ASIC
Australian Securities & Investments Commission

CONSULTATION PAPER 128

# Handling confidential information

December 2009

## About this paper

This consultation paper contains our proposals for best practice relating to the handling of confidential information, primarily in the context of capital raisings and mergers and acquisitions.

The proposed guidelines are designed to help companies, advisers and other service providers raise the standard of their policies and procedures to reduce the occurrence of market-sensitive leaks. We are seeking views on the draft guidelines from companies, advisers and other service providers who handle market-sensitive information to ensure they are appropriate and will be effective.

We have attached a draft regulatory guide reflecting the proposals outlined in this paper.

**About ASIC regulatory documents**

In administering legislation ASIC issues the following types of regulatory documents.

**Consultation papers**: seek feedback from stakeholders on matters ASIC is considering, such as proposed relief or proposed regulatory guidance.

**Regulatory guides**: give guidance to regulated entities by:

- explaining when and how ASIC will exercise specific powers under legislation (primarily the Corporations Act)
- explaining how ASIC interprets the law
- describing the principles underlying ASIC's approach
- giving practical guidance (e.g. describing the steps of a process such as applying for a licence or giving practical examples of how regulated entities may decide to meet their obligations).

**Information sheets**: provide concise guidance on a specific process or compliance issue or an overview of detailed guidance.

**Reports**: describe ASIC compliance or relief activity or the results of a research project.

## Document history

This paper was issued on 21 December 2009 and is based on the *Corporations Act 2001* as at 21 December 2009.

## Disclaimer

The proposals, explanations and examples in this paper do not constitute legal advice. They are also at a preliminary stage only. Our conclusions and views may change as a result of the comments we receive or as other circumstances change.

# Contents

# The consultation process

You are invited to comment on the proposals in this paper, which are only an indication of the approach we may take and are not our final policy.

As well as responding to the specific proposals and questions, we also ask you to comment on any other aspect of the attached best practice guidelines and to describe any alternative approaches you think would achieve our objectives.

We are keen to fully understand and assess the financial and other impacts of our proposals and any alternative approaches. Therefore, we ask you to comment on:

- the likely compliance costs;
- the likely effect on competition; and
- other impacts, costs and benefits.

Where possible, we are seeking both quantitative and qualitative information.

We are also keen to hear from you on any other issues you consider important.

Your comments will help us develop our policy on the handling of confidential information by listed companies and their advisers and service providers. In particular, any information about compliance costs, impacts on competition and other impacts, costs and benefits will be taken into account if we prepare a Business Cost Calculator Report and/or a Regulation Impact Statement: see Section F Regulatory and financial impact, p. 23.

## Making a submission

We will not treat your submission as confidential unless you specifically request that we treat the whole or part of it (such as any financial information) as confidential.

Comments should be sent by 21 February 2010 to:

Kate O'Rourke
Senior Manager
Corporations
Australian Securities and Investments Commission
GPO Box 9827
Sydney NSW 2001
facsimile: (02) 9911 2369
email: kate o'rourke@asic.gov.au

## What will happen next?

| | | |
|---|---|---|
| **Stage 1** | 21 December 2009 | ASIC consultation paper released |
| **Stage 2** | 21 February 2010 | Comments due on consultation paper |
| | February–March 2010 | Drafting of regulatory guide |
| **Stage 3** | April 2010 | Regulatory guide released |

# A Background to the proposals

**Key points**

The proper handling of confidential information promotes market integrity and efficiency by reducing the risk of leaks or insider trading. It empowers a company to manage the timely release of its information in accordance with the continuous disclosure rules.

It is the responsibility of all companies, advisers and other service providers to ensure their own policies and procedures for handling confidential information are sufficiently robust and effective to minimise the risk of leaks.

We propose to establish and publish best practice guidelines (see attached draft regulatory guide) on the handling of confidential information so that parties can benchmark themselves against best practice with a view to strengthening their own controls and adopting procedures appropriate to the nature, scale and complexity of their business.

## Introduction

1 ASIC is concerned about the leakage of price-sensitive confidential information about transactions prior to their announcement to the market.

2 Over the past financial year we have observed abnormal stock market trading immediately prior to the announcement of a reasonably high number of capital raisings and merger and acquisition transactions. There also appears to have been considerable leakage of inside information to the media prior to the formal announcement of transactions. Both of these issues raise concerns about the practices of companies, advisers and other service providers in handling confidential information.

3 The misuse of confidential information about a possible corporate transaction poses a number of serious risks to the company conducting the transaction. These include:

- the risk that the transaction as a whole, or an important aspect of it such as its pricing, will be jeopardised or that the company will otherwise have its business or reputation damaged;
- the risk that the company will be in breach of its continuous disclosure obligations under Ch 3 of the ASX Listing Rules;
- the risk that an employee or board member of the company will engage in insider trading in breach of s1043 of the *Corporations Act 2001* (Corporations Act);

- the risk that an employee or board member will trade in breach of the company's share trading policy; and
- the risk that possible disclosure will constitute pre-prospectus advertising in breach of s734 of the Corporations Act.

4 The misuse of confidential information can also pose risks to the advisers and other service providers a company engages to assist with corporate transactions (including investment banks, trading banks, lawyers, accountants, tax advisers, credit rating agencies, media relations firms and printers). Deliberate misuse of, or carelessness with, a client's information can damage the adviser's business, as well as the client's. It may also constitute insider trading by an employee of an adviser or a breach of an adviser's AFS licence.

5 ASIC believes that it is the responsibility of all parties to ensure their own systems and procedures are sufficiently robust and effective to minimise the risk of leaks to the maximum extent possible.

6 To assist companies and advisers in improving their systems, we undertook a project to better understand current market practices in relation to the handling of confidential information. Based on the best practices we observed in that review, we are proposing best practice guidelines (see attached draft regulatory guide) on the handling of confidential information. These guidelines can be used by companies, advisers and other service providers to benchmark themselves against best practice with a view to strengthening their own controls and adopting procedures appropriate to the nature, scale and complexity of their business.

## Overview of the Confidential Information Project

7 ASIC's Confidential Information Project, which was conducted over the course of 2009, focused on the handling of confidential information, primarily in the context of capital raisings and mergers and acquisitions. We identified a number of recent capital raisings and merger and acquisition transactions. In relation to some of these transactions, there had been abnormal stock market trading immediately prior to the transaction announcement.

8 To better understand existing market practices relating to the handling of confidential information in the context of actual transactions, we met with the companies involved in these transactions. Our discussions were undertaken on an informal, voluntary and confidential basis and covered topics including:

- the company's internal policies, practices and controls for handling confidential information;

- how the company engaged and communicated with third parties during confidential transactions; and
- how the company ensured its employees understood and complied with its policies on handling confidential information, including personal account dealing.

9 We also met with many of the advisers and service providers to the companies involved in these transactions including lawyers, investment banks, brokers, accountants, public relations firms and trading banks. In some cases advisers discussed their firm's policies and controls in relation to handling confidential information more generally, rather than in relation to any specific transaction, and commented on risk areas and general market practice.

10 To assist us in formulating our best practice guidelines, we also spoke with a number of other market participants including institutions, fund managers, industry bodies and corporate advisers.

11 In proposing best practice guidelines for the handling of confidential information we recognise that individual companies and advisory firms in receipt of confidential information need to consider their own needs and circumstances when implementing these policies and procedures.

## Areas covered by the best practice guidelines

12 Our proposed best practice guidelines describe systems that companies can adopt to maximise the protection of confidential information and implement more effective risk management. They cover:

- implementing the 'need-to-know' principle;
- information barriers, IT controls and physical document management;
- insider lists for sensitive transactions; and
- personal confidentiality obligations and personal account dealing.

13 The guidelines also set out the steps a company should take when providing confidential information to its advisers to minimise the risk of leaks or insider trading. These include:

- ensuring advisers have systems in place which, at a minimum, comply with the company's own practices for handling confidential information;
- executing specific confidentiality agreements and general umbrella agreements; and
- implementing strict controls around 'beauty parades' for the appointment of advisers.

14 The best practice guidelines provide guidance on how advisers and other service providers should handle confidential information and they should assist advisers in complying with their existing fiduciary and other legal obligations to their clients. We also provide best practice guidelines for sounding the market prior to a capital raising or other transaction.

15 This consultation paper discusses in detail only some of the proposed best practice guidelines in the regulatory guide. We would, however, encourage comments on all aspects of the proposed guidance.

## International practice

16 The current market practice around the protection of confidential information varies considerably in Australia, and in many respects falls short of practice in other jurisdictions such as the United States, United Kingdom and Hong Kong. In developing our best practice guidelines, we considered the guidance published by the Financial Services Authority in the United Kingdom, guidance published by the Hong Kong Financial Services Commission and market practices in the United States. If adopted, our best practice guidelines would bring Australia into line with international best practice, and most closely align us with UK market practices.

## Other relevant ASIC publications

17 The guidelines should be read in the context of previous guidance we have published on related areas including:

- Consultation Paper 5 *'Heard it on the grapevine'* (CP 5) released in November 1999;
- Regulatory Guide 181 *Licensing: Managing conflicts of interest* (RG 181) released in August 2004;
- Regulatory Guide 79 *Managing conflicts of interest: A guide for research report providers* (RG 79) released in November 2004; and
- Consultation Paper 118 *Responsible handling of rumours* (CP 118) released in September 2009.

18 In this consultation paper, any reference to companies should be understood to include other entities such as trusts, and references to shares should be understood to include other financial products including units and derivatives.

# B Proposal: Best practice guidelines

**Key points**

We believe best practice guidelines are the most appropriate mechanism through which to raise the standard of confidential information handling by companies, their advisers and other service providers at this point in time.

## Proposal

**B1** In order to raise standards in the market relating to the handling of confidential information, we propose to issue best practice guidelines for corporate transactions primarily in the context of capital raisings and mergers and acquisitions. This will allow parties to benchmark themselves against best practice with a view to strengthening their own controls and adopting procedures appropriate to the nature, scale and complexity of their business and the transaction in hand.

*Your feedback*

B1Q1 Are best practice guidelines the appropriate mechanism or should ASIC pursue other regulatory approaches such as licence conditions, changes to the ASX Listing Rules, incorporation of the guidelines into the ASX's Corporate Governance Principles and Recommendations, industry codes or law reform?

## Rationale

19 Best practice guidelines are designed to complement existing fiduciary and other legal obligations relating to parties' handling of confidential information. Companies, their advisers and other service providers should already have their own policies and practices in place to ensure they comply with their legal obligations. We see best practice guidelines as building on and improving current standards across the market as a whole. The benefit of best practice guidelines is that parties will be able to critically assess their existing policies and practices and make any changes where required. The guidelines are also flexible, enabling developmental and proportionate practices.

20 The alternative approaches mentioned in question B1Q1 would take considerably longer to implement and may not cover all segments of the market. It may be more appropriate for one or more of these options to supplement or supersede our best practice guidelines in the future, should further regulation be required.

# C Proposals: Internal corporate policies and procedures

**Key points**

Our best practice guidelines aim to set out standards for internal policies and practices for companies, their advisers and other service providers in relation to the handling of confidential information.

We are consulting the market on the internal corporate policies and procedures that are currently not widely implemented by market participants. These areas include:

- insider lists for sensitive matters;
- classification of documents;
- leak investigations, and
- umbrella agreements.

21 Companies should have clear, documented internal policies that establish standards of behaviour and procedures for the handling of confidential information. These standards of behaviour should be emphasised to all employees, as well as the board of directors, and should be embedded in the culture of the company. It is important that these policies are reviewed regularly, updated where appropriate, and systematically enforced.

22 The proposals we put forward in this section are practices that we think have merit, but which are currently not commonly adopted by market participants.

23 For a complete set of our best practice guidelines covering internal policies and procedures, please refer to paragraphs RG000.14–RG000.29 of our draft regulatory guide, which is attached at page 24 of this consultation paper.

## Insider lists for sensitive matters

**Proposal**

**C1** We propose that companies should maintain a register of all people (both at the company and at the company's advisers) who are insiders on sensitive transactions.

Third-party advisers should be required to provide the company with up-to-date lists of all the people within their firm that have been given access to the company's confidential information. This list should be provided to the company upon engagement and should be updated regularly.

*Your feedback*

C1Q1 Is the company the most appropriate body to hold any insider lists?

C1Q2 Is it appropriate to exclude from insider lists any category of employees of advisers (such as those undertaking solely legal, compliance or management type functions)?

## Rationale

### Companies to maintain insider lists

24 While fundraising and merger and acquisition transactions often have contact lists compiled that include many of the people involved in a transaction, it is rare for a team working on a transaction to have a complete list of insiders.

25 Our best practice guidelines propose that transaction teams create a complete insider list. We believe the benefits of maintaining up-to-date insider lists are threefold:

- if companies are encouraged to keep a complete and proper record of all staff who possess confidential information, this should help limit the number of staff in possession of that confidential information—in other words, the insider list helps to promote the 'need-to-know' principle;
- if a leak is detected or suspected, an insider list would assist in any investigation as it should provide a complete and proper record of all staff in possession of confidential information in relation to the transaction (see proposal C3 for our best practice relating to leak investigations); and
- the existence of the list may act as a deterrent for those on the list therefore discouraging careless or inappropriate behaviour.

26 Our proposal in relation to insider lists is consistent with the EU Market Abuse Directive and UK regulation (Disclosure Rule 2.8), which require an issuer to ensure that it and anyone acting on its behalf draws up and maintains a list of those people with access to inside information.

### Third parties to provide insider lists to companies

27 As a matter of best practice, we see the company as the most appropriate body to hold any insider lists. This is because it is the company's inside information that is being distributed, and because it is the company that is most likely to be adversely affected by any leak of confidential information.

28 We are concerned that, in our discussions, there was sometimes a feeling of powerlessness among listed companies when they suspected a leak had originated from a third party. We believe that requiring advisers and other

service providers to inform the company of all staff who have inside information better positions the company to then question those parties further, should a leak occur.

## Classification of documents

### Proposal

**C2** In the case of major transactions (involving substantial documentation), we suggest best practice may be for information that is created by or given to a company to be classified according to the level of protection it requires. This document classification system could prescribe the specific requirements for creating, distributing and storing each class of information, reflecting the risks relating to loss of confidentiality of that information.

*Your feedback*

C2Q1 Is it too onerous to require all information created by or given to a company to be classified according to the level of protection needed, or would it be helpful in assisting companies to apply the appropriate level of protection to different classes of information?

### Rationale

29 The draft regulatory guide (at paragraph RG 000.20) sets out our best practice guidelines on information barriers and physical document management. A practice we observed only occasionally in the market, but which we believe may be useful in protecting inside information, was to assign classifications to documents according to the level of protection each document required. Basic security procedures can greatly reduce mismanagement of confidential information. A classification system whereby a rating is given to all information created by or given to a company helps identify the level of protection employees should attach to the information and focuses the most stringent controls on sensitive material only.

## Leak investigations

### Proposal

**C3** We suggest it is best practice that when there is a leak, or the suspicion of a leak, of confidential information relating to a specific transaction, a formal (but proportionate) leak investigation should be considered by each party that had access to the confidential information on the transaction.

*Your feedback*

C3Q1 For advisers, should a leak investigation only be conducted if the company requests one?

C3Q2 What barriers do you see limiting or preventing effective investigations into leaks?

### Rationale

30 In our discussions, many companies and advisers were adamant that leaks did not occur from within their organisation. Formal, or even informal, investigations of leaks relating to sensitive transactions were rarely undertaken, meaning that there were no real repercussions stemming from the leak, and thereby making it hard to verify whether leaks did or did not come from a particular organisation.

31 Encouraging parties with access to confidential information relating to a transaction to conduct an effective leak investigation requires parties to take responsibility for ensuring that their employees have not misused that confidential information. Written policies clearly setting out the scope for these investigations should be in place and made available to all employees. Without being able to substantively demonstrate that an investigation into a leak has been undertaken, it is not enough for parties to respond that there is insufficient evidence to suggest a leak has occurred from within their organisation.

32 We acknowledge that even when the best compliance practices are in place, a company cannot control all of its employees' actions. An investigation process that is known to all employees would act as a deterrent, raising awareness and signalling to employees that the matter is taken seriously.

## Umbrella agreements

### Proposal

**C4** We propose that companies that are active participants in mergers and acquisitions or capital raisings and use the services of investment banks and other advisers on a regular basis should have umbrella agreements in place setting out general practices and principles the adviser must adhere to when undertaking work for the company, including how to handle confidential information. These agreements would be entered into prior to any specific transactions and additional side agreements would be negotiated at the time of each transaction.

*Your feedback*

C4Q1 What are the benefits and disadvantages of having umbrella agreements in place of the type set out in C4?

C4Q2 For which companies would this type of arrangement be most useful?

### Rationale

33 When companies are negotiating an urgent capital raising, or merger or acquisition, the confidentiality requirements are often included in agreements that remain unsigned until immediately before the transaction is announced. This is because such agreements also include fees or other negotiated terms. In these circumstances, much confidential information has already passed between companies and their advisers without any formal agreement on how that information will be protected. An alternative would be for companies that regularly conduct transactions to have advance agreements in place with their possible advisers to cover important issues, including how confidential information will be handled prior to disclosure of that information.

## Confidentiality agreements

### Proposal

**C5** We propose that all advisers should be required to sign transaction-specific confidentiality agreements. Among other things, these agreements should specifically restrict an adviser's use of the company's confidential information, including limiting the number of individuals given access to that information. Agreements could also cover conflicts of interest.

*Your feedback*

C5Q1 What are the benefits of confidentiality agreements? Are there any disadvantages?

C5Q2 Should any category of adviser or other service provider be excluded from the requirement to execute confidentiality agreements? If so, on what basis?

### Rationale

34 Engaging advisers or other service providers to assist with price-sensitive transactions will necessitate the release of confidential information. We consider that companies should not rely on past dealings and the professionalism of third parties alone as assurance that confidentiality will be maintained. We expect confidentiality agreements would also cover related issues such as conflicts of interest and dealings with the press.

# D Proposals: Individual obligations

**Key points**

Companies, advisers and other service providers should ensure their employees properly understand their responsibility to keep information confidential.

Highly sensitive transactions require more stringent policies and procedures surrounding confidentiality and may warrant the signing of individual confidentiality agreements.

Personal account dealing policies that are appropriately tailored to the company's or adviser's business and associated risks help to ensure that confidential information is not illegally or improperly used.

## Individual confidentiality agreements

### Proposal

**D1** For highly sensitive transactions, we propose that individuals involved in these transactions (both in the company and at advisory firms or other service providers) should be required to sign individual confidentiality agreements.

*Your feedback*

D1Q1 Is it beneficial to require all staff involved in a sensitive transaction to sign individual confidentiality agreements?

### Rationale

35 We consider policies and procedures aimed at increasing employees' personal responsibility and focusing their minds on the importance of maintaining confidentiality are to be favoured over more general or undocumented policies. From what we have seen, we believe that too much emphasis is placed on implicit confidentiality—that is, where parties rely on unstated, general confidentiality obligations to ensure confidentiality is maintained.

36 In highly sensitive transactions, it is important that stringent measures are adopted. By requiring individual confidentiality agreements to be signed at the commencement of an employee's involvement in a transaction, and thus focusing the employee's mind on their responsibilities, we believe the potential for preserving confidentiality will be enhanced.

37 We acknowledge that in some circumstances it may not be feasible to obtain signed hard copies of individual confidentiality agreements—for example, when a transaction is urgently put together. In these circumstances, some other way for staff to acknowledge their responsibility in maintaining confidentiality would be appropriate.

## Personal account dealing policies and controls

### Proposal

**D2** We propose that listed companies should have restrictions on employees with confidential price-sensitive information trading in the company's financial products in a personal capacity. Companies should provide for:

(a) pre-approval for all trades in the company's financial products by employees who are likely to hold confidential information;

(b) staff being required to provide the nominated company officer with confirmation of the trade immediately after the trade has been executed; alternatively, authorisation should be given to enable the company to receive contract notes directly from the employee's broker; and

(c) staff in sensitive roles being required to disclose all security holdings regularly (e.g. on a semi-annual basis), including those of any person or entity whose investments they control or have influence over.

*Your feedback*

D2Q1 What is an appropriate personal account trading policy for a company to require of its employees?

### Proposal

**D3** We propose that firms in the financial industry who advise on market-sensitive transactions should have personal account dealing policies in place. These policies, based on those adopted by the major investment banks, should, among other things, require:

(a) pre-approval for all trades;

(b) trading restrictions on financial products in a range of different entities; and

(c) agreements to be entered into to provide the advisory firm with contract notes or records of trade for all completed trades.

*Your feedback*

D3Q1 Should these restrictions be mandatory for all investment banks, at least for staff in the advisory and equities areas?

D3Q2 Should law firms have these trading restrictions in place in relation to the financial products of:

(a) all of their clients with whom they have an active, price-sensitive mandate; and

(b) any other entity?

If not, what is an appropriate measure?

D3Q3 Should accounting firms have these trading restrictions in place in relation to the financial products of:

(a) all of their clients with whom they have an active, price-sensitive mandate; and

(b) any other entity?

If not, what is an appropriate measure?

D3Q4 What should be the scope of the trading restrictions that are appropriate for other types of advisers, such as actuaries, valuers, public relations advisers, share registries, trading banks and other service providers? Should all employees be subject to general trading restrictions or only those with access to the price-sensitive confidential information regarding particular stocks? If not through formal policies, in what other ways could staff be discouraged from trading with the benefit of inside information?

## Rationale

### Companies to have personal account dealing policies

38 A well documented and enforced personal account dealing policy will help ensure that employees do not inappropriately use confidential information for their own financial gain. Requiring pre-approval for all trades in the company's financial products will require employees to consider whether they possess any material inside information prior to executing a trade. Employers will also be able to satisfy themselves that they have done all they can to ensure their employees are not acting improperly. Imposing stringent personal account dealing policies and procedures is one way to create a strong culture of proper confidential information handling.

39 Any policy directed at personal account dealing relies predominantly on employee cooperation as an employer has little or no power to prevent an employee from deliberately misusing confidential information. However, the damage caused to a company's reputation if an employee (especially a director) is found to have used confidential information inappropriately and for their own personal gain should not be underestimated. For this reason, it is important for companies to demonstrate the high standards required from their employees and how seriously they should take their responsibility as a holder of confidential information.

### Advisers to have personal account dealing policies

40 Advisers who are in receipt of market-sensitive information should have strict personal account dealing policies in place. This will help to ensure that no employees are trading with the benefit of inside information.

41 It may be appropriate for advisers, depending on the size and nature of their business, to have far more stringent personal account dealing policies than companies. Advisers, such as investment banks and brokers, who deal with confidential information from a range of parties have a significantly greater exposure to market-sensitive information and they should have in place more comprehensive controls.

# E Proposals: Sounding the market

**Key points**

The risk of price-sensitive confidential information being misused is heightened with market soundings.

Investment banks need to ensure they adopt adequate policies and procedures when sounding institutional shareholders.

## Proposal

**E1** We propose that investment banks should adopt the following practices and procedures:

(a) the company should be informed when the bank forms the view it needs to sound the market and the company's approval should be obtained to do so;

(b) soundings should only take place when the market is closed, or the particular stock is in a trading halt, and as few parties as possible should be sounded;

(c) a formal script should be adopted detailing the conversation that individual bankers are permitted to have with the institutions approached for sounding;

(d) when an institution agrees to become an insider, the institution must also agree to comply with insider trading restrictions before any confidential information is communicated. Following this verbal agreement, the investment banker should obtain written confirmation (e.g. by email) from the institution that it agrees to uphold the confidentiality of the information and comply with insider trading restrictions; and

(e) when an investment bank does not have the approval of the company to sound institutions, it should not discuss with institutions any price-sensitive confidential information in relation to that company.

*Your feedback*

E1Q1 In relation to proposal E1(d), should an investment bank be required to obtain written confirmation from the institutional shareholder that it agrees to uphold the confidentiality of the information and comply with insider trading restrictions?

E1Q2 Are there any other practices that should be included in our sounding best practice?

### Proposal

**E2** We propose that within 48 hours of conducting a sounding, an investment bank should notify ASIC of certain details about the sounding including:

(a) the name of all institutions contacted (and the contact person at each) and whether each of them agreed to be made an insider;

(b) the time and date contact was made with each institution as well as details of when the institution was made an insider or refused to become an insider; and

(c) the particular transaction that forms the subject of the sounding.

*Your feedback*

E2Q1 Is it appropriate, as a matter of best practice, for investment banks to provide details of soundings to ASIC within 48 hours of the sounding? If not, why not?

E2Q2 In the context of ASIC moving to active market supervision, is it appropriate for investment banks to notify us in advance of soundings they are intending to undertake?

E2Q3 Are there any other details of soundings that should be provided to us?

E2Q4 Is this an area where an industry code would be beneficial?

## Rationale

42 A company's circumstances, and market conditions in general, will determine whether market soundings are required. In this way, we recognise that sounding potential investors could be an important resource in some circumstances.

43 However, given the sensitivity of information provided and the potentially conflicting interests of parties involved in a market sounding, it is vital that tight controls surround market sounding practices. Our best practice guidelines contained in proposals E1 and E2 are aimed at ensuring that all parties—the company and institutional investors in particular—are properly informed, and fully aware, of the market sounding process and its legal implications.

#### Company approval, and timing, of market soundings

44 As the confidentiality of a sensitive transaction is at risk whenever confidential information is provided to a third party, it is essential that the company consents to any market sounding. The company's consent to make specific institutional shareholders insiders should also be obtained as the company may wish only certain trusted institutional shareholders to be provided with the confidential information.

45 From a market integrity perspective, it is essential that the sounding occurs when the market is closed or while the company's securities are in a trading halt. There must be no opportunity for 'over the wall' investors to trade in the company's securities prior to a formal release of the details of the transaction to ASX.

### Market sounding script

46 The use of a formal market sounding script ensures that the dissemination of confidential information is undertaken in a controlled, systematic and transparent way. There should be little or no variance in the process of ascertaining whether a shareholder wants to be brought 'over the wall'.

### Shareholder confirmation

47 When bringing an investor 'over the wall' an investment bank should satisfy itself that the shareholder will uphold the confidentiality of the information they are given. Requiring written confirmation from the shareholder that they will maintain confidentiality fulfils this end.

### Details of sounded investors

48 In our view, if an investment bank provides details of sounded investors to us, the sounding process will become more transparent. We also believe sounded investors will be deterred from misusing the confidential information because their identity, along with the few other sounded investors, will have been provided to the regulator.

 

# F Regulatory and financial impact

49 In developing the proposals in this paper, we have carefully considered their regulatory and financial impact. On the information currently available to us we think they will strike an appropriate balance between:

(a) increasing the standard of market practice relating to companies' handling of confidential information; and

(b) ensuring that the efficiency of the market in executing transactions is not inhibited through unnecessary and overly burdensome compliance.

50 Before settling on a final policy, we will comply with the requirements of the Office of Best Practice Regulation (OBPR) by:

(a) considering all feasible options;

(b) if regulatory options are under consideration, undertaking a preliminary assessment of the impacts of the options on business and individuals or the economy;

(c) if our proposed option has more than low impact on business and individuals or the economy, consulting with OBPR to determine the appropriate level of regulatory analysis; and

(d) conducting the appropriate level of regulatory analysis, that is, complete a Business Cost Calculator report (BCC report) and/or a Regulation Impact Statement (RIS).

51 All BCC reports and RISs are submitted to the OBPR for approval before we make any final decision. Without an approved BCC Report and/or RIS, ASIC is unable to give relief or make any other form of regulation, including issuing a regulatory guide that contains regulation.

52 To ensure that we are in a position to properly complete any required BCC report or RIS, we ask you to provide us with as much information as you can about:

(a) the likely compliance costs;

(b) the likely effect on competition; and

(c) other impacts, costs and benefits,

of our proposals or any alternative approaches: see 'The consultation process' p. 4.

ASIC
Australian Securities & Investments Commission

REGULATORY GUIDE 000

# Handling confidential information: Best practice guidelines

December 2009

## About this guide

This regulatory guide provides best practice guidelines to help listed companies, their advisers and other service providers to develop and maintain good practices in the handling and control of confidential information, and to promote market practices that reduce the risk of insider trading and non-compliance with continuous disclosure laws.

**About ASIC regulatory documents**

In administering legislation ASIC issues the following types of regulatory documents.

**Consultation papers**: seek feedback from stakeholders on matters ASIC is considering, such as proposed relief or proposed regulatory guidance.

**Regulatory guides**: give guidance to regulated entities by:

- explaining when and how ASIC will exercise specific powers under legislation (primarily the Corporations Act)
- explaining how ASIC interprets the law
- describing the principles underlying ASIC's approach
- giving practical guidance (e.g. describing the steps of a process such as applying for a licence or giving practical examples of how regulated entities may decide to meet their obligations).

**Information sheets**: provide concise guidance on a specific process or compliance issue or an overview of detailed guidance.

**Reports**: describe ASIC compliance or relief activity or the results of a research project.

## Document history

This draft regulatory guide was issued on 21 December 2009 and is based on legislation and regulations as at 21 December 2009.

## Disclaimer

This guide does not constitute legal advice. We encourage you to seek your own professional advice to find out how the *Corporations Act 2001* and other applicable laws apply to you, as it is your responsibility to determine your obligations.

Examples in this guide are purely for illustration; they are not exhaustive and are not intended to impose or imply particular rules or requirements.

# Contents

# A Overview

**Key points**

The proper handling of price-sensitive confidential information promotes market integrity and efficiency by reducing the risk of leaks or insider trading. It empowers a company to manage the timely release of its information in accordance with the continuous disclosure rules.

Companies should have clear internal policies that establish standards of behaviour and procedures around the handling of confidential information.

Companies should also be concerned about, and actively manage, how their advisers and other service providers handle the company's confidential information.

When engaging advisers and other service providers to assist on price-sensitive transactions, companies should ensure that there is an express agreement from the adviser or service provider to maintain the confidentiality of information.

Firms that are in receipt of confidential information from a client, such as investment banks, trading banks, lawyers, accountants, tax advisers, credit ratings agencies, media relations firms and printers, should each adopt policies relating to the handling of confidential information to protect their client's information and interests.

RG 000.1 These draft guidelines have been designed to help companies, their advisers and other service providers to protect price-sensitive confidential information and to avoid any unintentional or deliberate misuse of that information. They are intended to assist parties in complying with their existing obligations under the law such as those relating to continuous disclosure, insider trading and licensing. The guidelines include some suggestions for implementation of the general principles. These measures may need to be tailored to suit the individual requirements and circumstances of each listed company, its advisers and other service providers and should be applied in a proportionate manner, reflecting the level of risk involved. ASIC's aim in publishing these draft guidelines is to encourage companies, their advisers and other service providers to implement and enforce best practice, and not just a minimum level of compliance with the law.

RG 000.2 Confidential information in relation to equity raisings or merger and acquisition activity is often the most price-sensitive and should remain secret until released to ASX. When companies are engaging in these types of transactions, it is particularly important that they and their advisers have robust procedures in place for ensuring inside information remains confidential and that these procedures are rigorously enforced.

RG 000.3 In contrast to large overseas markets, such as the United Kingdom and the United States, there is a considerable amount of speculation in the Australian market and the financial press around potential transactions prior to a formal announcement to ASX. The leakage of information prior to an ASX release undermines market integrity.

RG 000.4 In addition to reviewing international practices in relation to handling confidential information, ASIC observed existing market practices in Australia. Through these best practice guidelines, we are encouraging all companies to adopt and tailor to their own circumstances the good practices we observed.

RG 000.5 In these guidelines, any reference to companies should be understood to include other entities such as trusts, and references to shares should be understood to include other financial products, including units and derivatives.

## Companies' handling of confidential information

RG 000.6 These best practice guidelines describe a set of policies and practices that companies can adopt to maximise the protection of price-sensitive confidential information. They emphasise the importance of minimising the number of people in receipt of confidential information, and quarantining these people to reduce the likelihood that others will inadvertently learn of an impending transaction. Policies in relation to the handling of confidential information should apply to all staff of the company as well as the board of directors.

RG 000.7 Section B describes a range of policies for companies covering:

(a) the 'need-to-know' principle;

(b) information barriers and physical document management;

(c) information technology controls;

(d) insider lists for sensitive transactions; and

(e) compliance with the continuous disclosure regime.

RG 000.8 Section B also describes arrangements companies should implement with their employees to ensure they are mindful of their confidentiality obligations, and to regulate trading by employees. We provide guidance on:

(a) personal confidentiality obligations;

(b) staff training;

(c) personal account dealing and controls; and

(d) exiting employees.

RG 000.9 Finally, Section B sets out our best practice guidance on leak investigations. It encourages companies to have an effective leak investigation policy, and to consider undertaking a formal investigation when a company suspects that its confidential information has been leaked, either by an employee or an adviser.

## Releasing confidential information to third parties

RG 000.10 Companies normally engage advisers and other service providers to assist them with capital raisings or merger and acquisition transactions. When releasing confidential information to those external parties prior to the announcement of a transaction, a company must be confident that each has sufficient policies and procedures of its own to protect that information. Section C sets out the steps a company should consider taking when providing confidential information to its advisers or other service providers to minimise the risk of leaks or insider trading.

RG 000.11 In our guidance we recommend companies:

(a) ensure that advisers and other service providers have systems in place which, at a minimum, are consistent with the company's own practices for handling confidential information;

(b) consider umbrella agreements, which include obligations regarding confidentiality;

(c) have controls that should be implemented before conducting a 'beauty parade' for the appointment of advisers; and

(d) sign confidentiality agreements with parties to whom they provide confidential information.

## Advisers' handling of confidential information

RG 000.12 Advisers and other service providers that receive confidential information from a client need to have appropriate systems in place to ensure that confidential information is not leaked or misused. In many ways these policies need to replicate those adopted at the company level (see Section B). In addition, Section D sets out our guidance for advisers when their systems need to differ from those of the company. The areas where we provide further guidance for advisers include:

(a) insider lists;

(b) confidentiality agreements;

(c) personal account dealing; and

(d) leak investigations.

## Sounding the market

RG 000.13 Section E describes our best practice for investment banks when sounding the market about a possible capital raising or acquisition proposal. Soundings necessarily involve releasing price-sensitive confidential information and great care should be taken to ensure that there is no breach of the continuous disclosure or insider trading laws.

# B Companies' handling of confidential information

Companies should adopt policies and practices to protect price-sensitive confidential information. These policies should emphasise the need-to-know principle and should implement practical steps to ensure non-insiders are not inadvertently made aware of confidential information. Companies should also maintain insider lists for sensitive transactions.

Contact with the media about a possible transaction should be controlled by companies.

Employees of companies should have appropriate confidentiality obligations built into their employment contracts as well as specific agreements for each sensitive transaction. These should be supplemented by training and by personal account dealing policies and controls.

If a company knows of, or suspects, a leak of confidential information, it should consider instigating a formal leak investigation.

## Internal corporate policies and procedures

RG 000.14 Companies should have clear, documented policies that establish the standards of behaviour and procedures for handling confidential information that all employees are expected to comply with.

RG 000.15 Clear responsibility should be assigned within the company to oversee the implementation and enforcement of these policies and controls, and regular reviews of how the policies are working in practice will help to ensure they are being implemented effectively.

RG 000.16 To be most successful, good practices for handling confidential information should be embedded in the culture of an organisation and reinforced through regular messages from top management. Individuals need to understand why confidentiality is important and the purpose of various systems that are used to protect confidential information.

### The need-to-know principle

RG 000.17 The number of people with access to confidential information should be limited to the maximum extent possible in the circumstances. That is, only people who strictly require the information to undertake their business role should be given access to the information.

RG 000.18 Companies should take steps to minimise the risk of outsiders finding out about, or speculating on, an impending transaction. Depending on the circumstances, these steps may include:

(a) locating staff involved in sensitive transactions in secure areas that are separate from other employees and public areas;

(b) holding meetings off-site; and

(c) using specifically trained administrative support staff that are dedicated to the project.

RG 000.19 Companies should ensure that the necessary systems and controls are in place to quarantine confidential information from contractors and other third parties that share access to the company's systems.

## Information barriers and physical document management

RG 000.20 Taking great care with documents relating to a proposed transaction can assist in minimising the leakage of confidential information. Companies should consider implementing the following practices:

(a) classifying information that is created by or given to the company according to the level of protection it requires, and escalating the level of protection as the sensitivity increases;

(b) adopting a 'clean desk' policy for those employees who are handling price-sensitive confidential information;

(c) ensuring physical copies of documents relating to price-sensitive confidential transactions are securely stored in locked cabinets when not in use, with access restricted to authorised staff only;

(d) allocating dedicated printers, faxes, photocopiers, data rooms and other mechanisms for price-sensitive transactions;

(e) adopting appropriate code names for documents to disguise the parties involved in the transaction; and

(f) regularly reminding staff not to read confidential documents in public places or have confidential discussions in places they could be overheard by others (e.g. lifts).

## Information technology controls

RG 000.21 It is important that information technology systems and practices are sufficiently secure to ensure confidential information is not inadvertently leaked. Systems and practices that may help to achieve this include:

(a) storing confidential information on protected drives and tightly controlling access to these drives through password protection and blocking mechanisms;

(b) providing separate passwords when transferring confidential documents electronically. Alternatively, such documents should be encrypted;

(c) installing password protection mechanisms for all electronic equipment, such as laptops, smartphones, USB drives and other storage media containing confidential information. Automatic locking should be activated after brief periods on these devices;

(d) placing appropriate controls over indirect staff access to other employees' electronic mail;

(e) using individual PIN numbers for conference calls on sensitive transactions rather than using one group PIN. This enables the convenor of the call to identify how many separate parties have joined the call and who they are; and

(f) operating an IT system that has the capacity for a full audit trail of who has accessed particular files and when the access occurred.

## Insider lists for sensitive transactions

RG 000.22 Companies should maintain a register of both internal and external people (including directors and their staff) who are insiders on sensitive transactions, and efforts should be made to keep the number of these insiders to a minimum. Staff on an insider list should be made aware of who the other internal insiders are to ensure there is no inadvertent disclosure to staff who are not insiders.

RG 000.23 Companies should have a developed process for how and when people are brought 'inside' on sensitive transactions. Individuals should be reminded of their responsibilities each time they are made an insider and, in certain circumstances, be required to sign personal confidentiality agreements (see RG 000.30–RG 000.32).

RG 000.24 Third parties should be required to provide the company with lists, on engagement and then updated regularly, of the people within their firm that have been or will be given access to the company's confidential information. These lists should distinguish between people that are actively working on the transaction and those who are acting solely in a legal, compliance or management type role.

## Contact with the media

RG 000.25 Given that the media are likely to actively contact people they believe have inside knowledge, companies should have policies to control any interaction their staff might have with the media in relation to the company and its affairs.

RG 000.26 The existence of a binding policy and appropriate training should assist employees to deal with media questions.

### Continuous disclosure regime

RG 000.27 Listed companies should have appropriate systems in place to identify and quickly report price-sensitive information to the market when they are required to do so under Listing Rule 3.1. The ASX Corporate Governance Principles and Recommendations provide that companies should establish written policies designed to ensure compliance with these disclosure requirements.

RG 000.28 A company must comply with its continuous disclosure obligations even if the quotation of the company's shares is suspended or subject to a trading halt (see Listing Rule 18.6). Companies and their directors should be cognisant that trading can occur on markets other than the ASX and through over-the-counter (OTC) markets (such as the CFD markets), and the trading halt will not extend to those markets. Companies should also recognise the fact that a transaction in its securities may affect the trading of the company's peers and competitors.

RG 000.29 Details of a capital raising should never be provided to the market or the press before being released to ASX, regardless of whether the company's shares remain subject to a trading halt.

## Employees

### Personal confidentiality obligations

RG 000.30 Appropriate confidentiality obligations and securities trading restrictions should be incorporated into employment contracts or other arrangements with all staff (including temporary employees who may come across the confidential information). To ensure that a company can actively monitor any potential insider trading, employment contracts should also explicitly include the employer's right to access all communication records including email and phone records. An employee's confidentiality obligations should survive beyond the termination of their employment.

RG 000.31 When a company engages in highly sensitive transactions, it may be appropriate for the individuals involved in these transactions to be required to sign specific personal confidentiality agreements. Personal accountability more effectively focuses individuals on their responsibility for maintaining confidentiality.

RG 000.32 These types of confidentiality agreements should restrict individuals from discussing confidential information with other people who are not nominated as part of the transaction team. The agreements should also deal with document management, meeting protocols, securities trading restrictions and other confidentiality issues relevant to the specific transaction.

## Staff training

RG 000.33 Policies dealing with confidentiality obligations should be supported by regular training programs and internal communications, and included in induction programs for new employees. Staff should undergo training on the importance of not improperly or inadvertently divulging confidential information, with particular focus on employees with access to sensitive information.

RG 000.34 Staff should be made fully aware of the implications of improper disclosure of confidential information and the potential civil and criminal liabilities for both an individual and the company: see s180–184 of the *Corporations Act 2001*. The level of staff knowledge of, and compliance with, the company's policies on handling confidential information should be tested as appropriate, having regard to the sensitivity of the employee's position.

RG 000.35 Staff training should be reinforced by encouraging a culture that emphasises an individual's responsibility to adhere to the company's procedures and restrictions relating to confidential information.

## Personal account dealing policies and controls

RG 000.36 The ASX Corporate Governance Principles and Recommendations (Recommendation 3.2) provide that companies should establish a policy concerning trading in company securities by directors, senior executives and employees. The scope of these securities trading restrictions will depend on the specific circumstances of the company and its activities. At a minimum, a company should have policies in place that restrict trading by staff who may have confidential price-sensitive information in the company's own securities (including CFDs and other derivatives). For some companies trading restrictions should also cover securities in companies with which they are engaging in price-sensitive transactions or with whom they compete.

RG 000.37 ASX is consulting on a proposal to introduce a new Listing Rule that requires companies to adopt a trading policy that identifies the periods of the year when trading in its securities by key management personnel will be prohibited, except with clearance to trade in exceptional circumstances. Any trading would be subject to the overriding requirement that they do not have material, price-sensitive confidential information in relation to the company, as trading at that time could breach the insider trading laws.

RG 000.38 Companies should consider including a trading policy that stipulates that any employees with confidential information should obtain pre-approval from the company before trading in any restricted securities. Immediately after a trade has been executed, employees should be required to provide the designated company officer with confirmation of that trade or to authorise

that officer to receive copies of contract notes directly from the employee's broker. It may be practicable for larger organisations, particularly in the financial services industry, to have a computer compliance system that tracks, audits and oversees employees' securities transactions.

RG 000.39 Companies should also consider requiring employees in sensitive roles to disclose to the company, on a regular (e.g. semi-annual) basis, details of all their security holdings, as a check on trading in the relevant period.

### Exiting employees

RG 000.40 When employees who have access to confidential information leave the company, best practice is that exit interviews are conducted with them. The company should remind them of their ongoing responsibility to maintain the confidentiality of inside information. It may be appropriate to require written acknowledgement of this.

RG 000.41 In the context of merger transactions, there is a risk that employees who consider their position is in jeopardy become disaffected and leak information to outsiders. This issue should be addressed early on and, depending on the circumstances, appropriate termination provisions should be put in place.

## Leak investigations

RG 000.42 Companies should have written policies and procedures on how a suspected leak is to be investigated, and they should make employees aware that such a process may be undertaken if there is a suspected leak of confidential information. There should also be whistle-blower policies that make it easy for employees to report instances of confidential information being handled inappropriately.

RG 000.43 If a leak of confidential information occurs, parties should consider whether to undertake a proportionate, but formal, leak investigation. A review process not only highlights any risk areas but also acts as a deterrent, raising awareness and signalling to employees that the matter is taken seriously.

# C Releasing confidential information to third parties

**Key points**

Companies should ensure that any external party they release confidential information to has appropriate systems in place to protect that information. Confidentiality agreements should be signed to reiterate the obligation to maintain the confidentiality of information.

Companies should exercise extreme care when conducting beauty parades for advisers.

In certain circumstances, companies may establish confidentiality arrangements with advisers outside the scope of a particular transaction.

RG 000.44 Engaging advisers (such as investment banks, lawyers, accountants, tax advisers and specialist valuers) or other service providers (such as credit rating agencies, trading banks, registries, printers and public relations firms) to assist with price-sensitive transactions will necessitate the release of confidential information. This section sets out our recommended best practice for companies to adopt to minimise the risk that price-sensitive confidential information provided to an adviser or other service provider is inadvertently or deliberately misused.

## Compliance with the company's practices for handling confidential information

RG 000.45 Companies should require third parties they involve in price-sensitive confidential transactions to, at a minimum, comply with the company's confidentiality policies and procedures and insist that they operate on a need-to-know basis. Companies should obtain assurances that all parties have the necessary systems and controls in place to ensure confidentiality.

RG 000.46 Staff insiders should be made aware of all external advisory firms that have been given access to confidential information in relation to a sensitive transaction, including advisers to the board or individual board members.

## Umbrella agreements

RG 000.47 Companies that are active participants in mergers and acquisitions or capital raisings and use the services of investment banks and other advisers on a regular basis should consider setting up umbrella agreements. These types of arrangements set out in advance the general principles and practices an adviser must adhere to when undertaking work for the company. They would

be entered into when the company is consulting generally with advisers and releasing confidential information to them. Specific transactions would require additional side agreements, which would be negotiated at the time of the transaction, but all general principles, including how third parties are to handle confidential information, would be set out in the general umbrella agreement.

RG 000.48 Specific terms relating to confidentiality that this type of umbrella agreement might incorporate include:

(a) requiring advisers to:

(i) comply with the need-to-know principle in relation to all confidential information provided to them by the company and thus restrict which people in their firm the confidential information can be disclosed to;

(ii) keep all documents and information belonging to the company in a safe and secure manner and, on the company's request, promptly return or destroy such material;

(iii) establish and maintain, on request from the company, an insider list in relation to any matter on which the company has instructed the adviser;

(iv) participate in any leak investigation initiated by the company; and

(v) have in place appropriate IT systems and controls; and

(b) prohibiting advisers from:

(i) publicly disclosing they are acting for the company without prior approval from the company; and

(ii) speaking to the media in relation to the company without specific prior approval from the company, and only speaking to the media within the scope of any approval to do so given by the company.

RG 000.49 Companies should also give consideration to how their information may be used by other divisions of a service provider, and consider restricting how it may be divulged through the provider in an umbrella agreement (e.g. the credit division of a trading bank not advising the capital markets division).

## Beauty parades

RG 000.50 Conducting a 'beauty parade' to select advisers for a specific confidential transaction appears to involve a high risk of leaks, particularly from parties that miss out on a role in the transaction and have no ongoing relationship with the company. Before releasing any confidential information to potential advisers, companies should require them to sign confidentiality agreements. If investment banks are participating in the beauty parade, the confidentiality agreement should include restrictions on the particular business units of the

bank that are permitted access to the confidential information. Where possible, companies should keep the number of parties invited into beauty parades to a minimum, although we recognise the importance of competitive tension in selecting advisers.

## Confidentiality agreements

RG 000.51 All advisers should be required to sign confidentiality agreements for specific transactions. Among other things, these agreements should specifically restrict an adviser's use of the company's confidential information, including limiting the number of individuals given access to the information. The agreements should also cover conflicts of interest.

RG 000.52 Where an adviser has both private and public sides to its business, or needs to manage conflicts of interest, for example, between different clients, companies need to be confident that the adviser has in place sufficiently robust systems and controls to ensure there is no risk of the company's confidential information leaking from the private to the public side, or being used inappropriately within the firm.

# D Advisers' handling of confidential information

**Key points**

It is best practice for companies to be concerned about, and actively manage, how advisers and other service providers handle the company's confidential information.

Companies should require that their advisers and other service providers have appropriate systems in place to protect the company's confidential information.

These systems will differ to some extent from those adopted by a company, and will vary depending on the adviser's type of business.

## Advisers' and third parties' policies on confidential information

RG 000.53 Advisers (such as investment banks, lawyers, accountants or actuaries) and other third parties (such as credit rating agencies, public relations firms, share registries and printers) that receive confidential information from a client need to have appropriate systems in place to ensure that confidential information is not leaked or misused. At a minimum, these policies should incorporate the principles set out for companies (in Section B) on:

(a) internal policies and procedures (see RG 000.14–RG 000.16);

(b) the need-to-know principle (see RG 000.17–RG 000.19);

(c) information barriers and physical document management (see RG 000.20);

(d) information technology controls (see RG 000.21);

(e) staff training (see RG 000.33–RG 000.35); and

(f) exiting employees (see RG 000.40–RG 000.41).

RG 000.54 Different considerations are likely to apply to advisers (as members of the financial services industry) in relation to policies on insider lists, confidentiality agreements, personal account dealing and leak investigations. Specific discussion of these issues is included in this section. We have also included a separate section on sounding the market by financial advisers.

RG 000.55 There are a range of other issues relevant to the handling of confidential information by advisers that are outside the scope of this paper and are not specifically addressed. These include policies and procedures relating to establishing and managing information barriers between the public and private side of advisory firms, and managing conflicts of interest.

## Insider lists

RG 000.56 Advisers should actively manage the number of people at their firm that have access to a company's confidential information, and should regularly update the company with a list of those people's names.

## Confidentiality agreements

RG 000.57 Advisory firms or other service providers should include appropriate confidentiality obligations in employment contracts or other arrangements with all staff that have access to confidential information. In addition, there may be circumstances of heightened sensitivity where it is appropriate for particular employees to sign individual confidentiality agreements, as described in RG 000.31–RG 000.32.

## Personal account dealing

RG 000.58 The scope of securities trading restrictions that should be placed on the employees of advisers and other service providers will depend on the specific circumstances of the firm and its activities. Advisory firms should consider adopting the principles described in RG 000.36–RG 000.39.

RG 000.59 Advisers who regularly deal with price-sensitive confidential information relating to transactions from a range of parties should have significantly more comprehensive and restrictive controls over trading in financial products, and these should apply to all employees. To prevent the misuse of confidential information, as well as avoid real and perceived conflicts of interest, best practice is that these firms maintain lists of restricted entities. Among other things, these should cover:

(a) entities the firm is currently advising or acting on behalf of; and

(b) entities about which the firm has price-sensitive confidential information.

RG 000.60 The following guidelines are based on internal procedures adopted by some investment banks and may need to be tailored to reflect the advisory firms' actual business activities and the confidential information they receive.

RG 000.61 Advisory firms should require employees, on joining the firm, to disclose:

(a) all their investments in financial products (both listed and unlisted); and

(b) all brokerage and trading accounts they control or in which they have an interest.

RG 000.62 It may be best practice for these advisory firms to require employees to trade through an approved broker and, where that broker is not the firm itself, the employee should be required to authorise the firm to receive copies of all contract notes or records of trade directly from the employee's broker.

RG 000.63 Employees in these firms should be required to pre-clear all personal account dealing. Depending on the particular business area, it may be appropriate to impose additional restrictions on trading including:

(a) minimum holding periods; and

(b) prohibitions on trading in financial products of issuers in particular industry sectors or competitors of particular clients.

RG 000.64 Advisory firms should actively monitor employees' personal account dealing and rigorously enforce compliance with both the letter and the spirit of the restrictions.

## Leak investigations

RG 000.65 If a company's price-sensitive confidential information leaks into the market (reflected either in abnormal trading or discussion in the press), advisers and other service providers should be willing to actively participate in any leak investigation by the company. Even if the company does not initiate an investigation, we consider it best practice for any firm that had access to the leaked information to satisfy itself that the leak did not originate from any of its staff. The results of a leak investigation should be reported back to the company.

# E Sounding the market

**Key points**

An investment bank sounding the market on behalf of a client should do so in a carefully controlled manner to ensure there is no leak of price-sensitive confidential information.

RG 000.66 ASIC understands the necessity of obtaining direct market feedback from potential or existing investors about some transactions depending on the company's circumstances and on market conditions in general. However, it is important that confidentiality is maintained when sounding out capital raisings or acquisition proposals, and formal procedures should be adopted to ensure there is no breach of continuous disclosure or insider trading laws.

RG 000.67 Market practice in relation to the process of sounding has varied significantly. During the 2008–2009 financial year, we identified some examples of poorly controlled soundings. Soundings should be undertaken with greater formality and control to ensure they do not result in any leak of price-sensitive confidential information.

RG 000.68 Soundings should be a formal process that is well understood by the issuing company, its investment banks and the institutions involved. Banks should inform the company when they need to sound the market and should obtain the company's prior approval to do so. Soundings should be undertaken when the market is closed or the particular stock is in a trading halt. To help ensure confidentiality, only a limited number of parties should be sounded.

RG 000.69 Companies should have a good understanding of the process their banks intend to undertake if they sound the market in relation to a potential capital raising. This understanding should cover details of the actual process including:

(a) the specific institutions the bank intends to approach and whether the institutions have appropriate controls for protecting confidential information;

(b) the timing of any approaches;

(c) the level of coverage of the book the investment bank requires; and

(d) which institutions are to be allocated stock.

In the context of mergers and acquisitions, soundings of existing shareholders should also follow a similar process. In all cases, companies should be made aware that the bank will give certain details of the sounding process to ASIC.

RG 000.70 Individual bankers conducting the soundings should have a formal script detailing the conversation they are permitted to have with the institutions they approach for sounding. Among other things, this script should give an institution the opportunity to decline to be made an insider before the identity of the issuer or any confidential information is disclosed. If the institution agrees to be made an insider, it must agree to comply with insider trading restrictions before any confidential information is communicated. The institution should also confirm that the person providing the agreement has the authority to do so.

RG 000.71 Following this verbal agreement, and before the confidential information is disclosed, the bank should obtain written confirmation (e.g. by email) from the institution on various matters including:

(a) that the content of the conversation is confidential and may be price sensitive;

(b) that the information must be held in strict confidence until it is publicly disclosed and must not be disclosed to any third party (apart from other advisers who must also commit to the restrictions); and

(c) that the institution and the individual cannot trade or tip the particular securities.

RG 000.72 In very exceptional circumstances, where immediate written confirmation is not practicable because of timing or other restraints, verbal confirmation of these matters, together with an undertaking to provide written confirmation as soon as possible, would be acceptable.

RG 000.73 The bank must formally log all contact with the institutions it has sounded including the person making the contact, the date and time that the institution was made an insider, and the person(s) spoken to at the institution. Within 48 hours of the sounding, the bank must also notify ASIC of certain details about the sounding including:

(a) the name of all the institutions contacted (and the contact person at each) and whether each of them agreed to be made an insider;

(b) the time and date that contact was first made with each institution as well as details of when the institution was made an insider or refused to become an insider; and

(c) the particular transaction that forms the subject of the sounding.

RG 000.74 The institution should immediately notify its compliance personnel of the sounding and that it is now an insider on the particular transaction.

If the bank does not have a mandate from the company but anticipates one, or is pitching for one, the formal sounding process outlined in RG 000.68-RG 000.74 should be followed.

# Key terms

| Term | Meaning in this document |
|---|---|
| ASIC | Australian Securities and Investments Commission |
| ASX | ASX Limited (or Australian Securities Exchange) |
| beauty parade | Means a process through which companies invite advisers, such as investment banks and brokers, to tender for a role in a confidential transaction |
| Corporations Act | *Corporations Act 2001* including regulations made for the purposes of that Act |
| listed disclosing entity | Has the same meaning as s111AL(1) of the Corporations Act |
| Listing Rule | Means a listing rule which governs entities on the official list of the financial market operated by ASX Limited |
| s1043A (for example) | A section of the Corporations Act (in this example numbered 1043A) |
| over the wall | A person who has access to confidential information |
| sensitive transaction | Means a transaction that would have a material effect on the price or value of securities of a listed disclosing entity |
| soundings | Means obtaining direct market feedback from potential or existing investors |
| umbrella agreement | An agreement that sets out the general practices and principles, including how to handle confidential information, that a third party must adhere to when working on behalf of a company |

# Related information

## Headnotes

confidentiality agreements, confidential information, confidential transactions, compliance, continuous disclosure, financial adviser, third parties, information barriers, information technology, insider lists, inside information, leak investigations, market participant, personal account dealing, sounding, umbrella agreement

## Cases

R v. Rivkin (2004) 59 NSWLR 284

## Legislation

*Corporations Act 2001* Ch 6CA, s674, 675, 1043A–1043K

## Listing Rules

ASX Listing Rule 3.1

ASX Listing Rule 18.6

## Consultation papers

CP 5 *'Heard it on the grapevine'*

CP 118 *Responsible handling of rumours*

## Regulatory guides

RG 79 *Managing conflicts of interest: A guide for research report providers*

RG 181 *Licensing: Managing conflicts of interest*