Policy

Title:	**Breach Reporting Policy**
Responsibility:	**Company Secretary / Compliance Manager**

1. Purpose

Cromwell Property Securities Limited (CPS), Cromwell Funds Management Limited (CFM) and Cromwell Real Estate Partners Pty ltd (CRE) (together "Cromwell") are financial services licensees. Additionally, CPS and CFM are responsible entities. As such, Cromwell is obliged to report to ASIC certain breaches and likely breaches of the Corporations Act and its Australian financial services licence.

2. Scope

This Policy applies to all directors, staff and contractors of Cromwell.

This Policy also applies to any Cromwell group entity that is or becomes a financial services licensee or responsible entity.

3. Responsibilities

The Company Secretary will review this Policy each year to ensure it continues to reflect the law and ASIC policy and will ensure all staff are aware of this Policy.

The Compliance Manager is responsible for maintaining the Non-Compliance Register, monitoring the rectification plan and reporting to the Compliance Committee. The Compliance Committee reports all breaches and likely breaches to the Audit and Risk Committee and the Board, via the Company Secretary.

The Compliance Manager also monitors compliance with this Policy.

All staff are responsible for reporting any actual or likely breaches of Cromwell's obligations.

4. References

4.1 Legislation

- Section 912D of the Corporations Act
- Section 601FC(1)(l) of the Corporations Act
- ASIC Regulatory Guide 78: Breach reporting by AFS licensees

5. Policy Content

5.1 What are Cromwell's compliance obligations?

As a financial services licensee, Cromwell has the following obligations:

1. to do all things necessary to ensure that the financial services covered by its licence are supplied efficiently, honestly and fairly;
2. comply with the conditions of its licence;
3. have adequate resources to provide the financial services covered by its licence and to carry out supervisory arrangements;
4. be competent to supply the financial services covered by its licence;
5. have trained and competent representatives;
6. take reasonable steps to ensure that its representatives comply with the financial services laws;
7. have a dispute resolution system for retail clients;
8. have adequate risk management systems;
9. have compensation arrangements for retail clients; and
10. comply with the following financial services laws:
    a) Chapters 5C, 6, 6A, 6B, 6C, 6D, 7 and 9 of the Corporations Act;
    b) Division 2 of Pt 2 of the ASIC Act (unconscionable conduct and consumer protections for financial services); and
    c) any other relevant laws set out in the regulations.

Cromwell will be "likely to" breach an obligation if it becomes aware that at a future time it will be unable to comply with its relevant obligations.

It is important to note that the financial services laws referred to above include obligations to:

- comply with a scheme's constitution;
- not to make any misleading and deceptive statements about a product (whether in a product disclosure statement, information memorandum, flyer, advertisement or otherwise); and
- not to allow a product disclosure statement to become out of date.

Accordingly, if these obligations are breached, the breaches must be dealt with in accordance with this Policy.

5.2 How are breaches and likely breaches identified?

The Legal & Compliance team is responsible for ensuring that all relevant policies and procedures are in place to ensure compliance with the above obligations. This includes ensuring that reasonable steps are taken to make all staff aware of relevant policies, whether by way of making the policies and procedures available on the intranet and directing relevant managers or staff to them or undertaking compulsory training in relation to the policies.

Notwithstanding the role of Legal & Compliance, all staff are responsible for ensuring they are familiar, and comply, with Cromwell's policies.

If any member of staff believes that they have identified an actual or likely breach of Cromwell's compliance obligations (whether as a result of a policy being breached or the staff member's knowledge of a particular requirement) they should immediately notify Legal & Compliance either verbally or by email.

If in doubt, staff should report. Staff should not wait until rectification steps have been agreed upon or undertaken.

Breaches and likely breaches may also be identified as a result of the regular compliance checklists that relevant staff complete each month and/or compliance testing by the Legal & Compliance team in accordance with a managed investment scheme's compliance plan.

Legal & Compliance will confirm whether or not the particular issue is an actual or likely breach of Cromwell's obligations and record the breach appropriately.

5.3 How are breaches documented?

If a breach or likely breach is identified, a Breach Reporting Form will be completed by a member of the Legal & Compliance team. These reports contain all details required for including the breach on the applicable register as well as a detailed explanation and Filesite references to relevant correspondence.

Depending on the assessment of the breach it will be entered on either the Non-Compliance Register or Incidents Register. Entries on the Non-Compliance Register will include breaches of:

- scheme Compliance Plans;
- Corporations Act;
- other legislation (as applicable); and
- service provider agreements.

Any breaches that do not fall into the above categories will be recorded in the Incidents Register. The Incidents Register records breaches of policies and procedures that if not appropriately managed, could result in a breach of Cromwell's obligations. If a particular breach continually appears on the Incidents Register, the Compliance Manager will review the breaches and consider escalating the latest entry to the Non-Compliance Register.

The Non-Compliance Register will include all relevant information including:

- the relevant obligation;
- the date the breach or likely breach was discovered;
- the date the breach occurred (or if it is a likely breach, the date on which it is anticipated that Cromwell will no longer be able to comply with its obligation);
- how long the breach lasted;
- how the breach was identified;
- the rectification plan;
- the date of rectification; and

- if the breach was reported to ASIC, why the breach was considered significant.

The rectification plan will be agreed between the relevant manager and the Compliance Manager. The rectification plan must include appropriate measures to prevent recurrence of the breach (or likely breach).

The Non-Compliance Register will also include any breaches and likely breaches identified by Cromwell's service providers.

5.4 What must be reported to ASIC?

Any significant breach (or likely significant breach) of Cromwell's relevant obligations must be reported to ASIC, in writing, as soon as practicable, and in any case within 10 business days, of Cromwell becoming aware of the breach or likely breach. Provided the Legal & Compliance team are made aware of the breach or likely breach in a timely and efficient manner the 10 business days should not begin until the Legal & Compliance team are made aware of the breach.

If a Cromwell entity is a responsible entity, Cromwell must also report to ASIC as soon as practicable after becoming aware of any breach of the Corporations Act that relates to one of its schemes and has had, or is likely to have, a materially adverse effect on the interests of members. An adverse effect will be material if it is of significance and not trivial or inconsequential.

5.5 When is a breach or likely breach 'significant'?

Whether a breach or a likely breach is significant will depend upon the circumstances and impact of the individual breach or likely breach but particular regard needs to be had to:

- the number or frequency of similar breaches – is there a continuing underlying systemic problem?
- the impact of the breach or likely breach on Cromwell's ability to supply its financial services;
- the extent to which the breach or likely breach indicates that compliance arrangements are not adequate – how long did it take to discover the breach? Did the compliance arrangements identify the breach?
- the actual or potential financial loss to clients – this is likely to be significant unless the breach is isolated, the amount is immaterial or only a small number of clients are affected; and
- the materiality of the actual or potential financial loss to Cromwell.

The above factors can be considered in light of the nature, scale and complexity of Cromwell's business at the time. However, if in doubt, the breach (or likely breach) should be reported to ASIC.

Examples of breaches that may be assessed as 'significant' include: a number of previously undetected compliance breaches, representatives acting outside the scope of Cromwell's licence or a representative's fraud.

The Legal and Compliance team are responsible for assessing whether or not the breach or likely breach is significant. This assessment is documented in the Non-Compliance Register.

5.6 Breach Reporting Process - within Cromwell and to ASIC

The Compliance Manager provides the up-to-date Non-Compliance Register and Incidents Register to the Compliance Committee at each meeting for review and discussion. The Compliance Committee reports all Non-Compliance Register entries in a report to the Board, which also annexes the Non-Compliance Register. The Compliance Committee's report to the Board is also provided to the Audit and Risk Committee.

The Company Secretary is responsible for reporting any significant breaches or likely significant breaches to ASIC. In the absence of the Company Secretary, the Chief Executive Officer or Chief Financial Officer are responsible for reporting any significant breaches or likely significant breaches to ASIC.

The Compliance Manager must be involved in the process of assessing and reporting the significant breach or likely significant breach to ASIC.

ASIC Form FS80 'Notification by an AFS licensee of a significant breach of a licensee's obligations' is available for download from ASIC's website. The form must be downloaded each time notification is required, to ensure the most recent form is used. The completed breach notification can be emailed to ASIC at fsr.breach.reporting@asic.gov.au. The breach notification to ASIC should contain as much of the following information as is available at the time:

- the date that the breach occurred and the date Cromwell became aware of the breach;
- if it is a likely breach, the date from which it is anticipated that Cromwell will not be able to meet its obligations;
- the obligation that has been breached (or is likely to be breached);
- a description of the factors considered in determining whether or not the breach is significant;
- how the breach was identified;
- how long the breach has lasted;
- how the breach was rectified; and
- steps taken to ensure future compliance with the obligation.

If all of the above information is not available at the date of reporting it can be provided subsequently. It is crucial that reporting to ASIC occurs within the required timeframe.

Cromwell must not wait until the following are completed before reporting to ASIC:

1. all possible avenues of investigation have been completed to determine whether or not the breach is significant;
2. the breach or likely breach has been considered by the board of directors;
3. the breach or likely breach has been considered by internal or external legal advisers;
4. the breach has been rectified or some rectification steps have been taken; and/or
5. in the case of a likely breach, the breach has occurred.

6. Version Control

This Policy has been approved and adopted by the Board of CPS, the Board of CFM, and the Board of CRE. Each Board approved changes on 28 June 2017.

The Company Secretary is responsible for reviewing the Policy at least annually and will seek Board approval for any material changes to the Policy.

Last reviewed June 2018. No changes required.