



ASIC

Australian Securities & Investments Commission

REGULATORY GUIDE 78

Breach reporting by AFS licensees

First issued October 2004

Reissued May 2006

Note: Cross-references in this guide were updated in February 2008 to reflect ASIC's current regulatory document framework.

What this guide is about

1 This document provides general guidance on your obligation as an Australian financial services (AFS) licensee under s912D of the *Corporations Act 2001* (Corporations Act) to report to ASIC certain breaches or likely breaches of your obligations under the financial service laws.

Note 1: There are several other obligations requiring you to report specific matters to ASIC. These include, for example, where you are a body regulated by APRA and you cease to hold that status (e.g. where you are a superannuation trustee and you have your approval as a trustee revoked by APRA, see Pro Forma 209 [PF 209] condition 9), or where you become aware of a change in control of the licensee (see reg 7.6.04(1)(i)). These other obligations to report matters to ASIC are not dealt with in this guide.

Note 2: This guide does not deal with the breach reporting obligations imposed on auditors by s311, 601HG or 990K: see Regulatory Guide 34 *Auditors' obligations: reporting to ASIC* (RG 34) for further information.

2 We also provide some general guidance on the processes we follow after we receive a notification by an AFS licensee of a breach, as required under s912D. In doing so we aim to enhance the transparency of our processes by explaining how we deal with these notifications.

3 This guide should be read in conjunction with our policy statements and other guidance on how we administer Chapter 7 of the Corporations Act, including Regulatory Guide 104 *Licensing: Meeting the general obligations* (RG 104) and Regulatory Guide 105 *Licensing: Organisational competence* (RG 105).

4 Section 1 of this guide provides some general guidance in a question and answer format.

5 Section 2 describes what we do with your s912D reports after we receive them. It explains that we follow a process for assessing breach notifications and offers some guidance on what you can do to help us resolve any issues arising from the compliance breach.

6 We have published this document to provide general guidance to industry. It is not intended to describe how to comply with the breach reporting obligations in every situation. The guide does not consider all the issues that may be relevant to determining whether you must give a breach report to ASIC. For simplicity, this guide also paraphrases some aspects of the law.

Contents

What this guide is about.....	2
Section 1: When you must report a breach	4
Q1 What breaches or likely breaches must you report?.....	5
Q2 What does ‘likely to breach’ mean?	6
Q3 What does ‘significant breach’ mean?	6
Q4 What arrangements should you have in place to record and report breaches?.....	11
Q5 How do you report a breach?	13
Q6 When must you report a breach?	14
Q7 What will we do with the information in a breach report?	15
Q8 What is the penalty for not reporting a breach?	15
Q9 If you are a responsible entity, do you need to comply with the breach reporting requirements in s912D and 601FC(1)(l)?	15
Section 2: How we deal with breach notifications.....	17
Relevant factors	17
Possible enforcement action	18
Mitigating factors.....	19
Public comment	20
Key terms.....	21
Related papers	22

Important note: This publication is issued as a general guide to a licensee’s obligation to report to ASIC certain breaches of the law, and to how we apply our administrative enforcement powers. It is your responsibility to determine your obligations under the *Corporations Act 2001* and *Corporations Regulations 2001*. Examples provided in this guide are purely for illustration purposes; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

This guide does not constitute legal advice. We encourage you to seek your own professional advice to find out how the Corporations Act applies to you.

Section 1: When you must report a breach

1.1 As an AFS licensee, if:

- you breach any of the specified obligations; or
- you are likely to breach any of the specified obligations; and
- that breach or likely breach is ‘significant’ having regard to a number of prescribed factors,

then you must give a written report to ASIC as soon as practicable, and in any case within 5 business days of becoming aware of the breach or likely breach: s912D.

1.2 This section of the guide explains:

- What breaches or likely breaches must you report?
see paragraphs 1.3–1.6
- What does ‘likely to breach’ mean?
see paragraphs 1.7–1.8
- What does ‘significant breach’ mean?
see paragraphs 1.9–1.14
- What arrangements should you have in place to record and report breaches?
see paragraphs 1.15–1.20
- How do you report a breach?
see paragraphs 1.21–1.23
- When must you report a breach?
see paragraphs 1.24–1.26
- What will we do with the information in a breach report?
see paragraphs 1.27–1.28
- What is the penalty for not reporting a breach?
see paragraph 1.29
- If you are a responsible entity, do you need to comply with the breach reporting requirements in s912D and 601FC(1)(l)?
see paragraphs 1.30–1.37

Q1 What breaches or likely breaches must you report?

1.3 Section 912D requires you to report to ASIC any significant breach or likely breach of:

- your obligations under s912A and 912B (other than the obligation under s912A(1)(c)); and
- your obligation under s912A(1)(c) to comply with certain financial services laws.

Table 1: Summary of your obligations

Your obligations under s912A and 912B	Your obligation under s912A(1)(c)
<p>You must:</p> <ul style="list-style-type: none"> • do all things necessary to ensure that the financial services covered by your AFS licence are provided efficiently, honestly and fairly • comply with the conditions on your licence • have adequate resources to provide the financial services covered by your licence and to carry out supervisory arrangements (unless you are a body regulated by APRA: see paragraph 1.4) • be competent to provide the financial services covered by your licence • have trained and competent representatives • take reasonable steps to ensure that your representatives comply with the financial services laws • have a dispute resolution system for retail clients • have adequate risk management systems (unless you are a body regulated by APRA: see paragraph 1.4) • have compensation arrangements for retail clients. 	<p>You must comply with the following financial services laws:</p> <ul style="list-style-type: none"> • Chapter 5C of the Corporations Act (managed investment schemes) • Chapter 6 of the Corporations Act (takeovers) • Chapter 6A of the Corporations Act (compulsory acquisitions and buy-outs) • Chapter 6B of the Corporations Act (rights and liabilities in relation to Chapter 6 and 6A matters) • Chapter 6C of the Corporations Act (information about ownership of listed companies and managed investment schemes) • Chapter 6D of the Corporations Act (fundraising) • Chapter 7 of the Corporations Act (financial services and markets) • Chapter 9 of the Corporations Act (miscellaneous), but only as it applies in relation to the chapters of the Corporations Act listed above • Division 2 of Part 2 of the ASIC Act (unconscionable conduct and consumer protections in relation to financial services) • other Commonwealth Acts specified in reg 7.6.02A (see note below) in so far as they cover conduct relating to the provision of financial services.

Note: The Commonwealth Acts specified in reg 7.6.02A are the *Banking Act 1959*, *Financial Sector (Collection of Data) Act 2001*, *Financial Sector (Shareholdings) Act 1998*, *Financial Sector (Transfer of Business) Act 1999*, *Insurance Acquisitions and Takeovers Act 1991*, *Insurance Act 1973*, *Insurance Contracts Act 1984*, *Life Insurance Act 1995*, *Retirement Savings Accounts Act 1997*, *Superannuation Industry (Supervision) Act 1993* and *Superannuation (Resolution of Complaints) Act 1993*.

Bodies regulated by APRA

1.4 If you are a body regulated by APRA, there is no obligation under s912A of the Corporations Act in relation to adequate resources or risk management systems. Similarly, these obligations are not included as AFS licence conditions for bodies regulated by APRA. However, similar obligations are contained in Commonwealth legislation regulated by APRA and in prudential standards and rules determined by APRA under that legislation.

1.5 Commonwealth legislation regulated by APRA is listed in reg 7.6.02A (see note under Table 1 on previous page), and therefore a breach of this legislation may be a breach of your obligation to comply with a financial services law.

1.6 If you are a body regulated by APRA and you breach the APRA prudential standards or rules, this may also be a breach of your obligation under s912A(1)(c) to comply with a financial services law, but only if compliance with the prudential standards or rules is required by the Commonwealth legislation specified in reg 7.6.02A and the breach arises from conduct relating to the provision of financial services.

Q2 What does ‘likely to breach’ mean?

1.7 You must report to us not only when you breach an obligation, but also when you are ‘likely to breach’ an obligation. You are likely to breach an obligation if, and only if, you are no longer able to comply with the obligation: s912D(1A).

1.8 For example, you may become aware that on a future date your overdraft facility will be closed and you will no longer be able to comply with your base level financial requirements. If you do not have an alternative means of meeting the financial requirements at this time, you will become aware that you are likely to breach your obligations in relation to the financial requirements.

Q3 What does ‘significant breach’ mean?

1.9 You do not have to report all breaches or likely breaches. You only have to report those that are ‘significant’. The term ‘significant’ is not defined in the Corporations Act. If a breach is not significant, you must address that breach even though you may not have to report it to ASIC.

Note: For example, where there is a non-significant breach that requires compensation to clients or needs to be rectified in some other way, we expect you to take appropriate action even though you are not required to report the breach.

1.10 Whether a breach or likely breach is significant or not will depend on the individual circumstances of the breach. We consider that the nature, scale and complexity of your financial services business might also affect whether a particular breach is significant or not. You will need to decide whether a breach (or likely breach) is significant and thus reportable. Where you are not sure whether a breach or likely breach is significant, we encourage you to report the breach.

1.11 You must have regard to a number of factors specified in s912D(1)(b) when determining whether a breach or likely breach is significant: see Table 2 below. A breach may be significant where only one of the factors applies to your circumstances, or where there is a combination of factors.

1.12 We expect that, at the time that you become aware of *any* breach or likely breach, you will consider the circumstances and impact of that breach or likely breach in light of each of these factors to determine whether the breach is significant. We also expect you to document this process.

Table 2: Factors that determine whether a breach (or likely breach) is ‘significant’

<p>The number or frequency of similar previous breaches: s912D(1)(b)(i)</p>	<p>The greater the number or frequency of similar breaches, the more likely the new breach will be significant. We also consider that the repeat of a breach may indicate a continuing underlying systemic problem.</p> <p>Note: For example, you may consider a failure to comply with the requirement to notify ASIC of the appointment of an authorised representative within the 15 business days allowed by s916F to be a minor breach that does not require a breach report (provided that you have rectified the breach by providing the notification to ASIC). However, if you are habitually late in giving us these notifications, or other notifications required under the Corporations Act, a further occurrence of this type of breach may be significant.</p> <p>If minor breaches of this type repeatedly occur, you may become aware that you can no longer comply with your notification obligations under the financial services laws (e.g. because you have inadequate compliance arrangements, or inadequate technological or human resources). This may therefore also amount to a likely significant breach.</p>
<p>The impact of the breach or likely breach on your ability to provide the financial services covered by your licence: s912D(1)(b)(ii)</p>	<p>If a breach or likely breach reduces your ability or capacity to provide the financial services covered by your licence, it may be significant. For example, we consider that a breach of the financial requirements of your licence conditions may be significant. If these minimum requirements are not met, you may not have the financial ability or capacity to provide the financial services covered by your licence.</p> <p>If the breach or likely breach will not affect your ability or capacity to provide the financial services covered by your licence (as in the earlier example of a late notification to ASIC), it may still be significant having regard to one or more of the other factors.</p>

<p>The extent to which the breach or likely breach indicates that the licensee's arrangements to ensure compliance with those obligations is inadequate: s912D(1)(b)(iii)</p>	<p>If the breach or likely breach indicates that your arrangements to ensure compliance are inadequate only in an isolated instance, it may not be significant. However, if the breach or likely breach indicates broader inadequacies in your compliance arrangements, it is more likely to be significant and, if so, you should report it to us.</p> <p>Occasional and minor breaches do not of themselves mean that your compliance arrangements are inadequate. We recognise that compliance arrangements are unlikely to ensure full compliance with every aspect of the law at all times. However, this factor requires you to consider whether a breach indicates that your compliance arrangements are inadequate. We expect that under this factor you would ask yourself questions such as how long it took to discover the breach and to what extent the compliance arrangements helped in identifying the breach.</p>
<p>The actual or potential financial loss to your clients, or you, arising from the breach or likely breach: s912D(1)(b)(iv)</p>	<p><i>Loss to clients</i></p> <p>We consider that any breach or likely breach of your obligations that causes actual or potential financial loss to clients is likely to be significant. Of course, where the breach is an isolated or occasional breach, the amount of the loss involved is minimal and immaterial, and the breach affects a very small number of clients, the breach is less likely to be significant.</p> <p>Note: For example, where you breach s1017E by failing to pay client money into an appropriate account for several days after it was required to be paid, you may owe that client a relatively small amount of interest. This breach, on its own, is not likely to be significant even though it may involve a small financial loss to a client. On the other hand, where such a breach involves more than one client, or a larger amount of money, it is more likely to be significant.</p> <p>You must rectify breaches where that is appropriate, even where those breaches are not reported because they are not significant. In the above example, the amount of interest owed by you must be paid to the client, even if the breach need not be reported.</p> <p><i>Loss to the licensee</i></p> <p>If the breach or likely breach causes actual or potential loss to you, the breach may or may not be significant, depending on the size of the loss as compared with the overall business.</p> <p>However, if the actual or potential financial loss to you resulting from the breach causes non-compliance with your financial requirements under your licence conditions, we consider that the breach is likely to be significant. Such loss would also be likely to impact on your ability to provide the financial services covered by your licence.</p>
<p>Any other matters prescribed by regulations: s912D(1)(b)(v)</p>	<p>As at the date of publication of this guide, there were no relevant regulations. You should check to see whether the regulations have specified any further factors.</p>

Examples of breaches that may be significant

1.13 Table 3 sets out some examples of breaches that we consider may be significant.

Note: These examples are for illustrative purposes only, and do not purport to limit the types of breaches that must be reported to ASIC or the reasons why a particular breach might be considered significant. It is your responsibility to decide if a breach or likely breach is significant, taking into account the particular circumstances of the case.

Table 3: Examples of breaches that *may* be significant

<p>Example 1: Failure to maintain professional indemnity (PI) insurance, or an appropriate level of PI insurance cover</p>	<p>If you are required to maintain PI insurance as a condition of your AFS licence, your failure to maintain that insurance will be a breach of your obligations to comply with your licence conditions and the financial services laws.</p> <p>We consider that a failure to maintain PI insurance is very likely to be a significant breach of these obligations because:</p> <ul style="list-style-type: none"> • it may result in actual or potential financial loss to your clients; and • allowing PI insurance to lapse, or maintaining an inadequate level of PI insurance cover, may indicate that your arrangements for ensuring compliance with your obligations are inadequate.
<p>Example 2: Failure to prepare cash flow projections</p>	<p>Generally, you must prepare cash flow projections as a condition of your AFS licence (unless, for example, you are APRA regulated). Failure to do so will be a breach of your obligations to comply with licence conditions, and may indicate a breach of your obligation to have adequate risk management systems and your obligation to have available adequate financial resources to provide the financial services covered by your licence.</p> <p>ASIC sets minimum financial resource requirements to promote appropriate financial risk management and ensure that cash shortfalls do not put compliance with the licensee obligations at risk.</p> <p>We consider that a failure to prepare cash flow projections is likely to be a significant breach of these obligations. It is likely to indicate that your arrangements to ensure compliance with your obligations are inadequate. Such breaches may also indicate that you do not have the ability to provide the financial services covered by your licence.</p>
<p>Example 3: Previously undetected breaches</p>	<p>A breach of a s912A or 912B obligation may indicate previous breaches of those obligations that have not been detected.</p> <p>We consider that your failure to detect previous breaches may be significant (even if those previous breaches were only minor) because it could indicate that you do not have adequate arrangements to ensure compliance with your obligations.</p>

<p>Example 4: Provision of inappropriate advice by representatives</p>	<p>If your representatives provide inappropriate financial product advice to your clients, there may be breaches of your obligations to comply with the relevant financial services laws, and to take reasonable steps to ensure that your representatives comply with those laws.</p> <p>Where there is a breach of these obligations because your representatives have provided inappropriate advice and the breaches are of a sufficient scale or have occurred with a sufficient degree of regularity, the breaches may be significant because they are more likely to:</p> <ul style="list-style-type: none"> • have some impact on your ability to provide the financial services covered by your licence; • indicate that your arrangements to ensure compliance with your obligations are inadequate; and • involve actual or potential financial loss to your clients or to you.
<p>Example 5: Representatives operating outside the scope of your AFS authorisations</p>	<p>If your representatives provide financial services outside the scope of your AFS authorisations, there may be breaches of your obligations to:</p> <ul style="list-style-type: none"> • comply with the financial services laws, and take reasonable steps to ensure that your representatives comply with those laws; • have available adequate resources to carry out supervisory arrangements; • ensure that your representatives are adequately trained and competent; and • have adequate risk management systems. <p>We consider that the provision of unauthorised financial services by a representative is likely to be a significant breach of these obligations because such breaches may:</p> <ul style="list-style-type: none"> • impact on your ability to provide the financial services covered by your licence; • indicate that your arrangements to ensure compliance with your obligations are inadequate; and • involve actual or potential financial loss to your clients or to you.
<p>Example 6: Fraud in the provision of financial services by a representative</p>	<p>We consider that fraud by a representative, and your failure to prevent fraud by a representative, is likely to involve a significant breach of each of your obligations in s912A because such breaches will:</p> <ul style="list-style-type: none"> • have some impact on your ability to provide the financial services covered by your licence; • indicate that your arrangements to ensure compliance with your obligations are inadequate; and • involve actual or potential financial loss to your clients or to you.

Examples of breaches that may not be significant

1.14 Table 4 sets out some examples of breaches that we consider may not be significant.

Note: These examples are for illustrative purposes only, and do not purport to limit the types of breaches that must be reported to ASIC or the reasons why a particular breach might be considered significant. It is your responsibility to decide if a breach or likely breach is significant, taking into account the particular circumstances of the case.

Table 4: Examples of breaches that *may not* be significant

<p>Example 1: Provision of inappropriate advice by representatives</p>	<p>If a representative of yours provides inappropriate financial product advice to a client on one occasion only, this is unlikely to be a significant breach where it is an isolated incident that does not indicate a systemic breakdown of your compliance systems and the client is not expected to suffer material loss.</p> <p>However, if inappropriate advice is provided on multiple occasions or if the amount of client loss is substantial, the breach is more likely to be significant and reportable to ASIC.</p>
<p>Example 2: Unit pricing errors</p>	<p>If you make a unit pricing error of an immaterial amount involving one client only, this breach of your obligations under Chapter 5C is not likely to be significant and therefore will not need to be reported.</p> <p>Where the unit pricing error involves more than one client or shows a systemic problem, then the breach is more likely to be significant and, if so, will need to be reported to ASIC.</p>

Q4 What arrangements should you have in place to record and report breaches?

1.15 If you fail to properly consider whether every breach or likely breach that comes to your attention is significant by having regard to the s912D(1)(b) factors, you run the risk of failing to identify a breach or likely breach that is significant and must be reported to ASIC. Failure to report a significant breach or likely breach in accordance with s912D is in itself a breach of your obligation to comply with the financial services laws.

1.16 We consider that a failure to report a breach (or likely breach) that is significant is likely, in itself, to be a significant breach. This is because it indicates that your arrangements to ensure compliance with your obligations may be inadequate.

1.17 To ensure compliance with the obligation to report all significant breaches or likely breaches, you should have a clear, well-understood and documented process for:

- identifying breaches or likely breaches of your obligations;
- ensuring that the relevant people responsible for compliance are aware of those breaches or likely breaches;

- determining whether identified breaches or likely breaches are significant;
- reporting to ASIC those breaches or likely breaches that are significant;
- where appropriate, rectifying the breach or likely breach; and
- ensuring that arrangements are in place to prevent the recurrence of the breach or likely breach.

Breach register

1.18 The Corporations Act does not require you to maintain a breach register. However, we consider that, in practice, you will need to use a documented breach register to ensure that you have adequate arrangements in place to comply with your obligation under the Act to identify and report all significant breaches and likely breaches.

1.19 To ensure that you can satisfy yourself and us that you have done all things necessary to properly identify, report and deal with breaches or likely breaches, we consider that a breach register should contain the following information:

- the date of the breach (or the date on which you are likely to breach the relevant obligation) and the date on which you became aware of the breach or likely breach. If the breach is significant, you will be required to report it to ASIC within 5 business days of the latter date, and accordingly should have a record of that date to ensure timely reporting;
- a brief description of the breach or likely breach;
- how the breach or likely breach was identified (e.g. whether it was identified through your compliance arrangements or as a result of a client complaint);
- the process and responsibilities for handling the breach or likely breach, and a description of how the breach or likely breach is to be handled (i.e. steps to be taken to rectify the breach and prevent recurrence of the breach);
- a consideration of each of the factors in s912D(1)(b). You should have a record of matters that you have considered in determining whether each breach or likely breach is significant and therefore required to be reported to ASIC;
- the date a breach was reported to ASIC (where appropriate); and
- the date the breach was rectified (where appropriate).

1.20 You will need to consider how best to keep these documents or records (e.g. they may be kept electronically). Keeping documents and records helps you to demonstrate, to us and to yourself, that you know

whether or not you are complying with your obligations as a licensee, including the obligation to report significant breaches to ASIC. For more information, see [PS 164].

Q5 How do you report a breach?

1.21 A breach must be reported to ASIC *in writing*. Although there is no prescribed form for reporting a breach, to help you provide the information we need to assess the breach, we have provided a template form (FS80) for lodging written breach reports on our website at **www.asic.gov.au**. You may lodge your report in another form if that is more appropriate to your circumstances.

1.22 You can report a breach or likely breach of your obligations by giving us a written report that sets out:

- the date of the breach, or if it is a likely breach, the date from which you anticipate that you will no longer be able to comply with your obligations;
- a description of the breach (i.e. the obligation that has been breached or is likely to be breached, including references to the section of the Act that sets out that obligation, and any relevant financial services law or AFS licence condition);
- a description of why the breach is significant (i.e. a description of the factors in s912D(1)(b) that you considered);
- the duration of the breach;
- how the breach or likely breach was identified;
- if an authorised representative is involved, that authorised representative's name, representative number and, if the representative's authorisation has been revoked, all last known contact details;
- whether the breach has been rectified, or any steps that have been taken to remedy the breach or likely breach, including any compensation paid to clients. If ongoing steps are being taken to rectify the breach or likely breach, you should indicate when you expect to provide a report to us on your progress in rectifying the breach or likely breach; and;
- any steps that have been or will be taken to ensure future compliance with the obligation.

1.23 If you do not have information about any of these matters at the date of reporting, you should include the information you do have in your written breach report and supplement it by lodging further information as it becomes available.

How to lodge your breach report

- You can lodge the written breach report at any ASIC office (but preferably the office in the State or Territory where you live). The report should be addressed to **'Financial Services Regulation, Regulatory Compliance'**. For contact details of ASIC offices, go to www.asic.gov.au/asicoffices.
 - Or you can email the written breach report to ASIC at fsr.breach.reporting@asic.gov.au.
-

Q6 When must you report a breach?

1.24 You must give the written breach report to ASIC as soon as practicable, and in any case within 5 business days of becoming aware of either:

- the breach—if the breach had already occurred when you discovered it; or
- the likely breach—if you become aware that you will no longer be able to comply with an obligation before the breach has actually occurred.

1.25 The reporting period starts on the day you became aware of a breach or likely breach that you consider could be significant. We will administer this requirement as meaning that you become aware of a breach or likely breach when a person responsible for compliance becomes aware of the breach. We expect your internal systems to make the relevant people aware of breaches in a timely and efficient manner.

Note: In providing up to 5 days to report a breach, the law allows you to make a genuine attempt to find out what has happened and decide whether the breach is significant. In responding to the breach notification, we will take into account any delays or obfuscation in reporting.

1.26 In making your breach report, you should *not* wait until after:

- you have completed all possible avenues of investigation to satisfy yourself whether or not the breach or likely breach is significant;
- the breach or likely breach has been considered by your Board of Directors;
- the breach or likely breach has been considered by your internal or external legal advisers;
- you have rectified (where appropriate), or you have taken steps to rectify, the breach or likely breach; or
- in the case of a likely breach, the breach has in fact occurred,

since these extended processes may defeat the law's intention for ASIC to be informed of significant breaches as soon as practicable.

Q7 What will we do with the information in a breach report?

1.27 We will consider the information in a breach report to determine whether it is necessary or appropriate to take any further action. We do not take action on all matters reported to us.

Note: For further information about what we do when we receive a breach notification, see Section 2 of this guide.

1.28 Breach notifications play a very important role in our oversight of the financial services industry. Apart from alerting us to significant breaches of the law, they also provide us with valuable information to help us identify emerging trends of non-compliance. From time to time we may publish information about trends in breach reporting.

Q8 What is the penalty for not reporting a breach?

1.29 The maximum penalty for not reporting a significant breach or likely breach within 5 business days of becoming aware of the breach or likely breach is, for an individual, \$5500 or imprisonment for one year, or both. For a company, the maximum penalty is \$27,500: s1311, 1312 and Schedule 3.

Q9 If you are a responsible entity, do you need to comply with the breach reporting requirements in s912D and 601FC(1)(I)?

1.30 Responsible entities are subject to breach reporting requirements under both s912D and 601FC(1)(I).

1.31 A responsible entity should be aware of both requirements for reporting breaches and apply each set of requirements to the relevant breach. If either requirement for reporting a breach to ASIC applies to the relevant breach, then you should report that breach.

1.32 If the breach is reported under either test you do not have to notify us separately about the same issue under the other section.

What is the requirement in s601FC(1)(I)?

1.33 If you are a responsible entity, you are required under s601FC(1)(I) to report to ASIC any breach of the Act that:

- relates to the scheme; and
- has had, or is likely to have, a material adverse effect on the interests of members,

as soon as practicable after becoming aware of the breach.

1.34 This requirement is more limited than the breach reporting requirement in s912D. In particular, as a responsible entity, under this requirement you are only required to report to ASIC a breach (i.e. you are not required to report likely breaches):

- that relates to the scheme operated by you; and
- that has had, or is likely to have, a material adverse effect on the interests of members.

1.35 ‘Material adverse effect’ is not defined in the Corporations Act. However, we consider that an adverse effect will be material if it is of significance and not merely trivial or inconsequential: *Minister for Immigration v Dela Cruz* (1992) 34 FCR 348; 110 ALR 367 at 371.

1.36 Breach reports under this requirement must be made as soon as practicable, but there is no maximum time limit as in s912D.

1.37 It is an offence for a person to be intentionally or recklessly involved in a responsible entity contravening this requirement: s601FC(6). The maximum penalty is, for an individual, \$220,000 or imprisonment for 5 years, or both. For a company, the maximum penalty is \$1,100,000: s1311(2), 1312 and Schedule 3.

Note: For example, if you, as the responsible entity of a scheme, fail to comply with the scheme’s compliance plan, you must consider whether you are required to report that breach to ASIC under s601FC(1)(l). If you decide that you are not required to report the breach because, for example, the particular breach has not had, and is not likely to have, a materially adverse effect on the interests of members, you must consider whether you are required, as an AFS licensee, to report the breach to ASIC under s912D. A failure to comply with a scheme’s compliance plan may be significant, and therefore reportable under s912D, because it may indicate that your arrangements to ensure compliance with the financial services laws are inadequate.

Section 2: How we deal with breach notifications

2.1 When we receive your breach report we assess it and decide what, if any, action on our part is necessary. Only a small proportion of breach notifications under s912D result in enforcement action. However, enforcement action is a potential response to a notification of a significant breach by an AFS licensee.

What we do with your breach report

We follow a standard procedure when we receive a breach notification. It comprises the following steps:

- On receipt of the breach report, we acknowledge it.
 - If we have insufficient information to form a view, we will ask you for further information.
 - When we have all the information we need, we'll decide whether any further action on our part is necessary.
 - If the factors identified in paragraph 2.2 are satisfied, we may simply inform you that we intend not to make further inquiries about the matter.
 - We may contact you to discuss how to improve your compliance procedures. This may involve working with you to address continuing compliance issues and determining how to reverse or minimise any damage resulting from the breach.
 - In appropriate circumstances, we may resolve outstanding compliance concerns by conducting a formal surveillance to test your compliance procedures or check whether there is a systemic compliance problem.
-

Relevant factors

2.2 When we receive a breach notification, we seek to ensure that:

- you have made a genuine attempt to comply with the law and your breach reporting obligations;
- the causes of the breach have been identified and, if readily rectified, addressed so that it is unlikely to recur;
- in other cases, a plan for rectifying the compliance failure has been developed and submitted to us;

- the consequences (particularly to consumers) are able to be dealt with comprehensively (e.g. by compensation and communication);
- there has been no undue delay in notifying us; and
- if the circumstances suggest there are some more significant compliance issues within your business, they are identified.

2.3 If we can be satisfied of the factors in paragraph 2.2, this will influence our response to the breach. In some cases we may not need to take any further action. If you involve us early by notifying us as soon as the breach is detected, and we are satisfied with the information provided, we may not need to make further inquiries about the breach. If you handle breach identification and reporting well, we can be more confident that we can rely on the your internal processes to promote and test compliance.

2.4 However, if we cannot be satisfied of the factors in paragraph 2.2, then it may be necessary for us to require you to take remedial action, such as to change your procedures, strengthen existing compliance measures, systems and controls, or give corrective disclosures or compensation, as appropriate, to clients. In more serious cases, or in cases involving unusual complexity to resolve the causes and consequences of the breach (even if the factors in paragraph 2.2 are satisfied), we will consider taking enforcement action.

2.5 Failing to report a significant breach is an offence and may result in penalties. In deciding whether to take action for a failure to notify ASIC of a significant breach, we will conduct inquiries to determine whether or not you have met your reporting obligations. In doing so, we will take into account whether or not you have genuinely attempted to comply with your breach reporting obligations more generally.

Possible enforcement action

2.6 The legislation for which we have jurisdiction sets out the remedies available to us. These remedies can be broadly categorised as:

- criminal action;
- civil action; and
- administrative action.

2.7 We can use these remedies in combination. In some cases, we may accept an enforceable undertaking as an alternative to civil or licensing action.

Note: For guidance on our use of enforceable undertakings, see Regulatory Guide 100 *Enforceable undertakings* (RG 100) and Regulatory Guide 98 *Licensing: Administrative action against financial services providers* (RG 98) at paragraphs 1.20–1.22

2.8 Factors underlying our decisions about whether to take enforcement action (and what type of enforcement action to take) include whether:

- the matter involves serious corporate wrongdoing or serious risk or detriment to consumers and the market;
- an achievable or appropriate remedy exists for us to pursue; and
- the matter satisfies our regulatory and enforcement priorities, including deterrence and public education.

2.9 In most cases of notifications advising of employee fraud or serious misconduct, we will consider banning and/or criminal action against the individual concerned, rather than the licensee. However, we may make further inquiries to ensure there is ongoing compliance with your licence obligations and that you take reasonable steps to ensure that your representatives comply with the financial services laws.

2.10 The inquiries may go to the adequacy of pre-employment checks, the monitoring and supervision of staff, and controls over client funds. Depending on the outcome of any inquiries, we may take administrative action. For example, we may seek to address any issues identified by imposing additional conditions to the licence, or we may accept an enforceable undertaking offered by you.

Note 1: For guidance on a licensee's procedures for monitoring, supervision and training of representatives, see RG 104 and RG 105.

Note 2: For further guidance about our approach to taking administrative action against financial services industry participants, see RG 98.

Mitigating factors

2.11 Breach notification is a legal obligation; we are not influenced by whether a notification is made in accordance with this obligation. However, we may take into account where a breach notification should have been made and you failed to notify us, as this is a further contravention and may be indicative of your general approach to compliance.

2.12 Where you advise us of a contravention in circumstances where there is some uncertainty that you are obliged to do so, we may take this into account in considering whether any action may be taken against that party.

2.13 We may take into consideration your conduct after you have reported a breach as required by s912D. It is likely that we will take the following factors into account:

- the extent to which you are willing and able to address the consequences of the breach through communication and compensation to those adversely affected;

- any review and modification of compliance procedures by you to prevent recurrence of the conduct;
- appropriate disciplining of wrongdoers by you where the circumstances do not suggest there are more significant compliance issues within your business; and
- the extent to which you co-operated with us, including providing us with all information relevant to the underlying breaches and your remedial efforts.

2.14 Where you have taken the steps in paragraphs 2.12 and/or 2.13, we may:

- in serious cases, where civil or licensing action may otherwise be considered, accept an enforceable undertaking;
- in less serious cases (e.g. inadvertent breach, albeit with significant consequences) or cases where the steps that would be necessary to remedy the breach are not complex, require you to provide a statement (in some cases to be audited) under s912C;
- undertake a follow up inspection; or
- take no further action following assessment.

Public comment

2.15 If we take enforcement action against a financial services provider, our approach to public comment on that action will be governed by Regulatory Guide 47 *Public comment* (RG 47). As a general principle it is our view that there is significant public interest in ensuring that consumers, industry and the broader community are aware and informed about action taken by ASIC. Transparency and disclosure are important factors in market integrity and consumer confidence and serve to promote deterrence as well as to educate.

2.16 We may also from time to time publish information about trends in breach reporting: see paragraph 1.28 of this guide.

Key terms

In this guide, the following terms have the following meanings:

AFS licence An Australian financial services licence under s913B that authorises a person who carries out a financial services business to provide financial services.

Note: This is a definition contained in s761A.

AFS licensee or you A person who holds an AFS licence.

ASIC or we The Australian Securities and Investments Commission.

ASIC Act The *Australian Securities and Investments Commission Act 2001* including regulations made for the purposes of the ASIC Act.

consumer Includes an existing, potential or prospective client.

Corporations Act The *Corporations Act 2001* including regulations made for the purposes of the Corporations Act.

licensee An AFS licensee.

representative (of a licensee) Is:

- an authorised representative of the 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.

representative (of any other person) Is:

- an employee or director of the person;
- an employee or director of a related body corporate of the person; or
- any other person acting on behalf of the first person.

Note: This is a definition contained in s910A.

s912A (for example) A provision of the Corporations Act (in this example numbered 912A), unless a contrary intention appears.

Related papers

Regulatory guides

RG 36 *Licensing: Financial product advice and dealing*

RG 40 *Good transaction fee disclosure for bank, building society and credit union deposit and payments products (transaction accounts)*

RG 98 *Licensing: Administrative action against financial service providers*

RG 100 *Enforceable undertakings*

RG 104 *Licensing: meeting the general obligations*

RG 105 *Licensing: Organisational competence*

RG 146 *Licensing: Training of financial products advisers*

RG 164 *Licensing: Organisational capacities*

RG 165 *Licensing: Internal and external dispute resolution*

RG 166 *Licensing: Financial requirements*

RG 175 *Licensing: Financial product advisers—Conduct and disclosure*

RG 181 *Managing conflicts of interest*

RG 182 *Dollar disclosure*

Pro formas

PF 209 *Australian financial services licence conditions*

You can download copies of these publications from the Financial Services home page on www.asic.gov.au/fs. You can also get copies of these publications from ASIC Infoline on 1300 300 630.

Register for our free email update service, which alerts you to the latest developments, at www.asic.gov.au/joinfsupdate.
