ASIC
Australian Securities & Investments Commission

PETER KELL
Deputy Chairman

Level 5, 100 Market Street, Sydney
GPO Box 9827 Sydney NSW 2001
DX 653 Sydney

Telephone: + 61 2 9911 5760
Facsimile: +61 2 9911 2414

Our Reference: CCU-14\0429

16 September 2014

Ms Julie Young
Executive Officer & Company Secretary
The Institute of Internal Auditors Australia
PO Box A2311
SYDNEY SOUTH NSW 1235

Dear Ms Young

**Guidance on breach reporting to ASIC**

Thank you for your letter dated 3 July 2014 seeking guidance from ASIC on behalf of members of the Institute of Internal Auditors Australia on complying with the breach reporting obligations in section 912D of the *Corporations Act 2001* (Corporations Act).

**Breach reporting obligations**

Breach reporting by Australian Financial Services (AFS) licensees forms an important part of the financial services regulatory framework. Reporting to ASIC in a timely way helps us to identify and address problems with individual financial services businesses, as well as assisting us to identify and assess emerging risks and issues.

Under section 912D of the Corporations Act, AFS licensees must report significant breaches to ASIC as soon as practicable and in any case within 10 business days after becoming aware of a breach.

ASIC takes this opportunity to stress to members of the Institute of Internal Auditors Australia who hold compliance roles within AFS licensees of the importance in lodging breach reports with ASIC promptly.

If ASIC has concerns with the timeliness of an AFS licensee lodging a breach report with us, ASIC may consider further action against the AFS licensee in relation to this issue, in addition to any further action in response to the reported breach. ASIC has previously taken enforcement action against AFS licensees or accepted enforceable undertakings from AFS licensees in relation to their compliance with breach reporting obligations.

**Your compliance interpretations**

We understand that members of the Institute of Internal Auditors Australia have discussed two interpretations of how they can comply with section 912D of the Corporations Act. Your letter sets out these as 'Interpretation 1' and 'Interpretation 2'.

Broadly, we understand that these interpretations differ as to when the period to report a breach to ASIC commences, including the finding that the breach is significant. For Interpretation 1, the obligation commences from when the compliance unit becomes aware of the breach, and for Interpretation 2, the obligation commences after a view is formed by senior staff following internal investigation by the compliance unit and escalation within the licensee.

**ASIC consideration**

ASIC does not administer the law on the basis of Interpretation 2. We consider that Interpretation 2 would appear to defeat the legislative intention of timely breach reporting by AFS licensees.

We consider that Interpretation 1 is a considerably more accurate description of the basis on which ASIC administers the law. See Regulatory Guide 78 *Breach reporting by AFS licensees*, which states:

> 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'.
>
> ...
>
> 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.

You advised that many of your members are employed by Authorised Deposit-taking Institutions (ADIs). Please note that ASIC's position applies to all AFS licensees regardless of whether they are an ADI.

We thank you again for considering this issue and engaging with us about it. As we have previously discussed, ASIC intends to publish our correspondence on ASIC's website for the assistance of all AFS licensees. We trust that our comments will be of assistance to your members and AFS licensees in complying with their obligations.

Please contact Michael Saadat, Senior Executive Leader – Deposit Takers, Credit & Insurers, if you have any questions in relation to this letter.

Yours sincerely

**Peter Kell**
**Deputy Chairman**