example numbered 912D), unless otherwise specified
significant breach	A breach or likely breach that an AFS licensee has determined to be significant under s912D(1)(b) of the Corporations Act
significance test	The factors in s912D(1)(b)(i)–(iv) of the Corporations Act that an AFS licensee may use to determine whether a breach or likely breach is significant
Suncorp	Suncorp Group
system	Information technology system
Westpac	Westpac Banking Corporation

Related information

Headnotes

AFS licensee, financial groups, breach, breach management culture, breach reporting, compensation, financial services, investigation, licensee obligations, likely breach, rectification, remediation, significant breach

Regulatory guides

RG 3 *AFS Licensing Kit: Part 3—Preparing your additional proofs*

RG 78 *Breach reporting by AFS licensees*

RG 104 *Licensing: Meeting the general obligations*

RG 105 *Licensing: Organisational competence*

RG 165 *Licensing: Internal and external dispute resolution*

RG 166 *Licensing: Financial requirements*

RG 175 *Licensing: Financial product advisers—Conduct and disclosure*

RG 181 *Licensing: Managing conflicts of interest*

RG 256 *Client review and remediation conducted by licensees*

RG 259 *Risk management systems of responsible entities*

Legislation

Corporations Act, s601FC(1)(l), 912A, 912A(1), 912B, 912D, 912D(1)(b), 912D(1A), 912D(1B), 1311(1)

Reports

REP 515 *Financial advice: Review of how large institutions oversee their advisers*

REP 528 *Responsible entities' compliance with obligations: Findings from 2016 proactive surveillance program*

REP 531 *Review of compliance with asset holding requirements in funds management and custodial services*

Media and other releases

IR 06/14 *Industry embraces early notification of breaches*

13-240MR *ASIC accepts enforceable undertaking from Wealthsure Pty Ltd, Wealthsure Financial Services Pty Ltd and their former CEO*

14-233MR *ASIC urges prompt breach reporting by AFS licensees*

16-045MR *ASIC suspends AFS licence for failing to lodge financial statements*

ASIC forms

Form FS80 *Notification by an AFS licensee of a significant breach of a licensee's obligations*

Other ASIC documents

ASIC Annual Report 2006–07

Improving business through compliance: A regulator's perspective, speech by ASIC Commissioner, Cathie Armour, 4 May 2016

Why breach reporting is important, speech by Deputy Chair, Peter Kell, 16 September 2014

Witness statement of Peter Kell, Exhibit 2.1, prepared for the Royal Commission, 16 April 2018

Opening statement, statement by then ASIC Chairman, Greg Medcraft, PJC, 11 August 2017

Other documents

AFM, *Learning from errors: Towards an error management culture—Insights based on a study in the capital markets*, October 2017

APRA, *Prudential inquiry into the Commonwealth Bank of Australia—Final report*, May 2018

ASIC Enforcement Review, *ASIC Enforcement Review taskforce report*, December 2017

ASIC Enforcement Review, *Position and Consultation Paper 1: Self-reporting of contraventions by financial services and credit licensees*, April 2017

De Nederlandsche Bank, *Supervision of behaviour and culture: Foundations, practice and future developments* (PDF 3.5 MB), September 2015

M Power, S Ashby & T Palermo, *Risk culture in financial organisations: A research report*, Centre for Analysis and Risk Regulation, 2013

Treasury, *Australian Government response to the ASIC Enforcement Review taskforce report*, April 2018

Treasury, *Budget 2016–17: Budget measures—Budget paper no. 2*, May 2016