Breach Reporting and Consequence Management Policy

Entity:	Integrity Financial Planners Pty Ltd (**IFP**)
ABN:	71 069 537 855
AFSL:	225051

Contents

Intellectual Property and disclaimer

Version:

Version	Date	Amendments
1	October 2021	New Policy

References:

- REGULATORY GUIDE 256: Client review and remediation conducted by advice licensees
- REGULATORY GUIDE 78: Breach reporting by AFS licensees
- ASIC INFO SHEET 259: Complying with the notify, investigate and remediate obligations

1 Background and purpose of document

1.1 Background

(a) Section 912DAA of the Corporations Act requires a holder of an Australian Financial Services Licence (**AFSL**) to report to ASIC all 'reportable situations' within 30 days after the AFSL first knows or is reckless with respect to whether there are reasonable grounds to believe a reportable situation has arisen.

(b) This includes the obligation to report to ASIC any 'significant' breach (or likely significant breach) of its core obligations (eg. the AFSL's obligations under 912A (licence conditions), 912B (compensation arrangements) and financial services laws).

(c) Section 912A(1) requires an AFSL, amongst other requirements, to:

(i) do all things necessary to ensure that the financial services covered by the licence are provided efficiently, honestly and fairly (s912A(1)(a));

(ii) comply with the conditions on the licence (s912A(1)(b));

(iii) comply with the financial services laws (s912A(1)(c));

(iv) take reasonable steps to ensure that its representatives comply with the financial services laws (s912A(1)(ca));

(v) have available adequate resources (including financial, technological and human resources) to provide the financial services covered by the licence and to carry out supervisory arrangements (s912A(1)(d));

(vi) maintain the competence to provide those financial services (s912A(1)(e));

(vii) ensure that its representatives are adequately trained and are competent, to provide those financial services (s912A(1)(f)); and

(viii) have adequate risk management systems (s912A(1)(h)).

(d) Part 7.6, Division 3, Subdivision C of the Corporations Act requires AFSLs to notify clients affected by certain breaches of the law, investigate the nature and full extent of those breaches and remediate affected clients within strict timeframes.

1.2 Purpose and framework

This policy (**Policy**) is developed by Integrity Financial Planners Pty Ltd (the Licensee) for the purposes of:

(a) enabling the Licensee to meet its obligations under the Corporations Act, ASIC guidance and AFS Licence condition; and

(b) enabling the Responsible Manager(s) and key staff members of the Licensee to understand the obligations of the Licensee under the Corporations Act, ASIC guidance and AFS licence condition.

1.3 Responsibility

(a) A Responsible Manager and the Directors of the Licensee (or its delegate with appropriate experience) will be responsible for ensuring that the Licensee is aware of and meets the requirements of this Policy.

(b) A Responsible Manager will monitor the adequacy of this Policy by reviewing it at least annually (unless more frequent review is required) to ensure the content remains up to date, accurate and adequate.

(c) A Responsible Manager will ensure that all staff receive appropriate training about this Policy.

2 The reporting obligation

2.1 What is the reporting obligation?

(a) The Licensee is required to report to ASIC within 30 days after it first knows or is reckless with respect to whether there are reasonable grounds to believe a reportable situation has arisen.

(b) The types of reportable situations detailed further below relate to:

(i) situations that require a determination of 'significance' before they are reported to ASIC, namely, breaches or likely breaches of core obligations that are found to be significant; and

(ii) situations that must be reported and do not require a determination of significance, including:

(A) deemed significant breaches;

(B) investigations into breaches or likely breaches that last more than 30 days; and

(C) additional reportable situations, such as gross negligence or serious fraud.

(c) Appendix A contains a decision-making matrix to assist the Licensee in identifying if a reportable situation exists, and if so, when to report it.

2.2 What is a breach or likely breach?

(a) A breach is an actual breach of the core obligations.

(b) A 'likely breach', as defined in s912D(1A), requires Licensees to report breaches that have yet to occur. ASIC interprets this as the Licensee becoming aware that they are no longer able to comply with their core obligations: see RG 78.26.

2.3 Is the breach (or likely breach) significant?

(a) Not all breaches or likely breaches need to be reported to ASIC. The Licensee is required to report any breaches or likely breaches that are 'significant'.

(b) Some breaches are deemed significant breaches. **In determining whether a breach is significant, the Licensee will first consider whether the breach is a deemed significant breach: see clause 2.5 below**.

(c) In other situations, the Licensee will need to consider a breach or likely breach of a core obligation against factors in section 912D(5) of the Corporations Act to determine whether it is significant.

(d) If a breach is not significant, the Licensee will nonetheless need to record the breach in the breach register and determine the appropriate remediation action as required. Sometimes, there may be breaches of 'Licensee Policy' which may not of itself constitute a breach of financial services laws. In these instances, it will be up to the Responsible Manager to determine the appropriate treatment of the breach.

(e) In determining the significance of the breach or the remediation required, the Licensee may seek the opinion of its external compliance consultants.

(f) Section 912D(5) sets out the factors that determine whether a breach, or likely breach, is 'significant' (significance test). These are set out below.

Factors	Explanation
The number or frequency of similar previous breaches s912D(5)(a)	The greater the number or frequency of similar breaches, the more likely the new breach will be significant. This may also be an early indicator of systemic issues.
The impact of the breach or likely breach on the Licensee's ability to supply the financial services covered by the AFS Licence: s912D(5)(b)	If a breach (or likely breach) reduces the Licensee's ability or capacity to supply the financial services covered by the Licence, it may be significant. For example, a breach of the financial requirements of the Licence conditions may be significant. If these minimum requirements are not met, the Licensee may not have the financial ability or capacity to supply the financial services covered by the Licence.
The extent to which the breach or likely breach indicates that the Licensee's arrangements to ensure compliance with those obligations is inadequate: s912D(5)(c)	If the breach (or likely breach) indicates that the Licensee's 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 the Licensee's compliance arrangements, it is more likely to be significant. Occasional and minor breaches do not of themselves mean that the Licensee's compliance arrangements are inadequate.
Any other matters prescribed by regulations: s912D(5)(d)	There are currently no regulations made under this paragraph.

2.4 Examples of breaches that may be significant

Factors	Explanation
Failure to notify ASIC of changes in key persons	Failing to inform ASIC within the required time period in relation to the replacement of a key person may be a significant breach. ASIC considers that the departure of a key person may impact a Licensee's ability to provide adequate financial services as required by section 912A(1)(b) of the Corporations Act.
Failure to lodge statutory reports	If the Licensee fails to lodge financial reports and other required reporting obligations on time, it may be a significant breach where the delay is substantial or where it occurs on multiple occasions. ASIC considers significant delays or repeated failures may indicate compliance failures, financial difficulties or unresolved issues in the audit process such as a failure to maintain adequate books and records.
Repeated failures to give a disclosure document	Failure to provide an FSG or PDS is excluded from being a deemed significant breach under section 912D(4) by reg 7.6.02A(2) of the Corporations Regulations. However, ASIC considers that if the if a Licensee identifies multiple breaches of the same nature, or issues suggest there are deficiencies in the Licensee's compliance systems, the breach may be significant.

2.5 Deemed significant breaches

(a) Under section 912D(4) of the Corporations Act, certain breaches of core obligations are taken to be significant. If a breach or likely breach is a deemed significant breach, the Licensee must not take additional steps to determine whether the breach is significant before reporting it to ASIC: see RG 78.39 - 43.

(b) Deemed significant breaches include breaches:

(i) that constitute an offence which is punishable by a penalty that may include imprisonment for three months if the offence involves dishonesty, or 12 months or more in any other case;

(ii) of a civil penalty provision (except where excluded by regulations);

(iii) misleading and deceptive conduct;

(iv) that results, or are likely to result, in material loss or damage to clients.

(c) Material loss or damage includes financial and non-financial loss or damage. The Licensee will consider the clients' circumstances, the number of clients affected, and the aggregate loss or damage (if relevant) in determining whether the loss or damage is material. The breach is 'likely to result in material loss or damage' if there is a real and not remote possibility that loss or damage will occur as a result of the breach.

2.6 Civil penalty provisions (deemed significant)

(a) Breaches of civil penalty provisions that are deemed significant breaches include:

(i) failure to give a statement of advice (section 964A);

(ii) misleading and deceptive conduct (section 1041H);

(iii) breach of the best interests duty (section 961B);

(iv) failure to give appropriate advice (section 961G);

(v) incomplete and inaccurate information (section 961H);

(vi) prioritising the adviser's interests over the client's (section 961J);

(vii) failing to provide an FDS (section 962S);

(viii) charging ongoing fees after termination of an ongoing fee arrangement (section 962P)

(ix) not obtaining consent before deducting ongoing fees from an account (section 962R(4))

(x) failure to give written notice of cessation of consent to account provider (section 962V(3))

(xi) the Licensee accepts conflicted remuneration or fails to ensure authorised representatives do not accept conflicted remuneration, or authorised representatives accept conflicted remuneration, or an employer pays its employees conflicted remuneration (sections 963E-H);

(xii) charging asset-based fees on borrowed amounts (section 964D(1) and 964E(1));

(xiii) breach of the anti-avoidance provision (section 965).

(xiv) engaging in retail product distribution conduct before review of target market determinations (subsection 994C(7));

(xv) engaging in retail product distribution conduct where there is no target market determination (section 994D)

(xvi) failure to ensure that retail product distribution conduct is consistent with target market determinations (subsections 994E(1) and (3))

(xvii) failure to keep records (subsections 994F(1) and (3))

(xviii) failure to report complaints and other information (subsections 994F(4), (5) and (6)).

(b) A complete list of the civil penalty provisions can be found at section 1317E of the Corporations Act.

(c) Certain breaches of civil penalty provisions are excluded from being deemed significant breaches under section 912D(4): reg 7.6.02A(2) of the Corporations Regulations. This includes:

(i) failing to provide clients with a FSG; and

(ii) failing to provide clients with a PDS.

(d) When a breach is excluded from deeming under the regulations, the Licensee must still consider whether it is a deemed significant breach under any of the other criteria in section 912D(4) of the Corporations Act, or if none of those criteria apply, whether it is significant in light of the factors in section 912D(5) of the Corporations Act: see RG 78.43.

2.7 Investigations of breaches or likely breaches that are reportable

(a) Under section 912D(1)(c) of the Corporations Act, investigations into whether a significant breach (or likely significant breach) of a core obligation has occurred will be reportable situations where:

(i) the investigation has continued for more than 30 days; and

(ii) the outcome of an investigation that has continued for more than 30 days is that there are no reasonable grounds to believe a reportable situation has arisen.

(b) Where an investigation concludes within 30 days and there are no reasonable grounds to believe that a reportable situation has arisen, it is not a reportable situation.

(c) However, where an investigation has concluded within 30 days, and the investigation identified reasonable grounds to believe that a reportable situation has arisen, this must also be reported to ASIC.

(d) ASIC considers that a Licensee is likely to have commenced an investigation where there has been information gathering or human effort applied to determine whether a breach has occurred or will occur. This may include:

(i) communicating with representatives or staff who may have been involved in the conduct;

(ii) communicating with potentially affected clients; or

(iii) seeking specialist advice.

(e) For the avoidance of doubt, ASIC clarifies that the following does not trigger the commencement of the 30 day timeframe (until such time actual investigation involving deployment of human resources is carried out):

(i) the mere receipt of a complaint, a whistle-blower disclosure or a regulatory request;

(ii) preliminary steps and initial fact-finding inquiries into the nature of the incident (completed over a short timeframe) and conducted as an initial response; and

(iii) 'business as usual' inquiries, such as routine audits, quality assurance monitoring, or other internal compliance review processes. These are only reportable if they are triggered by an incident.

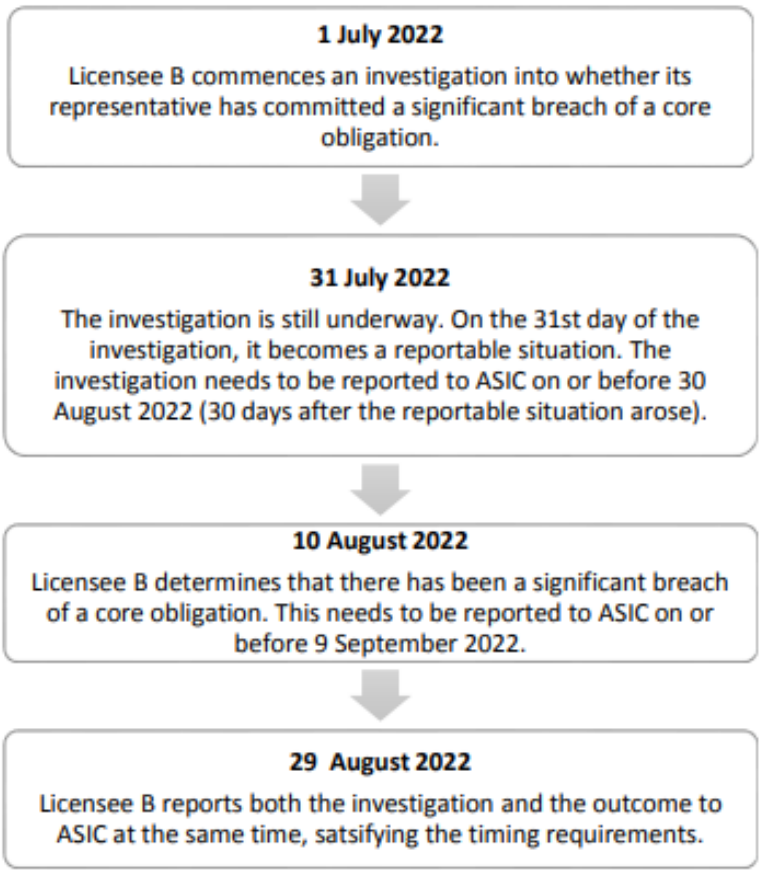
(f) Routine internal audit and quality assurance monitoring procedures that are not directed at identifying whether a significant breach of a core obligation has arisen will not constitute an investigation, unless they are triggered by an incident or assess a possible breach of a core obligation: RG 78.57 Table 6.

(g) In some circumstances, it may be clear to the Licensee that the circumstances constitute a reportable situation, and an investigation will not be required. Where an investigation is required, the Licensee will commence and complete investigations in a timely manner and without unreasonable delay.

(h) If additional reportable situations arise from the investigation, the Licensee must report this to ASIC and does not need to determine whether or not it is significant.

(i) The Licensee is also required to comply with its notify, investigate and remediate obligations: **see section 6 below.**

2.8 Example reporting timeline



2.9 Additional reportable situations

(a) Under section 912D(2) of the Corporations Act, the Licensee must report certain additional reportable situations.

(b) Additional reportable situations includes where the Licensee or its representatives:

(i) engage in gross negligence in the course of providing a financial service;

(ii) commit serious fraud; or

(iii) other circumstances prescribed by regulations.

(c) There are currently no regulations prescribing additional reportable situations.

3 Reportable situations about other Licensees

3.1 Reporting other Licensees

(a) The Licensee may be required to report other Licensees to ASIC in certain circumstances.

(b) Where the Licensee has reasonable grounds to believe that a reportable situation, other than a reportable situation involving an investigation, has arisen in relation to an individual who:

(i) provides personal advice to retail clients about financial products; and

(ii) is another AFS Licensee, or is an employee, director or other representative of an AFSL,

the Licensee will lodge a report with ASIC.

(c) The threshold of 'reasonable grounds' does not require facts or evidence amounting to certain proof there is a breach; the test is whether the Licensee has reasonable grounds to believe a reportable situation has arisen. This exists when any facts or evidence induce in a reasonable person a belief that a reportable situation has arisen: see RG 78.74 - 75.

(d) Within 30 days after the Licensee first knows or is reckless with respect to whether there are reasonable grounds to believe the reportable situation has arisen, it must:

(i) lodge the report with ASIC; and

(ii) provide a copy of the report to the other licensee.

(e) The Licensee will not need to lodge a report where there are reasonable grounds to believe that ASIC is aware of the reportable situation and all of the information required in a report. However, ASIC considers this is a 'high threshold', for example, the Licensee is aware a third party has lodged a breach report because of a relevant ASIC media release.

4 Reporting to ASIC

4.1 When to report

(a) The Licensee will report to ASIC within 30 calendar days after a reportable situation has arisen. The reporting period starts on the day the Licensee first knows, or is reckless with respect to whether, there are reasonable grounds to believe that a reportable situation has arisen ('reasonable grounds').

(b) Reasonable grounds exist where there are facts to induce a belief that a reportable situation has arisen in a reasonable person: RG 78.86. This legal threshold does not require facts or evidence amounting to certain proof there is a breach. For example, a progress report which indicates that clients may have been overcharged may be a reportable situation, even if final calculations of loss have not been determined.

(c) The Licensee will be reckless where:

  (i) the Licensee is aware of a substantial risk there are reasonable grounds; and

  (ii) having regard to the circumstances known to the Licensee, it is unjustifiable to take the risk that there are reasonable grounds.

(d) The Licensee will be taken to be reckless or have knowledge with respect to reasonable grounds where a director, employee or agent of the Licensee has gained that state of mind by engaging within their actual or apparent authority: section 769B(3). For example, a Licensee will be reckless or have knowledge of reasonable grounds where a compliance employee or agent first gains the state of mind, even if it is later referred to a committee or CEO: RG 78.97 - 98.

(e) In relation to reporting investigations, the Licensee will report the investigation within 30 calendar days after the reportable situation has arisen, namely:

  (i) the day the investigation exceeds 30 days; or

  (ii) the day an investigation that exceeded 30 days concludes there are no reasonable grounds to suspect a reportable situation has in arisen.

(f) The Licensee will avoid any unnecessary delays in lodging a report with ASIC.

4.2 How to report

(a) The Licensee must report to ASIC using the prescribed form through the ASIC Regulatory Portal at https://regulatoryportal.asic.gov.au.

(b) Where there are multiple reportable situations arising from a single, specific root cause, the Licensee may notify ASIC of the reportable situations in one report.

(c) Where there are *similar* or *related* reportable situations that arise from the same root cause, the extent to which they can be grouped together for the purposes of reporting to ASIC will depend on the circumstances. For example:

(i) where several instances of misleading conduct are only connected by the fact that one internal audit identified those instances, they cannot be grouped together. However, multiple contraventions of the law relating to a single root cause of fraud may all be reported to ASIC in one report;

(ii) where a systemic overcharging issue is identified in relation to a product, and the Licensee is unable to immediately stop overcharging this fee and additional customers are overcharged, with each instance of overcharging a reportable situation, these may be reported to ASIC together;

(iii) where a systemic overcharging issue is identified in relation to multiple products, whether the instances may be reported together depend on the circumstances of the fee-charging error. For example, if the products belong to the same category or relate to one client, this may indicate the instances are tied to a single, specific root cause.

(d) The Licensee will update ASIC using the update functionality available on the ASIC Regulatory Portal in certain circumstances, including:

(i) to provide an update on a report that has already been lodged – for example to provide updates on an estimate earlier provided in response to one of the questions;

(ii) to notify ASIC of the completion of rectification and remediation processes; or

(iii) if after the Licensee lodges the breach report, it identifies additional instances of reportable situations that are similar or related to reportable situations that arise from the same, single specific root cause.

(e) The prescribed form on the ASIC Regulatory Portal asks a series of questions about the nature of what is to be reported and generates questions relevant to the reportable situation. An overview of the content of the prescribed form can be found in Appendix B.

5 Breach Reporting Steps

Appendix A contains a decision-making matrix to assist the Licensee in identifying if a reportable situation exists, and if so, when to report it.

5.1 Step 1: Identifying potential reportable situations

(a) All staff are responsible for reporting actual or potential breaches immediately to the Responsible Manager. Staff will receive adequate training on this Policy to enable them to identify actual and potential breaches.

(b) Once the potential reportable situation is identified, it is the role of the Responsible Manager to:

(i) review the situation to assess whether it is a reportable situation;

(ii) record and document all correspondence, notes and information relating to the assessment; and

(iii) log the potential reportable situation, along with all relevant decisions and actions taken in relation to the potential reportable situation, on the breach register.

(c) The Responsible Manager will also be required to ensure if the notify, investigate, and remediate obligations are engaged and that the Licensee meets the timelines of these obligations: see section 6 below.

5.2 Step 2: Is the situation a deemed significant breach?

(a) The Responsible Manger will have regard to clause 2.5 and clause 2.6 above in order to determine whether the issue is a deemed significant breach.

(b) If the Responsible Manager finds that the situation constitutes a deemed significant breach, the Responsible Manager will lodge a report with ASIC in accordance with Step 6 below. The Responsible Manager will not need to consider Steps 3-5.

(c) If the situation is not a deemed significant breach, the Responsible Manager will consider Step 3.

5.3 Step 3: Is the situation a significant investigation?

(a) The Responsible Manger will have regard to clause 2.7 above in order to determine whether the issue is a reportable investigation.

(b) If the Responsible Manager finds that the situation constitutes a deemed significant breach, the Responsible Manager will lodge a report with ASIC in accordance with Step 6 below. The Responsible Manager will not need to consider Steps 4-5.

(c) If the situation is not a reportable investigation, the Responsible Manager will consider Step 4.

5.4 Step 4: Is the situation an additional reportable situation?

(a) The Responsible Manger will have regard to clause 2.9 above in order to determine whether the issue is an additional reportable situation.

(b) If the Responsible Manager finds that the situation constitutes a deemed significant breach, the Responsible Manager will lodge a report with ASIC in accordance with Step 6 below. The Responsible Manager will not need to consider Step 5.

(c) If the situation is not a reportable investigation, the Responsible Manager will consider Step 5.

5.5 Step 5: If the incident is a breach (but not a deemed significant breach), is the breach otherwise 'significant'?

(a) If the incident is a breach, the Responsible Manager must assess whether the breach is significant or not, having regard to the factors set out in section 2 of this policy as well as the Licensee's legal and regulatory obligations.

(b) In making this assessment, the Responsible Manager may form a breach assessment committee or seek the views of its external consultants.

(c) The Responsible Manager must record and document all correspondence, rationale, notes and information relating to the assessment and notify all relevant stakeholders in the business.

(d) If the Responsible Manager concludes that the breach is not a significant breach, the Responsible Manager will log the breach in the breach and incidents register and include the reasons for their assessment.

(e) The Responsible Manager must make this assessment within 5 business days of becoming aware of the incident.

(f) The Responsible Manager must update the key management staff and stakeholders of the Licensee.

5.6 Step 6: If the issue is a reportable situation

(a) If the Responsible Manager determines that an issue is a reportable situation, the Responsible Manager will prepare and lodge a report to ASIC on the reportable situation in accordance with the guidance set out in Appendix B below;

(b) The Responsible Manager will submit the report via the Regulatory Portal at https://regulatoryportal.asic.gov.au/;

(c) In preparing the breach report, the Responsible Manager must ensure they are familiar with the requirements under:

(i) ASIC Regulatory Guide 78: Breach reporting by AFS licensees;

(ii) ASIC Report 594: Review of selected financial services groups' compliance with the breach reporting obligation;

(iii) ASIC Regulatory Guide 256: Client review and remediation conducted by advice licensees; and

(iv) ASIC Form FS80.

(d) The Responsible Manager will log the breach in the breach and incidents register and include the reasons for their assessment;

(e) The Responsible Manager must ensure that the report is lodged within 30 days of the reportable situation arising, namely:

(i) when the Licensee first knows or is reckless with respect to whether there are reasonable grounds to believe a reportable situation has arisen; or

(ii) where the reportable situation relates to an investigation into whether there are reasonable grounds to suspect a reasonable investigation exists:

(A) the day after the investigation exceeds 30 days (i.e. on day 31); and

(B) the day that an investigation that exceeded 30 days concludes there are no reasonable grounds to suspect a reportable situation has arisen.

(f) Once the breach report has been lodged with ASIC, the Licensee will periodically update ASIC on progress until the breach remediation is met.

5.7 Step 7: Remediation and prevention

(a) Whilst steps 1-6 are being carried out, the Responsible Manager must take reasonable steps to carry out remediation of the breach or incident if remediation is required.

(b) If the notify, investigate, and remediate obligations are engaged, the Responsible Manager must ensure that the Licensee meets the timelines of these obligations: see section 6 below.

(c) If the notify, investigate, and remediate obligations are not engaged, the Responsible Manager will consider what remediation is appropriate in accordance with section 7 below.

(d) The Responsible Manager must also:

(i) review the incident/breach and determine how to prevent similar breaches from recurring;

(ii) review the incident against previous breaches to ascertain any trends, areas of concern or systemic issues; and

(iii) consider implementing appropriate accountability checks after significant breaches.

5.8 Step 8: Review of the Breach Reporting Processes

(a) The Responsible Manager will ensure there is a regular review or audit of the breach reporting process and internal benchmarking on:

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

(ii) any trends; and

(iii) timeliness, including for ongoing investigations, remediation and incident identification.

(b) The Responsible Manager will continually assess whether the Licensee's consequence management, governance structures and resourcing are adequate.

6 Notify, Investigate and Remediate obligations (applicable for reportable situations arising after October 1 2021)

6.1 Obligations to notify, investigate and remediate

(a) Part 7.6, Division 3, Subdivision C of the Corporations Act requires the Licensee to notify clients affected by certain breaches of the law, investigate the nature and full extent of those breaches, and remediate affected clients within certain timeframes;

(b) These obligations apply where the following conditions are satisfied:

(i) the Licensee provides personal advice to retail clients in relation to financial products (other than basic banking products or general insurance products);

(ii) there are reasonable grounds to believe that a relevant reportable situation has arisen;

(iii) there are reasonable grounds to suspect an affected client has suffered, or will suffer, loss or damage as a result of the relevant reportable situation; and

(iv) there are reasonable grounds to suspect an affected client has a legally enforceable right to recover the loss or damage from the licensee.

(c) These obligations may overlap and are not necessarily sequential. For example, the Licensee may prepare aspects for remediation during the investigation, or triage affected clients so that some are notified and remediated while others are investigated.

6.2 Notify obligation – reportable situation

(a) Where the obligations in clause 6.1(b) exist, the Licensee must take reasonable steps to notify affected clients in writing of the breach within 30 calendar days of the Licensee first knowing of, or being reckless with respect to the relevant reportable situation arising.

(b) The notice must be in writing and should explain the nature of the reportable situation (breach) and the basis for the suspicion that the affected client has suffered or will suffer loss or damage.

(c) ASIC considers the following will be relevant to include in the notice to clients:

(i) the date of the reportable situation;

(ii) a description of the reportable situation;

(iii) the consequences of the relevant reportable situation for the affected client and how they may be affected;

(iv) relevant information about the investigation that is to be carried out;

(v) when the affected client should expect to hear from the Licensee next;

(vi) their consumer rights.

6.3 Investigate Obligation

(a) Where the obligations in clause 6.1(b) exist, the Licensee must start an investigation into the nature and full extent of the breach within 30 calendar days of the Licensee first knowing of, or being reckless with respect to the relevant reportable situation arising.

(b) The investigation must:

(i) identify the conduct that gave rise to the reportable situation;

(ii) quantify the loss or damage that there are reasonable grounds to believe affected clients have suffered (or will suffer) and have a legally enforceable right to recover.

(c) Where the investigation finds reasonable grounds to believe that additional reportable situations have arisen, the Licensee will report the additional breach to ASIC and notify clients and remediate as required.

(d) The Licensee will, where possible, keep affected clients informed of the progress of the investigation.

6.4 Notify obligation - outcome

(a) When the investigation is concluded, the Licensee must take reasonable steps to notify affected clients in writing of the outcome of the investigation within 10 calendar days of the investigation concluding.

(b) This notice will:

(i) explain the nature of the breach identified and any related breaches;

(ii) describe how the breach affected the client's interests;

(iii) assess the loss or damage the Licensee reasonably believes the affected client is entitled to recover.

(c) Where the investigation finds that an affected client has not suffered or will not suffer loss or damage which they have a legally enforceable right to recover, the Licensee must still notify the affected clients of the outcome of the investigation.

6.5 Remediate Obligation

(a) Where the obligations in clause 6.1(b) exist, if there is loss or damage and a legally enforceable right to recover, Licensees must take reasonable steps to pay affected clients' remediation of an amount equal to the loss or damage within 30 days of the investigation concluding.

(b) Where clients fall outside the scope of the obligation to remediate, the Licensee must still consider the requirements of the existing remediation framework in deciding whether it is efficient, honest and fair to remediate; see clause 7 below.

7 Remediation and consequence management

7.1 Regulatory requirement

The Licensee is responsible for the action and conduct of its representatives. As an AFSL, the Licensee has an obligation to ensure that their financial services are provided efficiently, honestly and fairly: s912A(1)(a).

7.2 Types of remediation

(a) Remediation is a process that is instigated at the request of the Licence to correct a non-compliance matter or breach by the Licensee or its adviser. Remediation of clients may be monetary (e.g. compensation), non-monetary

(e.g., providing disclosure not previously given or moving clients into more appropriate products), or a combination of both.

(b) As the impact of the non-compliance can vary in its impact on retail clients, the Licensee considers that in general, the two types of remediation set out below would be relevant:

(i) Advice remediation (non monetary); and

(ii) Client review and remediation (monetary).

(c) If remediation is required, the Licensee will determine the appropriate remediation methodology depending on the nature of the non-compliance.

7.3 What is advice rectification?

(a) Advice rectification refers to the process of rectifying the advice provided to the client by providing supplementary information to the retail client to rectify the deficiency in the initial advice. Alternatively, it may also involve re-producing the advice with all the legal and regulatory requirements met and providing the subsequent advice to the retail client.

(b) In general, the Licensee considers that advice rectification would be appropriate where areas of non-compliance identified in the advice have not resulted in client loss. This may be the case where the advice (e.g. strategy and recommendations) is generally appropriate but areas of non-compliance against the requirements of the Corporations Act (e.g. disclosure of costs, risks or interests that could influence advice) have been identified.

(c) Depending on the nature of the non compliance, the Licensee may determine that it is necessary to notify the professional indemnity insurers.

7.4 What does advice rectification involve?

(a) Advice rectification involves rectifying the advice initially provided to the client by providing the client with all the material information that should have been provided to them and could have been reasonably known by the adviser when personal advice was initially given. The nature of the 'missing' information is usually identified via an advice file audit.

(b) Where advice rectification is required, the Licensee may at its discretion allow the adviser to provide the missing material information in writing to the client (e.g., via email). Once missing information is given, the adviser must allow the client reasonable time to decide whether they would still proceed with the advice having the benefit of all the information.

(c) If the client elects to proceed given the information, the adviser is required to make a note of this on the client file.

(d) If the client does not elect to proceed given the information, the adviser is required to notify the Responsible Manager immediately who will determine the most appropriate way to remediate the client.

(e) Where advice rectification is required, the Licensee reserves the right to request further files from the adviser to determine if a certain issue is ongoing or systemic.

7.5 What is client review and remediation?

(a) *ASIC Regulatory Guide 256: Client review and remediation conducted by advice licensees* sets out ASIC's expectations regarding client review and remediation.

(b) In general, client review and remediation will be appropriate if:

(i) a systemic issue has been identified that is a result of the decisions, omissions or behaviour of the Licensee, or its advisers, in relation to the provision of personal advice to retail clients; and

(ii) the affected clients may have suffered a loss or detriment.

(c) The aim of the review and remediation is generally to place affected clients in the position they would have been in if the misconduct or other compliance failure had not occurred.

7.6 What does client review and remediation involve?

(a) If a review and remediation program is to be commenced, the Licensee will have regard to *ASIC Regulatory Guide 256: Client review and remediation conducted by advice licensees* and design the review and remediation program accordingly.

(b) In particular, the Licensee will have regard to matters such as:

(i) **Scope of review and remediation** - The scope of review and remediation will often depend on the type of misconduct or other compliance failure, the size and structure of the adviser's business, and the size of its client base. There is no one-size-fits-all approach to determining the appropriate scope of review and remediation. The scope of review and remediation should be determined in a way that ensures it covers the right advisers, the right clients and the right timeframe.

(ii) **Design and implementation of review and remediation** - The process of review and remediation should be comprehensive, timely, fair, and transparent. There should be clearly defined principles to guide the process and an appropriate governance structure (including oversight by a senior person). The process should also be straightforward for the client.

In some situations, it may also be appropriate for the Licensee to engage an independent expert to provide assurance about the governance and operation of the review and remediation.

(iii) **Communicating with clients** - Effective, timely and targeted communication is key to ensuring that clients understand the review and remediation and how it will affect them. The Licensee will require the adviser to proactively contact potentially affected clients and

consider the best way to do this in light of the client base and appropriate methods of communication.

(iv) **External review of decisions** - It is important that clients have access to the Licensee's external dispute resolution scheme (Australian Financial Complaints Authority) if they are not satisfied with the decision made in relation to whether misconduct or other compliance failure has occurred and whether remediation is appropriate, and about the nature of remediation offered.

7.7 Internal corrective measures

(a) In addition to co-operating with the Licensee, the Licensee may also require the adviser to undergo specific training and/or enhanced monitoring and supervision for a specific period.

(b) Some remediation actions that may be required from a Licensee perspective include:

(i) Undergoing a period of pre-vetting of the advice they produce to ensure it is of an appropriate standard;

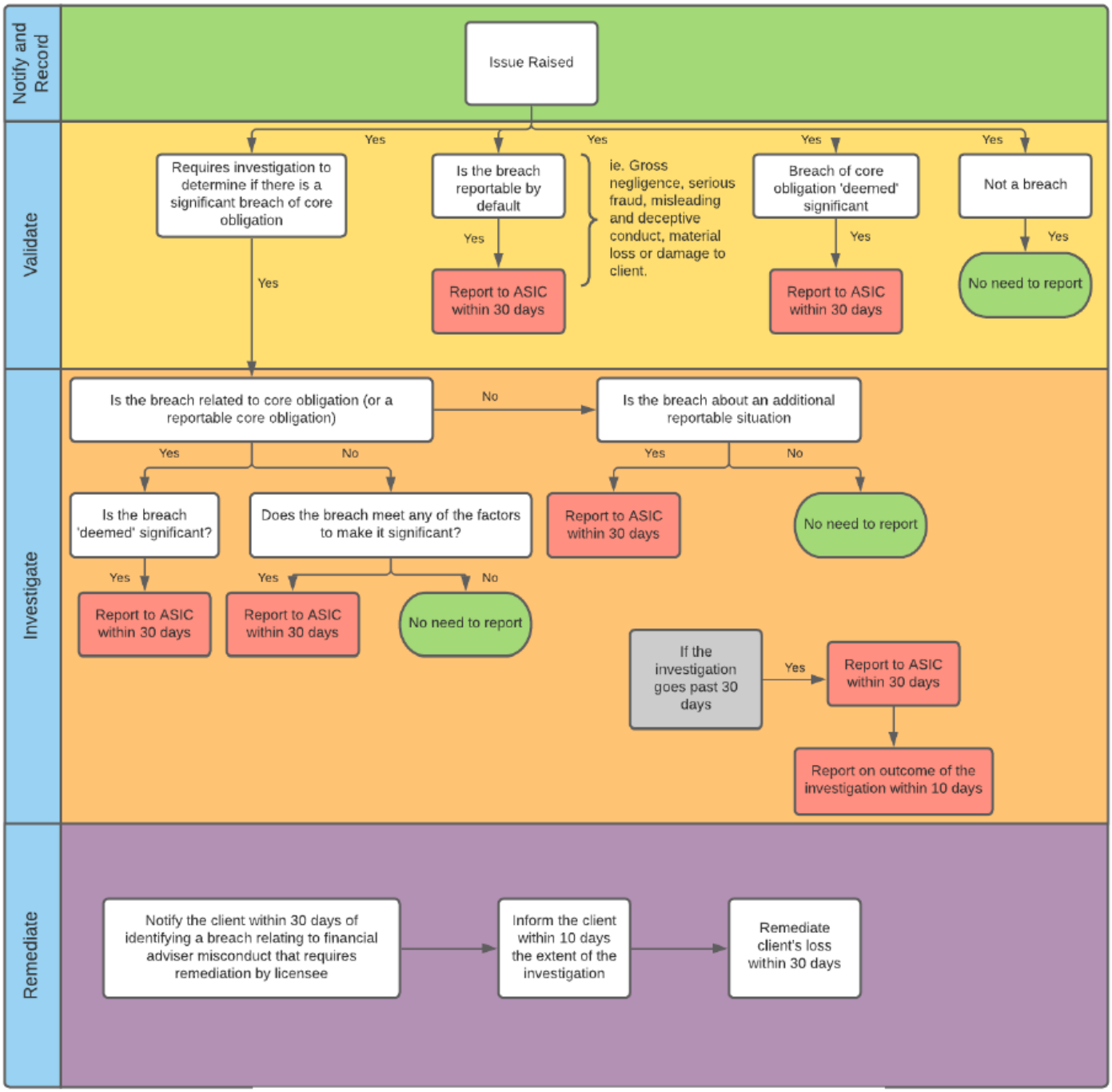
(ii) Undertaking specific training and assessment or performance coaching in accordance with a performance plan;

(iii) Suspension or termination of advice authorisations; and

(iv) Withholding and/or offsetting commissions and fees otherwise payable to the adviser against the costs and expenses incurred by the Licensee to carry out a review and remediation program.

8 Appendix A: Decision-Making Matrix for Reportable Situations

The Licensee will follow the decision-making process set out in the matrix below in determining if, and when, to lodge a report with ASIC



9 Appendix B: The Reportable Situation form

9.1 Lodging a reportable situation report with ASIC

The Licensee must report to ASIC using the prescribed form set out below.

What to include	Description of content
Date of the breach of the reportable situation	The report must include: • The date that the reportable situation arose or the date you anticipate that you will no longer be able to comply with your obligations; and • the date you first knew that there were reasonable grounds to believe that a reportable situation had arisen.
Nature of the reportable situation	The report must state whether it relates to: • a significant breach of a core obligation; • a likely significant breach of a core obligation; • an additional reportable situation (serious fraud or gross negligence); • an investigation into whether a breach (or likely breach) of a core obligation has occurred that has continued for more than 30 days; • an investigation into whether a breach (or likely breach) of a core obligation has occurred that has continued for more than 30 days that discloses that no reportable situation has occurred; or • a reportable situation about another licensee.
Description of the reportable situation	The report must describe the reportable situation, including the section of the Corporations Act that sets out the relevant obligation, including any relevant financial services law and any relevant AFS licence condition.
Instances of the reportable situation (if relevant)	The report must specify how many reportable situations relate to the breach or likely breach that is being reported. Reportable situations are related when they arise from a single specific root cause.
Why the breach is significant (if relevant)	Where relevant, the report must identify why the breach is significant. This may involve: • identifying that the reportable situation relates to a deemed significant breach; or • identifying the factors in s912D(5) of the Corporations Act that the Licensee considers apply in determining whether the breach (or likely breach) is significant and required to be reported to ASIC.
How the reportable situation was identified	The report must include details of how the Licensee found out about the reportable situation. For example, the reportable situation may have been identified

	through its compliance arrangements, an audit or review, or as a result of a client complaint
How long the breach lasted	The report must include all details as relevant, including whether the breach is continuing.
Information about representatives	If an authorised representative is involved, you must include: • that representative's name and number; • if the representative's authorisation has been revoked or suspended; and • if the representative's work is being monitored or supervised.
Whether and how the reportable situation has been rectified	Where relevant, the Licensee must provide details of plans to rectify the breach (or likely breach). This includes: • when the Licensee expects to complete the rectification (or complete a plan for rectifying the breach); and • how the rectification will be achieved. If ongoing steps are being taken to rectify the breach (or likely breach), the report must indicate when the Licensee expects to send ASIC a report on its progress in rectifying it, as well as a notification that rectification is complete.
Whether and when affected clients have been compensated - Remediation	The Licensee must provide details of any remediation program (including preventative measures) that has been or is being developed to compensate clients that have suffered a loss. The report must include relevant dates or expected dates for the start and conclusion of the remediation program. The Licensee should also provide information about completion of remediation.
Future compliance	The Licensee must describe any steps that have been, or will be, taken to ensure future compliance with the obligation.