

# Boardroom questions

## Unpublished Price Sensitive Information (UPSI)

Board Leadership Center



### Insider trading – a harsh reality

Insider trading creates an unfair advantage for those who profit from securities based on Unpublished Price Sensitive Information (UPSI).

As per Securities and Exchange Board of India (SEBI) Prohibition of Insider Trading Regulations, 2015 (PIT Regulations), UPSI means any information relating to a company or its securities, directly or indirectly that is not generally available, which upon becoming available, is likely to materially affect the price of the securities.

### UPSI leakages

In addition to external data threats, companies nowadays are facing increasing internal attacks. These have been described as the 'five Es':



### Amendments to SEBI Prohibition of Insider Trading Regulations, 2015

Following are some of the stringent regulatory requirements post the December 2018 amendments:

- All trades undertaken while in possession of UPSI will be presumed to be 'motivated' by UPSI, unless proven otherwise
- 'Designated persons' are required to disclose 'material financial relationships', employment history and educational institutes attended by them
- Whistle-blower policies to provide for employees to report instances of leakage of UPSI
- 'Informants' voluntarily reporting instances of insider trading to SEBI may get awarded up to INR1 crore
- Separate code of conduct required for intermediaries and fiduciaries dealing with listed companies' UPSI

### Implication of defaults:

As per section 15G of the SEBI Act, 1992, fines can be as high as INR25 crore or three times the amount of profits made from insider trading, whichever is higher. Imprisonment for a term, which may extend up to 10 years, or fine or both may also be levied in cases of contravening provisions of SEBI or any rules made thereunder.



## Boardroom questions

### Tone at the top

1. What are the standard operating procedures to identify, classify, process and store UPSI?
2. What is the contractual coverage of third parties and 'insiders' dealing with UPSI?
3. What are the policies and procedures that ensure compliance with SEBI PIT regulations, and how are such responsibilities communicated?
4. How effectively are UPSIs discarded?
5. How effectively are all stakeholders educated on the requirements of PIT regulations?



### Chief Finance Officer

1. How is the existing financial statement closure process safeguarded?
2. How are subsidiary-level material financial information safeguarded?
3. How well is communication with third parties protected?
4. How is routine data protected?
5. Is the finance team sufficiently distanced from other office spaces with restricted access?



### Chief Human Resources Officer

1. How are 'designated persons' educated on their roles and responsibilities while in possession of UPSI?
2. Are companies' social media policies exhaustive and effective to prevent UPSI leakages?
3. To avoid market speculation, how effectively are important announcements/disclosures protected?
4. What is the contractual coverage of employees' obligations vis-à-vis UPSI?
5. Are employees motivated to report UPSI leakages or even suspected leakages?



### Chief Compliance Officer/ Company Secretary

1. Are the lists of 'designated persons' and 'connected persons' regularly updated; how is their compliance ensured?
2. How are board and audit committee meetings guarded from UPSI leakages?
3. What determines 'legitimate purposes' of sharing UPSI?
4. How is compliance with amended PIT regulations ensured?
5. In cases of UPSI leakages, are whistle-blower policies sufficiently robust?
6. How do companies ensure 'pre-trade clearance'?



### Chief Information Technology Officer

1. How well are potential risks and vulnerabilities related to accounting applications, IT infrastructure and network components identified; also, are these timely?
2. How effectively and to what extent are vendors providing IT support services—who may have access to UPSI—made responsible, and how closely is this access monitored?
3. Are data servers and financial information backups well protected?



**Suveer Khanna**  
Partner  
Forensic Services  
KPMG in India



**Ritesh Tiwari**  
Partner  
Risk Consulting  
Leader, Board Leadership Center  
KPMG in India

[home.kpmg/in](http://home.kpmg/in)

#KPMGjosh

Follow us on:  
[home.kpmg/in/social-media](http://home.kpmg/in/social-media)



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2019 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

This document is for e-communication only. (033\_FLY1219\_RV)