BREACH MANAGEMENT POLICY

Purpose

To have a documented Breach Management program that records and reviews incidents, breaches or likely breaches of our general obligations as an AFS licensee or of financial services law. The Complaint Management program sets out the process for dealing with complaints.

PROCEDURES – THE REPORTING OFFICER MUST TARGET THAT	
1	All incidents, breaches or likely breaches and suspected or possible reportable situations are entered into the Breach Register in a timely and efficient manner including breaches by an outsourced service provider.
2	We assess and determine whether an identified incident is a reportable situation, including timely and appropriately resourced investigations as required.
3	All reportable situations are reported firstly to the Compliance and Risk Management Committee and then to ASIC within 30 calendar days of us becoming aware of a situation or breach.
4	The consequences of breaches are dealt with, including client communication and compensation.
5	We review breaches to prevent their recurrence and to identify any systemic issues.
6	Complaints are acknowledged within 24 hours and a final written outcome of the complaint is provided to the complainant in a timely fashion and within a maximum of 30 days.
7	Our Complaints Register is kept up to date and identifies any systemic issues.

Breaches

The Compliance and Risk Management Committee maintains the Breach Register and oversee the recording and escalation of all incidents and breaches.

Periodic training is conducted on managing breaches for relevant staff.

Arrangements for recording and reporting breaches

Consideration needs to be given to all breaches of the conditions of the licence and of the law applying to us as an AFS licensee. This includes potential breaches which have not, but are likely, to occur.

It is important that all breaches are considered, as systemic incidents need to be identified and prevented. Reportable situations concerning the AFSL or certain obligations relating to financial services law needs to be reported to ASIC within 30 days of us becoming aware of the situation.

We always need to rectify a breach and prevent a recurrence by identifying how the breach occurred.

What is a 'reportable situation'?

You must report to ASIC all 'reportable situations', including:

- Breaches or 'likely breaches' of core obligation that are significant;

- Investigations into breaches or likely breaches of core obligations that are significant;
- Additional reportable situations; and
- Reportable situations about other licensees.

What is a Significant Breach?

You must report any breach or likely breach of a core obligation if the breach is significant. There are two ways to determine whether a breach is significant; deemed significant breaches and other breaches that may be significant.

In determining whether a breach is significant, you should first consider whether a breach is a deemed significant breach. Only if it is not such a breach should you proceed to determine whether it is other breaches that are significant.

What are 'deemed significant breaches'?

Certain breaches of core obligation are taken to be deemed significant breaches. If a breach is a deemed significant breach, no additional steps are needed to determine whether the breach is 'significant' before reporting to ASIC.

Deemed significant breaches include:

- Breaches that constitute the commission of an offence and the commission of the offence is punishable on conviction by a penalty that may include imprisonment for, three months or more if the offence involves dishonestly; or 12 months or more in any other case;
- Breaches of a civil penalty provision (if the provision is not exempted under the regulations);
- For credit licensees, breaches that constitute a contravention of a key requirement under s111 of the National Credit Code (except if the key requirement is exempted under the regulations);
- Breaches that contravene s1041H(1) of the Corporations Act 2001 (Cth) or s12DA(1) of the Australian Securities and Investments Commission Act 2001 (Cth) (misleading or deceptive conduct); or
- Breaches that result, or are likely to result, in material loss or damage.

Examples of deemed significant breaches:

- Material loss or damage to clients
- Dishonestly obtaining client funds (criminal offence)
- Governance failures in a responsible entity (civil penalty provision)
- Quality of advice and failure to act in interests of the client (civil penalty provision)
- Misleading deceptive statements in relation to a financial product or service or credit activity (misleading or deceptive conduct)
- Charging prohibited fees to a debtor (key requirement under the National Credit Code)
- Efficiently, honestly, and fairly (civil penalty provision)

Other breaches that are significant

Except for deemed significant breaches and additional reportable situations, a breach (or likely breach) of a core obligation needs to be assessed to determine whether it is significant.

The Factors that determine if a breach is significant include:

- *Frequency* - the greater the number or frequency of similar breaches, the more likely a new breach will be significant. Repeat of a breach may indicate an underlying systemic problem and may mean that the compliance arrangements or resourcing is inadequate.
- *Ability to Supply Financial Services* – if a breach reduces the ability or capacity to supply the financial services, it is likely to be significant.
- *Ensuring Compliance* – if the breaches show broad or systemic inadequacies in our compliance system it is likely to be significant. Important factors to consider are how long it took to identify the breach and if the compliance system helped identify it.
- *Actual or Potential Loss to a Client* – a breach of the obligations that causes actual or potential financial loss to clients is likely to be significant. If the breach is an isolated event with minimal loss to a small number of clients, it is less likely to be considered significant.
- *Financial Loss* – a loss, or potential loss, needs to be considered against our financial position as a whole. If it is sizable (or material), or likely to affect the supply of financial services, it is likely to be significant.

Examples of Significant Breaches

- Failure to notify ASIC of changes in key persons
- Failure to follow disclosed investment mandates
- Recurring failure to lodge statutory reports
- Breach of ASIC market integrity rules
- Breach of Internal Dispute Resolution requirements
- Failure to provide key facts sheet
- PI Insurance – failure to maintain the adequate level of PI insurance.
- Cash Flow Projections – failure to prepare cash flow projections.
- Undetected Breaches – failure to identify previous breaches.
- Inappropriate Advice – depends on scale and severity.
- Exceeding License Authorisations – services provided outside the scope of the AFSL.
- Fraud by Adviser or Representative – fraud by an adviser and the failure to prevent it.

When does an investigation become a reportable situation?

You must lodge a report only in relation to investigations that have continued for more than 30 days. The investigation becomes a reportable situation on Day 31 of the investigation, and you must lodge a report within 30 days of this date.

What are additional reportable situations?

Additional reportable situations include when you or your representative:

- Engage in conduct constituting gross negligence while providing a financial service or engaging in a credit activity; or
- Commit a serious fraud.

If an additional reportable situation arises, you must report it to ASIC irrespective of whether it is 'significant'.

What are reportable situations about other licensees?

You must report to ASIC if you have reasonable grounds to believe that a reportable situation, other than a reportable situation arising from an investigation conducted for more than 30 days, has arisen in relation to an individual who:

- Provides personal advice to clients about relevant financial products or is a mortgage broker; and
- Is any of the following:
    - Another AFS licensee or credit licensee;
    - An employee of another AFS licensee or credit licensee (or a related body corporate of another licensee), acting within the scope of the employee's employment;
    - A director of another AFS licensee or credit licensee (or a related body corporate of another licensee), acting within the scope of the director's duties as director; or
    - A representative of another AFS licensee or credit licensee acting within the scope of the representative's authority given by us.
- Examples of reportable situations about other licensees
    - Falsification of loan application documents
    - Advisers transfer from Licensee A to Licensee B

Reporting Breaches

We do not have to report all breaches to ASIC, only those that are significant. Even if a breach is not reportable, it must still be evaluated and addressed, including reviewing processes to target that breaches are not repeated, as well as correction of the breach and compensation as required.

ASIC encourages breaches to be notified to them if we are uncertain if it is significant. The risk of not reporting these breaches, is that ASIC will likely consider a failure to report a significant breach will constitute a significant breach.

How to Report a Breach to ASIC

The breach must be reported in writing by the Board, having first notified the Compliance and Risk Management Committee. The written report should contain the following information:

- Date – The date it occurred and the date that we became aware of it. If it is a likely breach, then the anticipated date.
- Description – include reference to the Corporations Act 2001 (Cth), financial services law or AFSL condition.
- Scheme – include the managed investment scheme to which it relates.
- Significance – the factors considered to make this significant.
- Identification – how was it identified, e.g., by a client or compliance system.
- Duration – how long the breach lasted.
- Rectification – processes and responsibilities for handling the breach, including any remedies (e.g., compensation to clients). If there are ongoing steps, nominate when ASIC will be updated.

- Future – What steps have been taken to target future compliance.

If all the information above is not available when the initial report is made, include the information we do have and supplement it as it becomes available.

The report must be submitted to ASIC using the prescribed form, through the ASIC Regulatory Portal.

The Breach Register

To target that we properly identify and deal with all breaches, every breach (no matter how insignificant) must be recorded in the Breach Register. Examples of breaches include:

- Unauthorised or incorrect trades such as a trade in a security that is not a permitted asset,
- Breaches of a fund mandate,
- Trades that are allocated to an incorrect fund or failing to place a trade in accordance with instructions given.

  Trade breaches are not errors of judgement (investment decisions made in good faith that do not achieve the desired outcome) or errors found and corrected prior to execution.

When you first become aware of a breach, you are required to notify the Compliance Officer and enter it in the Breach Register, where required.

You should do so promptly, but no later than 24 hours after awareness of the breach. If you are uncertain whether a breach has occurred, you must still notify the Compliance Officer so that they can consider whether an entry onto the Breach Register should be made.

The information required will be as detailed as listed above for written reports to ASIC of significant breaches of the AFSL.

Timeline for reporting

We must lodge a report with ASIC within 30 days after we first know that, or are reckless with respect to whether, there are reasonable grounds to believe a reportable situation has arisen.

Generally, the 30 calendar days (the reporting period) starts on the day we first know that, or are reckless with respect to whether, there are reasonable grounds to believe that a reportable situation has arisen. The process may be extended to allow a genuine attempt to find out what happened and to decide if the breach is significant; however, we should not wait for a complete investigation, Board consideration, legal advice, attempts to rectify it, or, in the case of a likely breach, until it has actually occurred.