KPMG

ASSOCHAM INDIA

The 'insider' threat - Safeguarding UPSI

home.kpmg/in

SEBI regulations on the leakage of price sensitive information

The Securities and Exchange Board of India (SEBI) was among the first, and has been seen to be one of the more operative in terms of delivering on a mandate that includes:

- Protection of the investor
- Prudential regulation of securities markets intermediaries and
- Development of the markets

But it was felt overtime that the regulations needed to be further strengthened to serve their purpose. Resultantly, SEBI (Prohibition of Insider Trading (Amendment) Regulations, 2018 and SEBI (Prohibition of Insider Trading (Amendment) Regulations, 2019 were introduced. The amended regulations are aimed at ensuring accountability and robust control framework to prevent insider trading. The amendments are effective from April 1, 2019

It has been widely reported in the media, that the regulator is concerned about strong network of brokers and/or analysts seeking to glean data that they should not be privy to, and circulate the same among their clientele. This phenomena known as 'Heard on Street' (HOS) is seen as a regular behaviour by the brokers/analysts, however, recent events indicate that this conduct is questionable.

SEBI has framed regulations such as SEBI Prohibition of Insider Trading Regulations (PIT), 2015[1] to combat the menace of trading in securities with the unfair advantage of having access to 'Unpublished price sensitive information' (UPSI) which when published would impact the price of securities in the market. Any person who uses sensitive information not known to general public to make a profit either for themselves or a third party in the securities of a company is in breach of aforementioned laws laid down by SEBI. These regulations were originally framed in 1992 and thereafter, amended with revised regulations in 2015.

But it was felt overtime that the regulations needed to be further strengthened to serve their purpose. Resultantly, SEBI (Prohibition of Insider Trading (Amendment) Regulations, 2018 and SEBI (Prohibition of Insider Trading (Amendment) Regulations, 2019 were introduced. The amended regulations are aimed at ensuring accountability and robust control framework to prevent insider trading. The amendments are effective from April 1, 2019.

Leakage of any UPSI (covered under the definition of UPSI under regulation 2(n) of PIT Regulations) is prohibited and is in contravention of regulation 3(1) and (2) of SEBI (Prohibition of Insider Trading) Regulations 2015 (PIT Regulations) read with section 12A (e) of the Securities and Exchange Board of India Act, 1992 (SEBI Act) which prohibit procurement or communication of UPSI. The said provisions read as under:

Regulations 3(1) and (2) of PIT Regulations:

- 3(1) No insider shall communicate, provide, or allow access to any unpublished price sensitive information, relating to a company or securities listed or proposed to be listed, to any person including other insiders except where such communication is in furtherance of legitimate purposes, performance of duties or discharge of legal obligations
- 3(2) No person shall procure from or cause the communication by any insider of unpublished price sensitive information, relating to a company or securities listed or proposed to be listed, except in furtherance of legitimate purposes, performance of duties or discharge of legal obligations

Section 12A (e) of the SEBI Act[2]

- (e) Deal in securities while in possession of material or non-public information or communicate such material or non-public information to any other person, in a manner which is in contravention of the provisions of this Act or the rules or the regulations made thereunder

According to SEBI Act 1992 section 15G and subsequent amendment in 2014[3], a minimum penalty of INR10 lakh, which may extend up to INR25 crore, or three times the amount of profits made out of insider trading, whichever is higher, can be levied. In addition, if any person contravenes or attempts to contravene or abets the contravention of the provisions of the SEBI Act or of any rules or regulations made thereunder, he shall be punishable with **imprisonment for a term which may extend to ten years**, or with fine, which may extend to **INR25 crore or with both.**

1. SECURITIES AND EXCHANGE BOARD OF INDIA (PROHIBITION OF INSIDER TRADING) REGULATIONS, 2015, SEBI, 15th January 2015, accessed on 1 March 2018
2. THE SECURITIES AND EXCHANGE BOARD OF INDIA ACT, 1992, SEBI, 4th April 1992, accessed on 1 March 2018
3. THE SECURITIES LAWS (AMENDMENT) ACT, 2014, SEBI, 22nd August 2014, accessed on 1 March 2018

What constitutes unpublished price sensitive information (UPSI)?

A company these days has multiple applications installed with various data sources generating large and varied datasets. UPSI typically would consist of information which is confidential or is not public knowledge, which when disclosed to the public is likely to materially impact the performance of the companies' stocks.

The SEBI (PIT) Regulations, 2015 defines UPSI as:

'Unpublished price sensitive information' (UPSI) means any information, relating to a company or its securities, directly or indirectly, that is not generally available which upon becoming generally available, is likely to materially affect the price of the securities and shall, ordinarily including but not restricted to, information relating to the following: –

1. Financial results
2. Dividends
3. Change in capital structure
4. Mergers, de-mergers, acquisitions, delisting, disposals and expansion of business and such other transactions
5. Changes in key managerial personnel
6. All material events required to be disclosed as per the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 (LODR) may not necessarily be UPSI and hence have been omitted from the list of information/ event to be considered UPSI.

'Generally available Information' means information that is accessible to the public on a non-discriminatory basis.

Primarily, for a listed company, there are two types of data that constitute UPSI:

Material information: Every listed company has to disclose events or information which is material in nature. Companies prepare a materiality policy to help determine such material events or information. This would include information pertaining to executing large contracts, obtaining regulatory licenses, launch of civil, regulatory or criminal actions etc.

- Further, SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 lists certain deemed material events, which have to be mandatorily disclosed.

Since all such material events may not be UPSI, Companies would have to exercise caution and their own judgment to determine which of these deemed material events and other material events as determined by the materiality policy of the company would be UPSI as they are likely to affect the price of the company's securities and hence qualify as UPSI. Companies should ensure that confidentiality of such information is preserved and is only communicated on a 'need-to-know' basis.

Financial information: Financial statements would be considered to be UPSI as they are likely to affect the price of the company's securities.

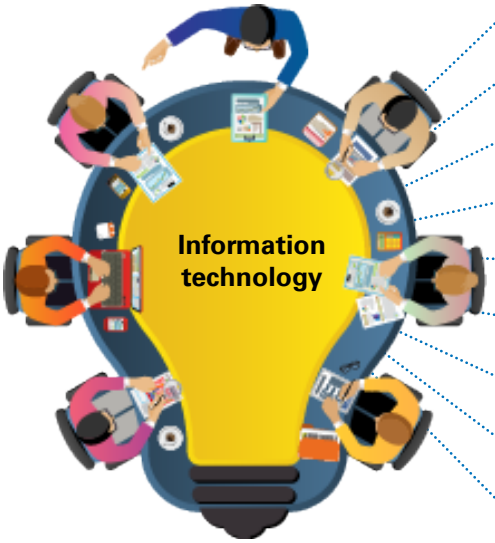
Indicative UPSI list

Sales and Expense	EBIDTA and net profit	Financials of subsidiary information
Standard operating procedure	Employee remuneration	Promoter group remuneration
Future management decisions	Key projections	Buybacks or rights issues
Stressed assets and Non-Performing Assets (NPAs)	Creditors and Debtors	Write offs

Indicative list of teams handling UPSI

Multiple teams are involved in handling data from various sources for creating and managing datasets required for the preparation of accounts and financial statements. Some or all of these datasets are UPSI and should be handled with utmost care to ensure datasets are available with designated persons only.

The indicative list of teams who handle UPSI at some stage of the financial statements preparation are shown alongside.



- Corporate finance and accounts
- Financials planning and analysis
- Investor relations
- Corporate secretarial team
- Taxation
- MD/CEO/CFO office
- Board of directors
- Audit committee
- Statutory auditors /Tax consultants

An indicative workflow in preparation and finalisation of quarterly earnings is depicted below.

- Prepartion of quarterly financial results begins
- Sales and expense numbers locked in accounting system
- Corporate finance consolidates financials from multiple divisions, if applicable
- Draft financials shared with Internal teams like planning and analysis, taxation, treasury as well as external teams like auditors and tax consultants
- Individual departments work on their set of deliverables parallely
- Consolidated financials ready for circulation
- Finalised consolidated financials are shared wih respective teams for their consumption
- Financials shared with senior management for their review
- Finalised board presentation shared with corporate Secreterial team
- Investor relations team prepares investor presentation, investor call commentary etc.
- Board and audit commitee presentation prepared and ready for circulation
- Corporate secreterial team shares audit commitee presentaion, board deck with board of directors and audit commitee members via

The general timeframe between quarter closure and the declaration of quarterly earnings results vary between 15 – 45 days and a few days more for annual results

As mentioned earlier, technology has made access to data easier. However, it has opened multiple ways in which perpetrators can get access to companies' UPSI. Based on KPMG in India's experience of executing multiple data theft related investigations, captured below are a few key avenues which make companies prone to data theft.

Social engineering

Insider threats

Malware attacks

Software vulnerabilities

Phishing

Lack of data classification

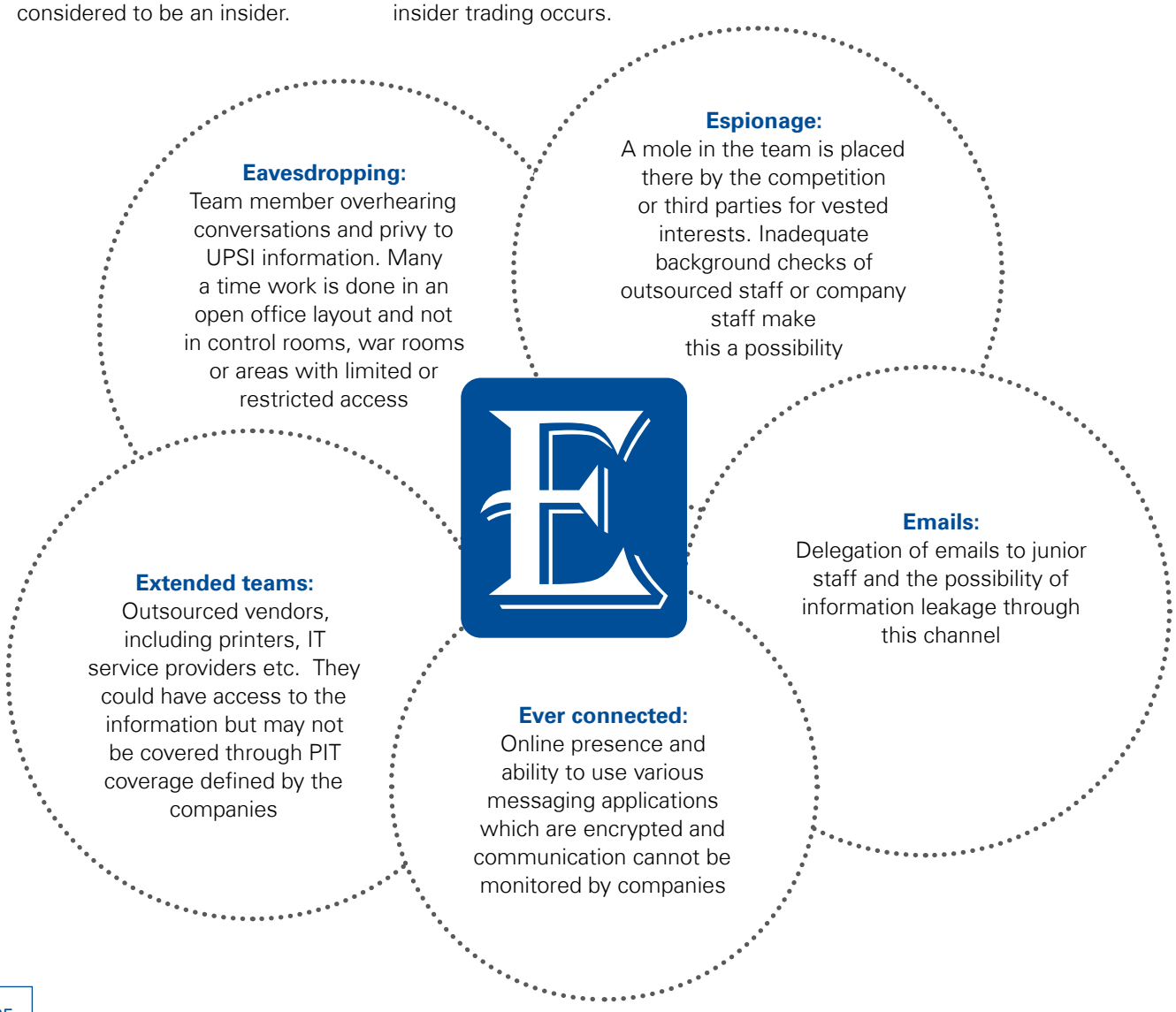
Who is an insider?

The SEBI (PIT) Regulations, 2015 prohibit insiders from communicating UPSI or trading in securities while in possession of UPSI. Insiders include any person who is in possession or has access to UPSI and any connected person. A connected person refers to any person who had been associated with the company up to six months prior to the concerned act, which allowed such a person to have access to UPSI or is reasonably expected to have such access. Further, any person related to these connected persons are termed as 'deemed connected' persons as per the regulations, and would be considered to be an insider.

As required under the SEBI (PIT) Regulations 2015, every company frames a Code of Conduct to regulate, monitor and report trading, where certain employees (including their immediate relatives) on the basis of their role and function have access to UPSI in addition to their professional designation (as defined in the amended regulations) are termed as 'designated employees.' The regulations extend to such employees of material subsidiaries of the listed company. The compliance officer of the company should maintain this list of designated employees and monitor their trades to ensure no insider trading occurs.

Further, the compliance officer should also ensure that any person falling outside the purview of the company's Code of Conduct and who may otherwise have possession of UPSI should also be covered as an insider.

In addition to external attacks towards attempts of data thefts, companies these days are being further exposed to Insider threats which is summarized as the **'five Es'** below:



Preserving the confidentiality of UPSI

Recently, there were reports in the media about financial results/ components of price sensitive data of several companies being leaked on private groups of instant messaging application hours or days ahead of official company announcements through their quarterly earnings results. The messages posted in these groups were allegedly precise leading to suspicions around insider trading activities. SEBI conducted various search and seizure operations and is investigating complaints of individuals spreading UPSI through messaging application and other mediums.[4]

As noted, the communication of UPSI is also prohibited. Even if no trading happens pursuant to such communication, the mere act of communication of UPSI is an offence under the regulations. The internal control systems of the company should be structured in such a manner that the UPSI is not communicated to anyone except in the furtherance of legitimate purposes, for performance of duties or for discharge of legal obligations.

In addition to an insider communicating the UPSI, procurement of UPSI by any other person is also a violation under the regulations. To avoid any unintentional access to UPSI, the companies should enforce strict separation of departments dealing with UPSI. Access to such departments should be restricted and no information, physical or otherwise, should be allowed to be transmitted outside the department except for legitimate purposes, for performance of duties or for discharge of legal obligations.

Companies should strengthen the internal control systems to ensure UPSI is not communicated. The amended Regulations address internal controls framework that companies should create.

Further SEBI by way of another amendment (SEBI (Prohibition Of Insider Trading)(Third Amendment) Regulations 2019)), introduced an Informant mechanism. This would serve as reporting mechanism for violations relating to insider trading and incentivizing (upto INR1 crore or as specified) and protecting such informants who report information related to violation of Insider trading laws. This would incentivise informants to pro-actively report such issues to SEBI.

Insider trading - A harsh reality

'Insider trading' is an undesirable practice that breaches the fundamental principle of 'Information symmetry' and tends to distort the market by creating unfair advantage in favour of those who profit on the basis of Unpublished Price Sensitive Information (UPSI).

Unfair practices like 'Insider Trading' are detrimental to the market integrity and pose a serious challenge to market participants including investors, investee companies, market regulators and intermediaries.

The perils of this unfair practice may put other market participants in an unfavorable position and result in loss of investor confidence in the securities market, which may, in turn adversely impact the process of raising capital.

According to the International Company of Securities Commissions (IOSCO)'s paper on 'Objectives and Principles of Securities Regulation' published in May 2003, the three objectives of good securities market regulation are:

1. Investor protection
2. Ensuring that markets are fair, efficient and transparent, and
3. Reducing systemic risk.

4. Sebi identifies 34 in WhatsApp earnings leak case, Business Standard, 23 December 2017

What is the regulator expecting companies to do?

Recent actions of the regulators clearly show that they are monitoring UPSI leakage, and requesting companies to:

- Strengthen the key pillars of people, process and technology to avoid leakage of UPSI
- Identify present system and controls on UPSI, responsibility of who manages such controls and periodicity of such a review
- If required, conduct an appropriate enquiry or investigations.

Company's responsibilities in handling UPSI include the following:

- Preservation of UPSI is an important duty of the company. Only responsible people should have access to UPSI and it should only be communicated in furtherance of legitimate purposes, performance of duties or for discharge of legal obligations.
- No private persons or non-employees, especially family members of the board of directors, should have access to the board meetings.
- For the preparation, discussion and finalisation of unpublished information, a dedicated room should be used and the persons involved in such preparation should be shifted to the said room. There should be a clear prohibition on discussing UPSI outside this room.
- Educating all insiders about the sensitivity of information and to restrict disclosures on 'need to know' basis and on the requirement to have differential closure of trading window depending on the nature of UPSI and manner in which information is to flow.
- Prepare a code of conduct policy for the preservation of data for the prevention of insider trading and for its designated persons and their immediate relatives.

  Fiduciaries and Intermediaries and every other person required to handle UPSI will be required to frame a code of conduct for trading by designated persons (and their immediate relatives) in securities.

  Amend the Code of Fair Disclosures in Conduct to include Policy for determination of legitimate purposes for sharing of UPSI; where legitimate purpose shall include sharing of UPSI in the ordinary course of business by an insider with partners, collaborators, lenders, customers, suppliers, merchant bankers, legal advisors, auditors, insolvency professionals or other advisors or consultants, provided that such sharing has not been carried out to evade or circumvent the prohibitions of these regulations.

  Companies to initiate appropriate inquiries on becoming aware of leak/ suspected leak of UPSI and inform SEBI of such leaks, inquiries and results of such inquiries.
- Prepare and maintain a list of designated persons and regularly update it. Ensure proper procedures to monitor their trades are in place. Designated persons shall provide information including details of their past employers and educational institutes. Additionally, they should provide names, Permanent Account Number (or any other identifier authorized by law), of their immediate relatives and persons with whom they share a 'material financial relationship',
- Implement and periodically review internal controls and processes to prevent leakage of UPSI including:
  - Identify all employees with access to UPSI as designated persons
  - Identify all UPSI and maintain its confidentiality
  - Place adequate restrictions on communication or procurement of UPSI
  - Responsibility of BOD to ensure that CEO/MD implements and ensures above internal controls
  - Audit Committee shall review effectiveness of these internal controls atleast once in a year.
- A company should always ensure:
  - Strictest confidentiality on price sensitive information - Employees do not discuss confidential data with other employees or with family or friends
  - Audit teams or teams working on UPSI data should not take any UPSI data outside the company
  - Audit committee and Board meetings should be scheduled one after another and preferably on the same day.

- Adherence to Company's internal code/protocol while speaking to press/public forums
- Trading in securities of any other company, of whom the company's executives have UPSI, is barred
- Maintenance of structured digital database with details such as persons/entities with whom UPSI is shared
- Investment team/ committee/ research desk of the company has 'Chinese wall' protection from such team as may have UPSI in relation to clients
- Restricted access of financial information could be considered in a module wise manner.
- Trading by all employees in company's securities are disclosed or blocked all together
- All employees involved in handling UPSI should be made aware of closure of trading window and take prior approval for any trading while trading window is open. They should also be made aware of contra trade restrictions

Additionally, in our view companies should ask themselves the following questions to identify inherent risks in handling UPSI. This is an indicative, not an exhaustive, list.

- Are there any standard operating procedures (SOPs) for handling the UPSI?
- Is there a complete list of teams / team members involved in handling UPSI?
- Is there an inventory of all locations where UPSI is being stored?
- Is the data required for working on financials stored on our server? Is the server access restricted to select individuals? Do we have all the names?
- Do we use password protection while sharing confidential information amongst team members via emails?
- Are audit logs / audit trails captured and reviewed to identify any potential instances of unauthorised access or intrusion attempts?
- Do we conduct information security assessments prior to and post the financial data preparation to identify any potential risks and vulnerabilities?
- Does the team undergo any data security sensitisation trainings?

Conclusion

Securing UPSI and ensuring that the data doesn't fall in wrong hands is critical for a company to ensure continued investor confidence, preserving its own reputation and goodwill in the market. Both these factors go a long way in ensuring smooth sailing for the company in these days of volatile markets and increased regulations and scrutiny.

It is imperative for companies to document the policy and process used to manage UPSI and ensure a comprehensive audit of the same from time to time. Red flags, if identified, from the audits should be documented and steps should be taken to mitigate the risks.

Increased awareness, automation and simplifying the whole process for Insiders to comply is the key. In many a cases, it is observed that ignorance leads to faults; hence the focus should be on educating and making employees and insiders aware of the law and the processes.

Additionally, companies may look at implementing a few good practices, as indicated below:

Invest in the right technology to:

- Avoid data leakage IP-based controls, blocking of emails containing key words, recording calls and restricted usage of mobile phones
- Avoid storing sensitive data over Internet or Public Online Storage Space
- Encryption and password protect the sensitive files
- Ensure physical security and encryption of data stored on computers
- Strengthen the procedures of data and data holding asset in storage and physical transit through use of offline and online encryption methods.

Invest in the right processes, for instance:

- Prepare an indicative list what can be UPSI and circulate it to all the employees, with guidance on how to handle it - should include the 'material events' as described in the materiality policy of the company, prepared as per the requirement under the SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015
- Use only official emails/ channels for sharing information and avoid public emails
- Try to create a separate work space with secured access for teams working on preparing financials during the 'non trading window'.

Invest in people controls to:

- Identify persons involved in major deals/activities and instruct them to not share any sensitive information beyond that set of people. Ensure information is percolated down to juniors or external teams only on a 'need to know' basis
- Ensure the proper background checks are in place for staff dealing with UPSI data
- Inculcate the culture to report on any attempt of breach and conduct refresher trainings around the sensitivity of the role played
- Monitor any significant price changes just before the declaration of financial earnings for any significant fluctuations proactively.

At the end, investigate as appropriate to ensure there is no exposure. Perhaps an innocuous failed login attempt locking a user account or a social taping to fetch sensitive information could be your next breach!

About ASSOCHAM

THE KNOWLEDGE ARCHITECT OF CORPORATE INDIA

The Associated Chambers of Commerce and Industry of India (ASSOCHAM), India's premier apex chamber covers a membership of over 4 lakh companies and professionals across the country. ASSOCHAM is one of the oldest Chambers of Commerce which started in 1920. ASSOCHAM is known as the "knowledge chamber" for its ability to gather and disseminate knowledge. Its vision is to empower industry with knowledge so that they become strong and powerful global competitors with world class management, technology and quality standards.

ASSOCHAM is also a "pillar of democracy" as it reflects diverse views and sometimes opposing ideas in industry group. This important facet puts us ahead of countries like China and will strengthen our foundations of a democratic debate and better solution for the future. ASSOCHAM is also the "voice of industry" – it reflects the "pain" of industry as well as its "success" to the government. The chamber is a "change agent" that helps to create the environment for positive and constructive policy changes and solutions by the government for the progress of India.

As an apex industry body, ASSOCHAM represents the interests of industry and trade, interfaces with Government on policy issues and interacts with counterpart international organizations to promote bilateral economic issues. ASSOCHAM is represented on all national and local bodies and is, thus, able to pro-actively convey industry viewpoints, as also communicate and debate issues relating to public-private partnerships for economic development.

About KPMG in India

KPMG in India, a professional services firm, is the Indian member firm affiliated with KPMG International and was established in September 1993. Our professionals leverage the global network of firms, providing detailed knowledge of local laws, regulations, markets and competition. KPMG has offices across India in Ahmedabad, Bengaluru, Chandigarh, Chennai, Gurugram, Hyderabad, Jaipur, Kochi, Kolkata, Mumbai, Noida, Pune and Vadodara.

KPMG in India offers services to national and international clients in India across sectors. We strive to provide rapid, performance-based, industry-focussed and technology-enabled services, which reflect a shared knowledge of global and local industries and our experience of the Indian business environment.

home.kpmg/in

Acknowledgements

KPMG in India

Avinash Kharkar
Darshini Shah
Iqra Bhat
Karan Marwah
Karan Sunthankar
Manish Deo
Meenakshi Sharma
Muntazar Sayed
Nisha Fernandes
Sudesh Anand Shetty
Suveer Khanna
Venkatesh Iyer
Kaushal Mehta

ASSOCHAM

Santosh Parashar
Abhishek Saxena
Jatin Kochar
Aditya Muvvala
Anish Yadav

CONTRIBUTORS:

Finsec Law Advisors

Anil Choudhary
Partner, Finsec Law Advisors
Raghuvamsi Meka
Associate, Finsec Law Advisors

KPMG in India contacts:

Vijay Chawla
Partner and Head
Risk Advisory
T: +91 80 6833 5509
E: vschawla@kpmg.com

Jagvinder S. Brar
Partner and Head
Forensic services
T: +91 124 3369 469
E: jsbrar@kpmg.com

Karan Marwah
Partner and Head
Capital Markets
T: +91 124 336 9064
E: kmarwah@kpmg.com

Suveer Khanna
Partner
Forensic services
T: +91 22 3090 2540
E: skhanna@kpmg.com

Sudesh Anand Shetty
Partner
Forensic services
T: +91 22 6134 9703
E: sashetty@kpmg.com

home.kpmg/in

ASSOCHAM contacts:

Santosh Parashar
Additional Director & Head Corporate
Affairs and Capital Market Division
ASSOCHAM
E: santosh.parashar@assocham.com

Abhishek Saxena
Assistant Director
Corporate Affairs Division
ASSOCHAM
T: +91 11 4655 0547
E: abhishek.saxena@assocham.com

#KPMG josh

Follow us on:
home.kpmg/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.