(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.

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.

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'.

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.

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