COMMUNITY
BROKER
NETWORK

Group Breach & Risk Event Procedure

November 2019

Navigating through the manual

This manual is designed to be used electronically. To go to a particular section of the manual, locate the item in the table of contents, hold down the "CTRL" key and then click *on the item* with the left mouse button.

Within the manual there are links to many documents and templates. These are highlighted throughout the manual in blue and underlined. To view them, hold down the "CTRL" key and then click *on the item* with the left mouse button.

Exit the document you have just viewed by clicking on the x in the right hand corner and this will return you to the manual.

Contents

BACKGROUND

Community Broker Network (CBN) is committed to ensuring that there are effective compliance processes and measures in place throughout the organisation to comply with legislative and industry code obligations and ensure adherence to internal policies and procedures.

This procedure details the approach adopted by CBN to ensure the identification, recording, monitoring and rectification of risk events and breaches.

This procedure applies to all employees of CBN and its Authorised Brokers. Identifying and managing breaches in the organisation is an essential part of CBN's compliance culture and everyone is responsible for ensuring that the appropriate action is taken.

The Risk & Compliance Team will ensure that training on the breach reporting process is conducted for all staff and Authorised Brokers at induction and on an ongoing basis.

What is a breach?

A failure to comply with legislation, industry code and contractual arrangements.

What is a risk event?

A failure to comply with internal policies and procedures not required by legislation or industry codes.

OBJECTIVE

The intent of this procedure is to:

- provide a systematic process for the reporting, recording and investigation of compliance risk events, breaches and likely breaches to enable proactive prevention in the future; and
- encourage all staff members and Authorised Brokers to be proactive and raise compliance issues that are of concern as soon as possible to prevent escalation.

The identification, management and reporting of breaches and risk events is important as it provides an opportunity to learn from mistakes and review and improve in the areas where the breach or risk event occurred.

All staff and Authorised Brokers are expected to take a proactive approach to the identification, management and reporting of all breaches and risk events that have occurred, or are likely to occur. They are all expected to comply with the requirements of this procedure. CBN may take disciplinary action against any staff member or Authorised Brokers involved in a contravention of this procedure.

This procedure is also intended to address the breach reporting obligations under:

- s912D of the Corporations Act 2001;

- RG78 – Breach reporting by AFS Licensees and RG104 – Licensing – Meeting the general obligations; and

- the Privacy Amendment (Notifiable Data Breaches) Act 2017

This procedure aims to provide a clear, well-understood and documented process for:

- identifying risk events, breaches or likely breaches;

- ensuring that the relevant people responsible are aware of those risk events, breaches or likely breaches;

- determining whether identified breaches or likely breaches are significant;

- reporting to ASIC those breaches or likely breaches that are significant;

- reporting to OIAC and the affected individuals those breaches deemed as notifiable data breaches;

- where appropriate, rectifying the risk event, breach or likely breach; and

- ensuring that arrangements are in place to prevent recurrence of the risk event, breach or likely breach.

OVERVIEW

There are a considerable number of laws that apply to our business and several industry codes that CBN subscribe to such as:

- Insurance Brokers' Code of Practice;
- Privacy Act 1988;
- The Insurance Act 1973
- The Insurance Contracts Act 1984
- Spam Act 2003;
- Competition and Consumer Act 2010 and Fair Trading Acts;
- Federal and State employment laws;
- Occupational health & safety legislation;
- Anti-discrimination legislation;
- Taxation legislation;
- NIBA Code of Conduct

Further information is available from the Risk & Compliance Team.

Corporations Act 2001

As an AFS Licensee, under s912D of the Corporations Act 2001 CBN must provide ASIC with 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:

- an authorised broker or CBN breach any of the specified obligations; or
- an authorised broker or CBN are likely to breach any of the specified obligations; and
- that breach (or likely breach) is 'significant'.

If CBN do not inform ASIC about a significant breach (or likely breach) then ASIC considers this in itself a significant breach.

Table 1: Summary of your obligations to report breaches

Your obligations under s912A and 912B	Your obligation under s912A(1)(c)
You must: • 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.	You must comply with the following financial services laws: • 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.

Only likely breaches, or 'significant' breaches must be reported. Whether a breach (or likely breach) is significant or not will depend on the individual circumstances of the breach and will be determined by the Risk & Compliance Team.

Notifiable Data Breach Scheme

The Privacy Amendment (Notifiable Data Breaches) Act 2017, which amends the Privacy Act 1988 came into force on 22 February 2018. The NDB Scheme imposes notification obligations in the event of an eligible data breach. Where CBN receives a report of a data breach or suspects there may be a data breach it is required to undertake an assessment to identify whether there are reasonable grounds to believe that there is an eligible data breach.

In order for a data breach to be notifiable, there must be unauthorised access to or disclosure of personal information, or a loss of personal information. In addition, the data breach must be likely to result in serious harm to any of the individuals whose personal information was part of the data breach. There are a number of aspects to consider when determining whether serious harm is likely including, the circumstances of the breach (number of affected individuals and type of individual) and the nature of the harm (financial, psychological etc.).

In the event that a potential notifiable data breach is identified CBN must also consider whether it has taken or can take remedial action. If remedial action removes the likelihood of serious harm, then there is no eligible data breach and no notification is required.

Where there is a notifiable data breach, CBN are required to notify the Office of the Australian Information Commissioner (OAIC) and the individuals whose information have been breached. This assessment must be made as soon as practiacable and no later than 30 days of CBN becoming aware of the potential eligible data breach.

BREACH MANAGEMENT PROCESS

Identification and Notification

Breaches and risk events can be identified in several different ways including, but not limited to:

- complaints and disputes;
- audits;
- quarterly declarations;
- monitoring and Supervision; and
- conflicts of interest.

When a breach or risk event has been identified it should be immediately reported to the Risk & Compliance Team using the form on The D.O.C.K.

Assessment & Regulatory Reporting

Upon receipt of the notification, the Risk & Compliance Team will conduct an initial assessment to establish whether the incident is a risk event or breach and log within the Risk Event & Breach Register.

If identified as a breach the Risk & Compliance Team, in conjunction with the Governance & Legal Manager, will determine whether any breach or likely breach is potentially significant and reportable, having regard to the relevant factors contained in the *Corporations Act 2001* and the *NDB Scheme*. If deemed reportable the CEO will be notified and, if appropriate, the matter will be referred to an external party to obtain any necessary legal or other advice. The CEO will also provide details to the Board as soon as possible, but in any event not later than 4 business days after becoming aware of the reportable breach or likely breach. This will allow for CBN to comply with the relevant 10 day timeframe for ASIC and 30 day time line for the OIAC.

In some cases, not all information will be available at the time the breach is identified. This should not delay the assessment of the breach and the possible reporting obligations however, the breach will be recorded in The D.O.C.K. immediately.

No blame will be attached to the reporting of accidental breaches or those identifying process errors. However, it should be noted that staff or Authorised Brokers committing deliberate or negligent breaches maybe subject to disciplinary processes or regulatory/criminal actions (where applicable and/or appropriate).

RESPONSIBILITIES IN RELATION TO BREACHES

All internal staff, Authorised Brokers and consultants have a responsibility to comply with applicable financial services laws and internal policies. In the event that any of them become aware of a risk event, breach or a likely breach of any of these requirements, they must follow the company procedure in relation to the reporting and management of the breach.

There is no legislative requirement to maintain a breach register however, to ensure best practice CBN have implemented The D.O.C.K. as a tool for reporting and monitoring breaches.

State Managers have a responsibility to:

- report all risk events, breaches or likely breaches to the Risk & Compliance Team; and
- aid in the investigation of a breach and help develop a proposed course of action to rectify the breach or prevent the likely breach occurring in consultation with the Risk & Compliance Team, and after obtaining appropriate legal or other advice ensure that the appropriate corrective action has been taken to rectify the breach or likely breach to prevent it from recurring.

The Risk & Compliance Team are responsible for:

- ensuring all risk events, breaches and likely breaches of which they are aware of are recorded;

- investigating the circumstances of all reported risk events, breaches and likely breaches.

- reporting to the General Manager, Operations

  - all potentially reportable breaches or likely breaches as soon as possible; and
  - all other breaches at least quarterly;

and

- reporting all significant breaches or likely breaches to ASIC and notifiable data breaches to the OIAC as soon as possible.

PROCEDURE REVIEW

The Risk & Compliance Team will review this Policy at least annually to ensure it remains relevant, current and compliant with all applicable laws governing our relevant activities and functions.

The State Managers will monitor their relevant Authorised Brokers on a regular basis and will immediately report any risk events, breach or likely breach to the Risk & Compliance Team.

DOCUMENT HISTORY AND VERSION CONTROL RECORD

Name of Document: Group Breach Procedure

Assigned review period: 12 months

Date of next review: November 2019

Version Number	Version Date	Reviewed by	Amendment Details
V2	**July 19**	**Emma Cansell**	**Rebranded**
V3	**Nov 19**	**Emma Cansell**	**Minor language updates, including updates to titles and roles.**