Article Information

Author: Andrea Beatty
Service: Banking & Finance
Sector: Financial Services

From breach to remediation – what is taking financial firms so long?

On 25 September, the Australian Securities and Investments Commission (ASIC) released a report on financial services industry compliance with the Corporations Act 2001 (Cth) breach reporting obligation.[1] The report provides licensees with a benchmark for acceptable breach reporting management.

This article will firstly outline the obligation of licensees to report significant breaches, including the current framework for determining significance. The details of the review will then be discussed, including the scope of review and the reasons behind the review. The six key stages of the breach reporting process will then be examined, including ASIC's findings as to the average length of each stage. This article will then conclude by detailing ASIC's ideal breach reporting management standards and how ASIC intends to act on the review.

Published for Lexis Nexis Banking and Finance Law Bulletin Vol 34, No.9

Breach reporting obligation

Breach reporting is a key component of the financial services regulatory regime, with licensees acting as the first line of compliance.

All AFS licensees are required to report significant breaches of their obligations under financial services laws that have occurred or likely to occur to ASIC.[2] A likely breach is one in which a licensee becomes aware that they will be unable to prevent the breach from occurring within 10 business days. Licensees are required to report the breach as soon as practicable within 10 business days of becoming aware of the significant breach.[3]

The concept of 'significant' is a subjective one, with the legislation providing a framework of considerations in determining whether a breach is significant. ASIC's report recognised the ambiguity of the concept of significance.[4] Factors to be considered when determining whether a breach is significant are:

- the number or frequency of similar previous breaches
- the impact on the licensee's ability to provide financial services covered by its licence
- the extent to which the breach indicates that the licensee's arrangements to ensure compliance with their obligations is inadequate, and
- the actual or potential loss to clients or to the licence itself.[5]

The maximum penalty for failing to breach report is $10,500 and/or one year's imprisonment for individuals or $52,500 for body corporates.

ASIC's review

Between 2017 and 2018, ASIC reviewed the breach reporting practices of 12 authorised deposit taking institutions and their associated licensees (**financial groups**), including the Big Four banks (**major financial groups**), AMP, Suncorp and Macquarie Group.[6]

The review considered whether the financial groups had adequate and effective breach reporting processes, complied with

their breach reporting obligations and demonstrated elements of a sound breach management culture.[7]

The review covers 715 significant breaches reported to ASIC by the financial groups between 2014 and 2017.[8]

ASIC's concerns with the current breach reporting processes include financial firms:

- failing to report breaches in a consistent, timely manner
- potentially extending timeframes for internal investigation and reporting processes to delay informing ASIC of significant breaches
- interpreting 'significant' differently
- providing ASIC with breach reports that often do not contain enough information for ASIC to assess and act,[9] and
- lacking constructive engagement with ASIC.[10]

As of the date of the report, ASIC has only once successfully pursued enforcement action for non-compliance with the breach reporting obligations.[11]

From 2016-2017, Treasury conducted a review of ASIC's enforcement regime (**ASIC Enforcement Review**), resulting in a number of recommendations for stronger and clearer rules for breach reporting.[12] The implementation of recommendations made in the 2017 ASIC Enforcement Review have been delayed until the findings of the Royal Commission are taken into account.[13]

Key stages of breach reporting

Stage 1: identification of incident

The report identified that delays in significant breach reporting were primarily caused by licensees failing to identify a potential breach. On average, the time between an incident occurring and the identification of a breach was 1,517 days.[14] As a result, ASIC observed that it receives reports concerning incidents that occurred years prior.[15]

The report found that major financial groups had the longest delay in identifying.[16] At least 256 of the 715 significant breaches reviewed went undetected for more than four years.[17] ASIC stated that these older breaches are generally more difficult to investigate, can be more resource intensive and expensive and may require a stronger regulatory response.[18]

Stage 2: identification to investigation

Once an incident is identified, it must be escalated to senior management. ASIC's report found that financial groups' policies often required reporting within 5 business days. However, the report found many instances where licensees took three times longer to record the incident.[19]

Financial groups took an average of 22 days to record an incident in their systems after identification of a breach.[20] It then took a further 28 days on average before the financial groups commenced an investigation.[21] Although the majority of breach investigations occurred within a 10-day period, 98 of the reviewed breaches took more than 40 days for an investigation to commence.[22]

Stage 3: investigation to breach report

Stage 3 of the breach reporting process involves an examination of the incident to determine whether the incident is a breach, and whether it is significant. The obligation to lodge a report with ASIC only arises after the decision maker determines that there has been a significant breach.[23]

Of the 715 significant breaches reviewed by ASIC, 110 were reported more than 10 business days after becoming aware of the breach.[24] The majority of these delayed reports were between one and three days late.[25]

The average time for a financial firm to investigate and lodge a report was 128 days,[26] with major financial firms double that of other groups with an average investigation time of 150 days.[27] One of the major banks' average wait time between investigation and breach reporting was 213 days.[28]

The report found that legal advice is a factor that can extend the length of an investigation, with firms often requesting advice on the significance of a breach.[29] 531 of the reviewed breaches involved legal advice.[30]

The report found also that the subjectivity of the significance test affects the consistency and number of significant reports.[31] The report supports the recommendation from the ASIC Enforcement Review that significant breaches must be reported within 30 days when a licensee becomes aware or has reason to suspect that a breach has, may have or may

occur.[32]

Stage 4: communication with customers

Stage 4 looks to the speed at which licensees respond to the breach and communicate this with the affected customers following the investigation. Financial groups communicated with affected customers in 364 of the 715 reviewed breaches.[33]

ASIC's investigation found that communication with customers appears to be given a lower priority by licensees that implementing a process or system change.[34] Major financial groups took an average of 218 days to communicate with customers following their investigation, whilst other groups took 29 days to communicate.[35] One of the major banks took an average of 299 days to communicate with customer.[36]

The report's data indicated that some licensees proactively began communicating with their customers prior to the end of their investigation.[37]

Stage 5: payment to customers

Stage 5 of the breach reporting processes involves how quickly licensees respond to the breach and remediate affected customers.

279 of reviewed breaches involved a financial loss to consumers. When providing responses to ASIC, licensees had commenced financial remediation to consumers affected by 260 breaches.[38]

It is not unusual for licensees to complete their investigation before remediating customers. ASIC found that although this process allows licensees to ensure they identify all affected customers, it leads to delays in commencing investigations.[39] Major financial groups took an average of 251 days to make direct payment after the end of their investigation,[40] with other financial firms taking an average of 84 days to make their first payments.[41] One major bank took the longest to remediate customers, taking an average of 352 days.[42]

ASIC identified the total financial loss to consumers for the breach reports to be approximately $497 million, being an average of $1.8 million per significant breach. [43] Licensees must ensure that they do not make a financial gain from the breach, with ASIC reinforcing that affected customers should be returned to their original position, as if the breach never occurred.[44]

Stage 6: process and/or system change

Stage 6 involves licensees responding to the significant breach and implementing a process and/or system change following the end of the investigation. The review found that 415 significant breaches led to a process change and 204 breaches led to a system change.[45]

Of the 334 instances where the first process change occurred after the licensee commenced their investigation, financial groups took an average of 42 days to implement the first process change.[46] Of the major financial firms, AMP was the most responsive to process changes, beginning process change on average 53 days prior to the end of its investigation.[47]

Of the 117 instances where the first system change occurred after the licensee commenced their investigation, financial groups took an average of 68 days to implement the first system change.[48] System changes generally take longer than process changes due to IT requirements.[49]

Stage 7: accountability

Stage 7 details at what speed licensees respond to the breach and implement consequence management, relative to their end of their investigation.

According to the financial groups, there were 296 instances where they attributed a root cause of a significant breach to their staff and/or management and only 100 instances of consequence management being applied to those responsible for the breach.[50]

Consequence management is real and meaningful consequences for management and staff who have failed to follow procedures.[51] The two most common consequences were a reduction in bonuses and adverse performance ratings.[52] Financial groups took an average of 22 days to commence consequent management following an investigation for responsible staff, and 66 days for management.[53]

Ideal breach management culture

ASIC made a general observation that reviewed financial groups did not give adequate priority to the management of breaches relative to other business priorities.[54] The report identified what features ASIC believes amount to a sound breach management culture.

Fast detection of breaches

The speed at which a breach is detected limits the impact it has on customers. ASIC believes that financial groups have written policies in place to prioritise reporting breaches.[55] However, ASIC's review highlighted that financial groups were generally not able to detect incidents quickly. ASIC believes the disconnect between sound policies and poor data could be a result of ineffective implementation of policies, staff not proactively looking for risks and/or management not actively promoting the desired behaviour.[56]

Compliance measures allow appropriate information to be captured

ASIC believes an important component of a sound breach management culture are compliance measures that ensure key information about breaches and incidents are consistently captured.[57] ASIC's review found that breach information was not always properly recorded and often recorded across multiple databases.[58]

Investigation of breaches is prioritised

Financial groups should prioritise the investigation of breaches so that the root cause of the problem is identified and corrected, and staff are not given 'mixed messages'.[59] ASIC's findings of low levels of oversight by senior management indicated a low priority given to investigating breaches, signaling to staff that the institution does not prioritise timely investigations.[60]

Customer outcomes following breaches are monitored and remediation is prioritised

ASIC found that the long timeframes for communicating with, and payment to, customers indicates that customers are not being prioritised within financial groups.[61] In its review of documents, ASIC found remediation was perceived as a distraction for management and from core business.[62] ASIC stated that this perception is not in line with the financial groups' stated values of putting the interests of customers first and resolving problems promptly.[63]

Learning from incidents and breaches

ASIC's review highlighted that licensees may not be maximizing opportunities for improvement. Only 28% of breach reports documented 'lessons learned', with ASIC finding many of these did not demonstrate a thorough analysis of the problem but instead merely provided a summary of key information about the breach.[64]

ASIC also found that only 4.8% of breaches involved financial groups sharing 'lessons learned' reports across other business units or licensees within the financial group.[65] ASIC believes that this prevents licensees taking proactive steps to determine whether the breach could occur in other aspects of the financial group's business.[66]

ASIC's actions

ASIC intends to maintain its supervision of licensees, including potential intervention in consumer remediation from significant breaches.[67] This will form part of their close and continuous monitoring of the major financial firms, with on-site monitoring commenced in October 2018. ASIC's on-site monitoring will involve supervisory staff monitoring the institutions' governance and compliance with laws.[68]

ASIC's new Regulatory Portal will assist ASIC in more complex data analysis to identify systemic issues in breach reporting processes.[69] The Portal will allow licensees to submit breach reports and updates from 2019.[70] ASIC also stated that they will update relevant regulatory guides, including RG 78 *Breach reporting by AFS licensees*.[71]

As previously mentioned, ASIC is advocating for legislative reform to extend the reporting period to 30 days. This change will mean licensees are required to report when they become aware of or have reason to suspect that a breach has occurred, may have occurred or may occur, rather than when they determine a significant breach has occurred.[72]

Summary

ASIC's report into Australian financial services licensees' breach reporting highlights areas for improvement in significant breach reporting. ASIC intends to continue supervision of licensees to ensure compliance with their breach reporting obligations and the making of timely remediation to customers.

[1] Australian Securities and Investment Commission (ASIC), 'Review of selected financial services groups' compliance with the breach reporting obligation' (Report No 594, 2018).

[2] *Corporations Act 2001* (Cth) s912D(1B).

[3] ASIC, above n 1, 4[1].

[4] Ibid 19[51].

[5] *Corporations Act 2001* (Cth) s912D(1)(b).

[6] ASIC, above n 1, 6.

[7] Ibid 6[16].

[8] Ibid [18].

[9] Ibid 20[55].

[10] Ibid [56].

[11] Top Quartile Management Ltd were convicted and fined for failing to provide ASIC with significant breach reports.

[12] ASIC, above n 1, 21[60].

[13] Ibid 22[66].

[14] Ibid 24.

[15] Ibid 27[87].

[16] Ibid 116.

[17] Ibid 29[92].

[18] Ibid [93].

[19] Ibid 37[134].

[20] Ibid 38[136].

[21] Ibid [139].

[22] Ibid 38-39.

[23] Ibid 41[156].

[24] Ibid 41.

[25] Ibid.

[26] Ibid [157].

[27] Ibid [158].

[28] Ibid 117.

[29] Ibid 44[177].

[30] Ibid 45.

[31] Ibid 48[192].

[32] Ibid 49[199].

[33] Ibid 67[307].

[34] Ibid [306].

[35] Ibid 68[309].

[36] Ibid 118.

[37] Ibid 68[312].

[38] Ibid 72[334].

[39] Ibid [336].

[40] Ibid 73[338].

[41] Ibid [338].

[42] Ibid 118.

[43] Ibid 77[357].

[44] Ibid [360].

[45] Ibid 82[386].

[46] Ibid [388].

[47] Ibid 84[398].

[48] Ibid 82[389].

[49] Ibid 84[400].

[50] Ibid 86[412].

[51] Ibid 87[415].

[52] Ibid 88[420].

[53] Ibid 87[413].

[54] Ibid 96[463].

[55] Ibid 97[470].

[56] Ibid 98[472].

[57] Ibid 99[477].

[58] Ibid 100[480].

[59] Ibid 101[483].

[60] Ibid [485].

[61] Ibid 103[491].

[62] Ibid [492].

[63] Ibid [493].

[64] Ibid 104[497].

[65] Ibid [499].

[66] Ibid.

[67] Ibid 106[504].

[68] Ibid 107[505].

[69] Ibid [506].

[70] Ibid 108[512-513].

[71] Ibid 107[507].

[72] Ibid [509].