

Expert Network Policy

Document Control

a. Version Control / Revision History

This document has been through the following revisions:

Version	Date of Approval	Remarks / Key changes / Reason for Update
1	November 2019	Initial version
2	May 2020	Approved changes for further clarification of applicability and pre-call checklist emails
3	November 2020	GLG confirmed as an approved Expert Network and further clarification of timing of contact with a former staff member of a listed company
4	February 2021	Revision
5	April 2021	Amended to reflect new Expert Networking monitoring procedures and ACA's recommendations.

b. Authorisation

This document requires the following approvals:

Authorisation	Name
Initial Version	Board
Revisions	Board

CONTENTS

Contents

Document Control	2
1 INTRODUCTION.....	4
1.1. Background	4
1.2. Application of Policy.....	4
2 PROHIBITIONS RELATED TO INSIDE INFORMATION	4
3 SELECTION OF EXPERT NETWORK FIRMS.....	6
3.1 Due Diligence	6
4 INTERACTION WITH EXPERTS.....	7
4.1 Restrictions on experts	7
4.2 Pre-call/meeting screening process	7
4.3 Issues and trading restrictions arising from the meeting	8
4.4 Documenting the call/meeting	8
5 MEANS OF COMMUNICATION WITH EXPERTS.....	9
6 MONITORING AND OVERSIGHT	9
7 BREACH OF POLICY.....	9
Schedule 1	10

1 INTRODUCTION

1.1. Background

Expert networks are firms that facilitate contact between individuals or organisations, typically professionals with specialised information, that are contracted by fund managers looking to build fundamental understanding of an industry and company of interest (i.e. target company). 'Experts' can include academics, scientists, engineers, doctors, lawyers, suppliers and professional participants in the relevant industry, including in some cases former employees of the target company.

This policy is to ensure that Hyperion Asset Management Limited (**Hyperion**), in its use of expert networks, is operating within insider trading laws.

1.2. Application of Policy

This policy applies to contact between Hyperion and Experts via an Expert network.

This policy does not apply to contact between Hyperion and senior management/investor relations of companies (i.e. company employees) acting in their official corporate role. This is regardless of whether the company is a portfolio holding of Hyperion or whether the contact with the company employee was organised by an expert network firm. For avoidance of doubt, this policy does not apply to contact arranged by brokers, but this does not absolve Hyperion employees of the obligation to notify the Managing Director and Risk & Compliance if they believe they have received material non-public information or inside information.

Contact with a company employee is covered by this policy if they operate outside of their official corporate role as a client of an expert network firm.

Hyperion must always conduct its business within insider trading laws and this policy must be read in conjunction with the Trading & Allocation Policy and Personal Trading Policy.

2 PROHIBITIONS RELATED TO INSIDE INFORMATION

Under s1043A of the Corporations Act, if:

- a) a person (the insider) possesses inside information; and
- b) the insider knows, or ought reasonably to know, that the information is not generally available and if the information were generally available, a reasonable person would expect it to have a material effect on the price or value of a financial product (e.g. securities; derivatives, interests in a managed investment scheme etc.);

then the insider must not (whether as principal or agent):

- i. apply for, acquire, or dispose of, the relevant financial products, or enter into an agreement to apply for, acquire, or dispose of, such financial products; or
- ii. procure another person to apply for, acquire, or dispose of, the relevant financial products, or enter into an agreement to apply for, acquire, or dispose of, such financial products; or
- iii. directly or indirectly, communicate the information, or cause the information to be communicated, to another person if the insider knows, or ought reasonably to know, that the other person would or would be likely to:
 - apply for, acquire, or dispose of, relevant Division 3 financial products, or enter into an agreement to apply for, acquire, or dispose of, relevant financial

- products; or
- procure another person to apply for, acquire, or dispose of, relevant financial products, or enter into an agreement to apply for, acquire, or dispose of, relevant financial products.

"Inside information" means information in relation to which the following paragraphs are satisfied:

- the information is not generally available;
- if the information were generally available, a reasonable person would expect it to have a material effect on the price or value of particular Division 3 financial products.

The United States Advisers Act and SEC has similar restrictions, but guidance refers to 'inside information' as 'material nonpublic information'.

Section 204A of the Advisers Act requires every investment adviser to establish, maintain, and enforce written policies and procedures reasonably designed, taking into consideration the nature of such investment adviser's business, to prevent the misuse of material nonpublic information or "inside information" by such investment adviser or any associated person. In the past, the U.S. federal securities laws have been interpreted to prohibit the following activities:

- Trading by an insider while in possession of material nonpublic information;
- Trading by a non-insider while in possession of material nonpublic information, where the information was disclosed to the non-insider in violation of an insider's duty to keep it confidential;
- Trading by a non-insider who obtained material nonpublic information through unlawful means such as computer hacking; and
- Communicating inside information to others in breach of a fiduciary duty.

Material non-public information is broadly defined in the Advisers Act and SEC guidance, and is included below:

What Information is Material?

Many types of information may be considered material, including, without limitation, advance knowledge of:

- Dividend or earnings announcements;
- Asset write-downs or write-offs;
- Additions to reserves for bad debts or contingent liabilities;
- Expansion or curtailment of company or major division operations;
- Merger, joint venture announcements;
- New product/service announcements;
- Discovery or research developments;
- Criminal, civil and government investigations and indictments;
- Pending labour disputes;
- Debt service or liquidity problems;
- Bankruptcy or insolvency;
- Tender offers and stock repurchase plans;
- Recapitalization plans; and
- Major developments in litigation or events that could lead to litigation (e.g., a cyber breach or a data leak).

Information provided by a company could be material because of its expected effect on a particular class of securities, all of a company's securities, the securities of another company, or the securities of several companies. The prohibition against misusing Material Nonpublic Information applies to a wide range of financial instruments including, but not limited to, equities, bonds, warrants, options, futures, forwards, swaps, commercial paper, government-issued securities, and Digital Securities. Material information need not relate to a company's business. For example, information about the contents of an upcoming newspaper column may affect the price of a security, and therefore be considered material. Advance notice of forthcoming secondary market transactions could also be material.

Employees should consult with Compliance if there is any question as to whether nonpublic information is material.

What Information is Nonpublic?

Once information has been effectively distributed to the investing public, it is no longer nonpublic. However, the distribution of Material Nonpublic Information must occur through commonly recognized channels for the classification to change. In addition, there must be adequate time for the public to receive and digest the information. Non-public information does not change to public information solely by selective dissemination. The confirmation by an insider of unconfirmed rumours, even if the information in question was reported as rumours in a public form, may be nonpublic information. Examples of the ways in which nonpublic information might be transmitted include, but are not limited to:

- In person;
- In writing;
- By telephone;
- During a presentation;
- By email, instant messaging, or Bloomberg messaging;
- By text message or through Twitter; or
- On a social networking site such as Facebook or LinkedIn.

Employees must be aware that even where there is no expectation of confidentiality, a person may become an insider upon receiving Material Nonpublic Information. Employees should consult with Compliance if there is any question as to whether material information is nonpublic.

3 SELECTION OF EXPERT NETWORK FIRMS

3.1 Due Diligence

Prior to entering into an agreement with an expert network firm, Hyperion must conduct appropriate due diligence.

At a minimum, Hyperion must request the following information:

- approval process of experts;
- processes employed for checking the backgrounds of the experts; and
- practices employed by the expert network firm to monitor the expert's compliance with insider trading laws.

Agreements must be reviewed by Risk & Compliance prior to execution, particularly in relation to compensation and the representations and warranties provided therein. Final approval of the arrangement with the expert network firm rests with the Managing Director.

Hyperion relies on the practices employed by the expert network firm to ensure:

- (a) the experts understand the definition of material non-public information, and that the experts have agreed not to disclose any such information, or any other information that is confidential in the consultation with Hyperion; and
- (b) transcripts available from the expert network have been reviewed by the expert networks' compliance team and all material nonpublic information has been removed.

Given this reliance, Hyperion will annually contact the expert network to confirm:

- (a) whether the expert network's policies have changed;
- (b) if any issues have been found during the last year; and
- (c) that their testing has remained in line with their stated policies.

The approved expert network firms currently engaged by Hyperion are listed in **Schedule 1**.

4 INTERACTION WITH EXPERTS

4.1 Restrictions on experts

Hyperion employees must not interact with any expert unless that expert satisfies the pre-call/meeting screening process outlined in section 4.2.

In Hyperion's request to the expert network firm for the recommendation of an expert, the Hyperion employee must clearly state:

- the target company(ies) if any;
- the desired expert background; and
- the general purpose behind the use of such an expert.

While Hyperion will generally rely on the expert network firm to undertake appropriate background checks on the experts it recommends, employees must be vigilant regarding any "red flags" on the expert's background information that is supplied by the expert network firm.

4.2 Pre-call/meeting screening process

Prior to any interactions with an expert, the Hyperion employee must seek pre-approval for the call from the Managing Director via email (copying Pinnacle Risk & Compliance).

The email requesting approval for contact with an expert must include answers to the following questions obtained from the expert network firm (or the expert themselves):

1. The expert understands the definition of material non-public information, and has agreed not to disclose any such information, or any other information that is confidential in the consultation with Hyperion.
2. Provide the name of the company(ies) the expert is affiliated with and their role at the company(ies), as well as their recent employment history, to confirm whether the expert was in the past 6 months, employed by or consulted to any target company(ies) that Hyperion has nominated in its request?
There needs to be at least one profit result or trading update between the Expert leaving the listed organisation that Hyperion holds or is considering holding in the portfolios and any scheduled meetings with Hyperion staff.

A template email is provided in Schedule 2.

As part of the due diligence process in Section 3, Hyperion has confirmed with each of the approved Expert Networks that they have policies to ensure the experts understand the definition of material non-public information, and that the experts have agreed not to disclose any such information, or any other information that is confidential in the consultation with Hyperion. Consequently, Question 1 above is satisfied for the approved Expert Networks in Schedule 1.

A calendar invite with details of the pre-approved call and dial-in details must be circulated to Risk & Compliance prior to the call to provide them the ability to chaperone the call in accordance with Section 6 of this policy.

Employees can only proceed with the expert interaction if the expert has not been disqualified by the screening questions.

Surveys and Transcripts

If the proprietary survey offering from GLG wishes to be used, the Hyperion employee must provide the list of questions to the Managing Director prior to the initiation of the survey for pre-approval (copying in Pinnacle Risk & Compliance) and ensure the

questions are not an attempt to solicit material, non-public information.

For completeness, any transcripts available from the expert network can be accessed without preapproval. The expert networks' compliance teams review these transcripts prior to them being made available and confirm material nonpublic information is removed.

4.3 Issues and trading restrictions arising from the meeting

Despite the screening process, where an employee identifies potential inside information being discussed during the meeting, they must immediately terminate the call and bring it to the attention of the Managing Director and Risk & Compliance.

No sharing or other use should be made with respect to such information, pending completion of the review process. If necessary, securities of the relevant issuers will be added to Hyperion's restricted list to ensure appropriate monitoring of future trading. This restriction applies to both Hyperion's portfolio and personal trading. The restriction remains in place until the Managing Director and the Risk & Compliance agrees to remove the security from the restricted list.

4.4 Documenting the call/meeting

The content of the call/meeting must be summarised and lodged on Hyperion's Evernote system.

The employee must record the call/meeting in their Outlook calendar, and the entry should include (1) date of the call, (2) name of each employee that participated in the call, and (3) name and title of the expert that participated in the call.

The employee must also update Hyperion's Company Meetings worksheet in the Meetings & Time Allocation workbook (Company Meetings and Tags worksheet) and ensure the entry clearly refers to the relevant Expert Network. An estimate of the dollar amount for the cost of the call must be included.

The same applies for any transcripts or surveys covered under this policy.

5 MEANS OF COMMUNICATION WITH EXPERTS

Hyperion prohibits employees from using informal means of communication, e.g. text messaging and social networking websites, when interacting with experts. Employees can only communicate by phone or in person with experts and, to a limited extent, via email. Email communications are limited to co-ordinating meetings with experts or to follow up points of clarification.

6 MONITORING AND OVERSIGHT

On an ongoing basis, Risk & Compliance will randomly select to chaperone employee discussions with experts.

Risk & Compliance will also review the call log of Hyperion and from the expert network firms and sample check the calls to ensure that this policy has been adhered to.

7 BREACH OF POLICY

Any employee breach of this this policy will be dealt with in accordance with the Incident Reporting Policy.

Schedule 1

APPROVED EXPERT NETWORK FIRMS

- Third Bridge
- Field Research
- GLG
- Tegus

Schedule 2

Template email for pre-approval

Mark/Compliance,

Seeking approval for a call with the below specialist via [insert expert network name], an approved Expert Network.

[Insert name of Specialist]

[Insert list of current employer and role] [Insert list of former employers and roles]

[Insert names of relevant portfolio stock holdings]

There has been more than one profit result or trading update between the Expert leaving the organisation that Hyperion holds or is considering holding in the portfolios and this proposed meeting.

Compliance has reviewed the expert network's policies and guidelines that aim to ensure the expert understands the definition of material non-public information, and the expert has agreed not to disclose any such information in our call.

Regards,