



ASIC

Australian Securities & Investments Commission

REGULATORY GUIDE 78

Breach reporting by AFS licensees

February 2014

About this guide

This guide is for Australian financial services (AFS) licensees and responsible entities. It sets out your obligations to report to ASIC certain breaches of the law, and how we apply our administrative enforcement powers.

The following obligations to report matters to ASIC are not dealt with in this guide:

- if you are a body regulated by the Australian Prudential Regulation Authority (APRA) and you cease to hold that status (e.g. when you are a superannuation trustee and you have your approval as a trustee revoked by APRA: see Pro Forma 209 *Australian financial services licence conditions* (PF 209) condition 9);
- if you become aware of a change in control of the licensee: see reg 7.6.04(1)(i); or
- if you are an auditor whose breach reporting obligations are imposed by s311, 601HG or 990K: see Regulatory Guide 34 *Auditors' obligations: reporting to ASIC* (RG 34).

About ASIC regulatory documents

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

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

Regulatory guides: give guidance to regulated entities by:

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

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

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

Document history

This version was issued in February 2014 and is based on legislation and regulations as at the date of issue. The only changes made are updates to the breach notification details (RG 78.25–RG 78.26) and penalty amounts (RG 78.32), deletion of former RG 78.38, and revisions to RG 78.54 that reflect the release of Information Sheet 152 *Public comment* (INFO 152).

Previous versions:

- Superseded Regulatory Guide 78, issued September 2008
- Superseded *Breach reporting by AFS licensees: An ASIC guide*, issued October 2004, reissued May 2006, and known in the *ASIC Digest* as [SGD 190]; rebadged as a regulatory guide 5 July 2007

Disclaimer

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

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

This document gives 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

A	Overview	4
B	When you must report a breach	5
	Q1 What breaches (or likely breaches) must you report?	5
	Q2 What does 'likely to breach' mean?	7
	Q3 What does 'significant breach' mean?	7
	Q4 What arrangements should you have for recording and reporting breaches?	11
	Q5 How do you report a breach?	12
	Q6 When must you report a breach?	13
	Q7 What will we do with the information in a breach report?	14
	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
C	How we deal with breach notifications	17
	Relevant factors	18
	Possible enforcement action	18
	Mitigating factors	19
	Public comment	20
	Key terms	21
	Related information	22

A Overview

- RG 78.1 This document gives 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 services laws.
- RG 78.2 We also give some general guidance on what happens if you notify us of a breach as required under s912D. By explaining how we deal with these notifications, we aim to enhance the transparency of our processes.
- RG 78.3 This guide should be read in conjunction with our regulatory guides on how we administer Ch 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).

B When you must report a breach

Key points

As an AFS licensee, you must tell ASIC in writing within 10 business days about any significant breach (or likely breach) of your obligations. If you don't tell us about a significant breach (or likely breach) then we consider that this in itself is a significant breach.

You should have a clear, well-understood and documented process for identifying breaches.

Responsible entities are also subject to breach reporting requirements.

Q1 What breaches (or likely breaches) must you report?

RG 78.4 As an AFS licensee, you must give us a written report as soon as practicable, and in any case within 10 business days of becoming aware of a breach (or likely breach), if:

- (a) you breach any of the specified obligations; or
- (b) you are likely to breach any of the specified obligations; and
- (c) that breach (or likely breach) is 'significant'.

Note: See s912D.

RG 78.5 Section 912D requires you to report to ASIC any significant breach (or likely breach) of:

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

Table 1 below summarises these obligations.

Table 1: Summary of your obligations to report breaches

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 supplied efficiently, honestly and fairly; • comply with the conditions of 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 RG 78.6–RG 78.8); • be competent to supply 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 RG 78.6–RG 78.8); and • have compensation arrangements for retail clients. 	<p>You must comply with the following financial services laws:</p> <ul style="list-style-type: none"> • Ch 5C of the Corporations Act (managed investment schemes); • Ch 6 of the Corporations Act (takeovers); • Ch 6A of the Corporations Act (compulsory acquisitions and buy-outs); • Ch 6B of the Corporations Act (rights and liabilities about Ch 6 and 6A matters); • Ch 6C of the Corporations Act (information about ownership of listed companies and managed investment schemes); • Ch 6D of the Corporations Act (fundraising) • Ch 7 of the Corporations Act (financial services and markets) • Ch 9 of the Corporations Act (miscellaneous), but only as it applies to the chapters of the Corporations Act listed above; • Div 2 of Pt 2 of the ASIC Act (unconscionable conduct and consumer protections for financial services); and • other Commonwealth Acts specified in reg 7.6.02A (see note below) in so far as they cover conduct when supplying 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

- RG 78.6 If you are a body regulated by APRA, there is no obligation under s912A of the Corporations Act about adequate resources or risk management systems. Similarly, these obligations are not included as AFS licence conditions for bodies regulated by APRA. However, there are similar obligations in Commonwealth legislation regulated by APRA and in prudential standards and rules determined by APRA under that legislation.
- RG 78.7 Commonwealth legislation regulated by APRA is listed in reg 7.6.02A (see note under Table 1), and therefore a breach of this legislation may be a breach of your obligation to comply with a financial services law.
- RG 78.8 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:
- (a) compliance with the prudential standards or rules is required by the Australian Government as listed in reg 7.6.02A; and
 - (b) the breach arises from conduct when supplying financial services.

Q2 What does ‘likely to breach’ mean?

- RG 78.9 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).
- RG 78.10 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 other means of meeting the financial requirements at this time, you will become aware that you are likely to breach your financial requirements obligations.

Q3 What does ‘significant breach’ mean?

- RG 78.11 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, if 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.

- RG 78.12 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. When you are not sure whether a breach (or likely breach) is significant, we encourage you to report the breach.
- RG 78.13 You must have regard to a number of factors listed in s912D(1)(b) when deciding whether a breach (or likely breach) is significant: see Table 2. A breach may be significant when only one of the factors applies to your circumstances, or when there is a combination of factors.
- RG 78.14 We expect that, when you become aware of any breach (or likely breach), you will:
- (a) consider the circumstances and impact of that breach (or likely breach) in light of each of the factors in Table 2;
 - (b) decide if the breach is significant; and
 - (c) 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 notifying 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 supply 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 supply 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 supply the financial services covered by your licence.</p> <p>If the breach (or likely breach) will not affect your ability or capacity to supply 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>Loss to clients</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, if 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, if 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, if 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 appropriate, even if those breaches are not reported because they are not significant. In the example, the amount of interest owed by you must be paid to the client, even if the breach need not be reported.</p>

<p>The actual or potential financial loss (cont.)</p>	<p>Loss to the licensee</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 compared with your overall business. However, if the actual or potential financial loss to you resulting from the breach causes non-compliance with the 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 supply 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

RG 78.15 Table 3 sets out 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:</p> <ul style="list-style-type: none"> • adequate risk management systems; and • available adequate financial resources to supply the financial services covered by your licence. <p>We set minimum financial resource requirements to promote appropriate financial risk management and ensure that cash shortfalls do not put compliance with your 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 supply the financial services covered by your licence.</p>

<p>Example 3: Previously undetected breaches</p>	<p>A breach of an obligation under s912A or 912B 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: Representatives give inappropriate advice</p>	<p>If your representatives give inappropriate financial product advice to your clients, there may be breaches of your obligations to:</p> <ul style="list-style-type: none"> • comply with the relevant financial services laws; and • take reasonable steps to ensure that your representatives comply with those laws. <p>If there is a breach of these obligations because your representatives have given 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 supply 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 licence authorisations</p>	<p>If your representatives supply financial services outside the scope of your AFS licence 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 supply 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 supply 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 supply 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 supply 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

RG 78.16 Table 4 sets out 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: Representatives give inappropriate advice</p>	<p>If your representative gives inappropriate financial product advice to a client on one occasion only, this is unlikely to be a significant breach if 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. However, if inappropriate advice is given 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 Ch 5C is not likely to be significant and therefore will not need to be reported.</p> <p>But if the unit pricing error involves more than one client or shows a systemic problem, 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 for recording and reporting breaches?

RG 78.17 If you fail to properly consider whether every breach (or likely breach) that comes to your attention is significant under 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 us.

RG 78.18 We consider that failure to report a significant breach (or likely breach) is likely, in itself, to be a significant breach of your obligation to comply with the financial services laws. This is because it indicates that your arrangements to ensure compliance with your obligations may be inadequate.

RG 78.19 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:

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

- (c) determining whether identified breaches (or likely breaches) are significant;
- (d) reporting to us those breaches (or likely breaches) that are significant;
- (e) when appropriate, rectifying the breach (or likely breach); and
- (f) ensuring that arrangements are in place to prevent the recurrence of the breach (or likely breach).

Breach register

- RG 78.20 The Corporations Act does not require you to maintain a breach register. However, we consider that, in practice, you will need a breach register to ensure that you have adequate arrangements in place to comply with your obligation to identify and report all significant breaches (or likely breaches).
- RG 78.21 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 your breach register should contain the information that we are likely to require in a written breach report: see Table 5 below.
- RG 78.22 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 us. For more information, see RG 104 and RG 105.

Q5 How do you report a breach?

- RG 78.23 A breach must be reported to us in writing:
- (a) There is no prescribed form for reporting a breach. However, you can use Form FS80 *Notification by an AFS licensee of a significant breach of a licensee's obligations* on our website at www.asic.gov.au/forms, for lodging written breach reports.
 - (b) You may lodge your report in another form if that is more appropriate for you. You can report a breach (or likely breach) by giving us a written report with the information in Table 5.
- RG 78.24 If you do not have information about any of the matters in Table 5 at the date of reporting:
- (a) include the information you do have; and
 - (b) supplement it by lodging further information as it becomes available.

Table 5: Content of a written breach report (or register)

Date of the breach (or likely breach)	<p>Include both:</p> <ul style="list-style-type: none"> • the date that the breach occurred; and • the date you became aware of the breach. <p>Note 1: If the breach is significant, you must report it to ASIC within 10 business days of the date when you became aware of this. Therefore you should have a record of that date to ensure timely reporting.</p> <p>Note 2: Your breach register might also include the date that the breach was reported to ASIC and rectified.</p> <p>If it is a likely breach, give the date from which you anticipate that you will no longer be able to comply with your obligations.</p>
Description of the breach	Describe the obligation that has been breached (or is likely to be breached), including references to the section of the Corporations Act that sets out that obligation, and any relevant financial services law or AFS licence condition.
Why the breach is significant	Describe the factors in s912D(1)(b) that you considered in determining whether the breach (or likely breach) is significant and therefore required to be reported to ASIC.
How the breach was identified	For example, the breach may have been identified through your compliance arrangements or as a result of a client complaint.
How long the breach lasted	Include details as relevant.
Information about an authorised representative	<p>If an authorised representative is involved include:</p> <ul style="list-style-type: none"> • that authorised representative's name and number; and • if the representative's authorisation has been revoked, all last known contact details.
How the breach has been rectified	<p>Describe the process and responsibilities for handling the breach (or likely breach), including any steps that have been taken to remedy it (e.g. any compensation paid to clients).</p> <p>If ongoing steps are being taken to rectify the breach (or likely breach), indicate when you expect to send us a report on your progress in rectifying it.</p>
Future compliance	Describe any steps that have been, or will be, taken to ensure future compliance with the obligation.

How to lodge a breach report

RG 78.25 Address the report to: 'Misconduct and Breach Reporting, Australian Securities and Investment Commission'.

RG 78.26 Email the written breach report to ASIC at fsr.breach.reporting@asic.gov.au.

Q6 When must you report a breach?

RG 78.27 You must give the written breach report to ASIC as soon as practicable, and in any case *within 10 business days* of becoming aware of either:

- (a) the breach—if the breach had already occurred when you discovered it; or
- (b) 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.

RG 78.28 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 sure that the relevant people are aware of breaches in a timely and efficient manner.

Note: In providing up to 10 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 a breach notification, we will take into account any delays or obfuscation in reporting.

RG 78.29 Because extended processes may defeat the law’s intention for ASIC to be informed of significant breaches as soon as practicable, you should *not* wait until after the following events to send us your report:

- (a) you have completed all possible avenues of investigation to satisfy yourself whether or not the breach (or likely breach) is significant;
- (b) the breach (or likely breach) has been considered by your board of directors;
- (c) the breach (or likely breach) has been considered by your internal or external legal advisers;
- (d) you have rectified (when appropriate), or you have taken steps to rectify, the breach (or likely breach); or
- (e) in the case of a likely breach, the breach has in fact occurred.

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

RG 78.30 We will consider the information in a breach report to decide whether it is necessary or appropriate to take any further action. We do not take action on all matters reported to us.

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

RG 78.31 Breach notifications play a very important role in ASIC’s oversight of the financial services industry. Apart from alerting us to significant breaches of the law, they also give us 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?

RG 78.32 The maximum penalty for not reporting a significant breach (or likely breach) within 10 business days of becoming aware of the breach (or likely breach) is:

- (a) for an individual, \$8,500 or imprisonment for 1 year, or both; and
- (b) for a company, \$42,500.

Note: See s1311, 1312 and Sch 3.

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

RG 78.33 Responsible entities are subject to breach reporting requirements under both s912D and 601FC(1)(l).

RG 78.34 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.

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 us 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 us 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.

RG 78.35 If a breach is reported under one section, you do not have to notify us separately about the same issue under the other section.

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

RG 78.36 If you are a responsible entity, you must report to ASIC as soon as practicable after becoming aware of a breach, any breach of the Corporations Act that:

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

Note: See s601FC(1)(l).

RG 78.37 This requirement is more limited than the breach reporting requirement in s912D. In addition to the factors in RG 78.36(a)–RG 78.36(b), 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).

- RG 78.38 '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.
- RG 78.39 Breach reports under s601FC(1)(l) must be made as soon as practicable, but there is no maximum time limit as in s912D.

C How we deal with breach notifications

Key points

When we receive a breach report, we assess it and decide what, if any, action on our part is necessary.

Enforcement action is one potential response to a report of a significant breach, although only a small proportion of breach notifications result in us taking enforcement action.

RG 78.40 We follow a standard procedure when we receive a breach notification: see Table 6.

Table 6: What we do with a breach report

Acknowledgement	On receipt of the breach report, we acknowledge it.
Request for more information (if needed)	If we have insufficient information to form a view, we will ask you for more information.
Decision by ASIC	When we have all the information we need, we will decide whether any further action on our part is necessary.
Notification to licensee	<p>If the factors identified in RG 78.41 are satisfied, we may inform you that we do not intend to make further inquiries about the matter.</p> <p>If the factors identified in RG 78.41 are not satisfied, we will consider whether to take enforcement action: see RG 78.46–RG 78.49.</p>
Addressing compliance issues (if appropriate)	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.
Formal surveillance (if appropriate)	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

- RG 78.41 When we receive a breach notification, we seek to ensure that:
- (a) you have made a genuine attempt to comply with the law and your breach reporting obligations;
 - (b) the causes of the breach have been identified and, if readily rectified, addressed so that it is unlikely to recur;
 - (c) in other cases, a plan for rectifying the compliance failure has been developed and submitted to us;
 - (d) the consequences (particularly to consumers) are able to be dealt with comprehensively (e.g. by compensation and communication);
 - (e) there has been no undue delay in notifying us; and
 - (f) if the circumstances suggest there are some more significant compliance issues within your business, they are identified.
- RG 78.42 If we can be satisfied of the factors in RG 78.41, 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.
- RG 78.43 However, if we cannot be satisfied of the factors in RG 78.41, 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 (where 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 RG 78.41 are satisfied), we will consider taking enforcement action.
- RG 78.44 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 us 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

- RG 78.45 The legislation for which we have jurisdiction sets out the remedies available to us. These remedies can be broadly categorised as:
- (a) criminal action;

- (b) civil action; and
- (c) administrative action.

RG 78.46 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 RG 98.38–RG 98.40

RG 78.47 Factors underlying our decisions about whether to take enforcement action (and what type of enforcement action to take) include whether:

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

RG 78.48 In most cases of reports 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.

RG 78.49 The inquiries may involve 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 on your licence, or we may accept an enforceable undertaking offered by you.

Note: For guidance on procedures for monitoring, supervision and training of representatives, see RG 104 and RG 105. For further guidance about our approach to taking administrative action against financial services industry participants, see RG 98.

Mitigating factors

RG 78.50 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 when a breach notification should have been made and you failed to notify us, because this is a further contravention and may indicate your general approach to compliance.

- RG 78.51 If you advise us of a contravention in circumstances when 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.
- RG 78.52 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:
- (a) the extent to which you are willing and able to address the consequences of the breach through communication and compensation to those adversely affected;
 - (b) any review and modification of compliance procedures by you to prevent recurrence of the conduct;
 - (c) appropriate disciplining of wrongdoers by you when the circumstances do not suggest there are more significant compliance issues within your business; and
 - (d) the extent to which you co-operated with us, including giving us all information relevant to the underlying breaches and your remedial efforts.
- RG 78.53 If you have taken the steps in RG 78.51 and/or RG 78.52, we may:
- (a) in serious cases, when civil or licensing action may otherwise be considered, accept an enforceable undertaking;
 - (b) 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:
 - (i) require you to supply a statement (in some cases to be audited) under s912C;
 - (ii) undertake a follow up inspection; or
 - (iii) take no further action following assessment.

Public comment

- RG 78.54 If we take enforcement action against a financial services provider, our approach to public comment on that action will be governed by Information Sheet 152 *Public comment* (INFO 152). We may make a statement about an investigation when it is in the public interest to do so. We will consider whether making a statement would promote confidence in the integrity of the market, or facilitate the protection of consumers and investors in relation to the financial system.
- RG 78.55 We may also from time to time publish information about trends in breach reporting: see RG 78.31.

Key terms

Term	Meaning in this document
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
APRA	Australian Prudential Regulation Authority
ASIC (or we)	Australian Securities and Investments Commission
ASIC Act	The <i>Australian Securities and Investments Commission Act 2001</i> including regulations made for the purposes of the ASIC Act
Ch 7 (for example)	A chapter of the Corporations Act (in this example numbered 7)
consumer	Includes an existing, potential or prospective client
Corporations Act	The <i>Corporations Act 2001</i> including regulations made for the purposes of the Corporations Act
licensee	An AFS licensee
representative (of a licensee)	Is: <ul style="list-style-type: none"> • 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 in s910A
representative (of any other person)	Is: <ul style="list-style-type: none"> • 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 in s910A
RG 104 (for example)	An ASIC regulatory guide (in this example numbered 104)
s912A (for example)	A provision of the Corporations Act (in this example numbered 912A), unless a contrary intention appears

Related information

Headnotes

AFS licensee, breach, breach reporting, compensation, financial services, licensee obligations, likely breach, material adverse effect, significant breach

Regulatory guides

RG 34 *Auditors' obligations: reporting to ASIC*

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 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*

Legislation

Corporations Act 2001: s601FC(1)(l), 912A, 912A(1)(c), 912B, 912D, 912D(1A), 912D(1)(b), 912D(1)(b)(i), 912D(1)(b)(ii), 912D(1)(b)(iii), 912D(1)(b)(iv), 912D(1)(b)(v), 1311, 1312, Sch3, Ch 5C, 6, 6A, 6B, 6C, 6D, 7, 9, reg 7.6.02A

Australian Securities and Investments Commission Act 2001: Div 2 Pt 2

Other Commonwealth Acts as specified in reg 7.6.02A: *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, Superannuation (Resolution of Complaints) Act 1993

Cases

Minister for Immigration v Dela Cruz (1992) 34 FCR 348; 110 ALR 367 at 371

ASIC forms

Form FS80 *Notification by an AFS licensee of a significant breach of a licensee's obligations*

Media and other releases

IR 04/53 *ASIC provides guidance on breach notification requirements of AFS licensees*

IR 06/14 *Industry embraces early notification of breaches*